TRUNG TÂM TIN HỌC - ĐẠI HỌC KHOA HỌC TỰ NHIÊN TP.HCM

227 Nguyễn Văn Cừ - Quận 5 – TP. Hồ Chí Minh
Tel: 8351056 – Fax 8324466 – Email: ttth@hcmuns.edu.vn

BÀI TẬP

CHƯƠNG TRÌNH KỸ THUẬT VIÊN

Ngành MẠNG & PHẦN CỨNG

Học phần III

MÔN HỌC
DỊCH VỤ MẠNG
WINDOWS 2003

Mã tài liệu: DT_NCM_MG_BT_DVMS

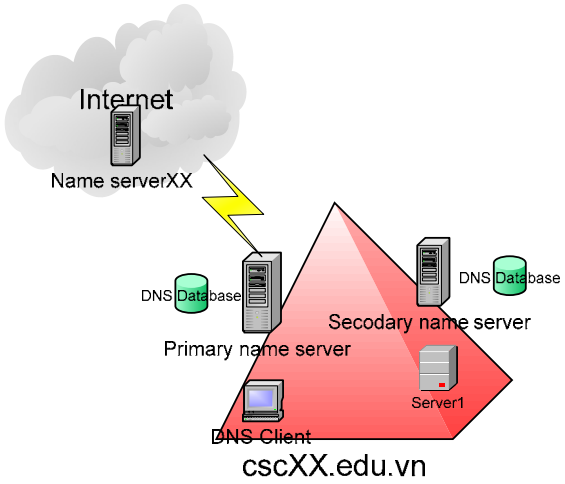
Phiên bản 1.0 – Tháng 09/2005

MỤC LỤC

MỤC LỤC **2**
Bài 01 Dịch Vụ DNS **3**
Bài tập 01.1 3
Bài tập 01.2 5
Bài 02 Dịch Vụ FTP **7**
Bài tập 02.1 7
Bài tập 02.2 9
Bài 03 Dịch Vụ Web **11**
Bài tập 03.1 11
Bài tập 03.2 13
Bài 04 Dịch Vụ Mail **14**
Bài tập 04.1 14
Bài tập 04.2 16
Bài 05 Dịch Vụ Proxy **17**
Bài tập 01 17
Bài tập 05.2 19
Bài Tập Ôn Tập Cuối Môn **21**
Phần Hướng Dẫn Giải **22**
Bài 01 Dịch Vụ DNS **23**
Bài tập 01.1 23
Bài tập 01.2 35
Bài 02 Dịch Vụ FTP **38**
Bài tập 02.1 38
Bài tập 02.2 51
Bài 03 Dịch Vụ Web **53**
Bài tập 03.1 53
Bài tập 03.2 64
Bài 04 Dịch Vụ Mail **67**
Bài tập 04.1 67
Bài tập 04.2 69
Bài 05 Dịch Vụ Proxy **96**
Bài tập 05.1 96
Bài tập 05.2 155

Bài 01
Dịch Vụ DNS

Bài tập 01.1



Một mạng LAN có sơ đồ như hình vẽ và có đường mạng là 192.168.10.200+XX (XX là số thứ tự máy). Các máy tính trong mạng có tên và địa chỉ IP như sau :

Miền cscXX.edu.vn có một số thông tin cụ thể như sau:

- Primary name server có tên dns1 có địa chỉ IP: 192.168.10.200+XX
- Secondary name server có tên dns2 có địa chỉ IP: 192.168.10.201+XX
- Máy dns1 là máy chủ www, ftp, mail, proxy.
- Máy Client có địa chỉ : 192.168.10.200+XX

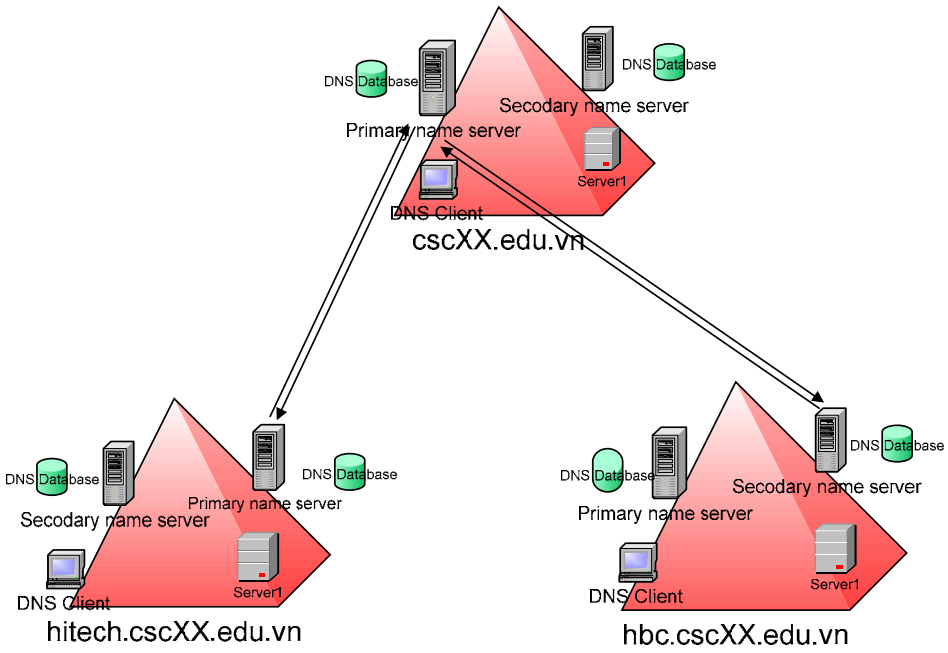
Giả sử máy tính ta đang ngồi là máy tính dns1 chạy hệ điều hành Windows 2003, ta dự định dùng làm Primary DNS Server, WWW server, MAIL server, FTP server. Ta đăng ký một domain name là "cscXX.com.vn", đăng ký địa chỉ ip cho các server từ nhà cung cấp dịch vụ (ISP) VNNIC.

➢ **Yêu cầu :**

1. Cài đặt dịch vụ DNS trên máy chủ dns1.
2. Cấu hình dns1 là một Primary Name Server cho domain name của mình với những dữ liệu đã cho.
3. Khai báo DNS Client (resolver) cho máy trạm và sau đó dùng tiện ích **nslookup, ping** để kiểm quá trình phân giải tên miền vừa được cấu hình.
4. Cấu hình forwarders cho máy chủ dns1 lên server chủ phía trên có tên là **name serverXX có thể có địa chỉ như sau:** 203.162.4.1, 203.162.0.11 hoặc máy chủ DNS trong phòng server của cơ sở đào tạo.

5. Dùng trình tiện ích nslookup để phân giải các tên miền ngoài quốc tế như: vnn.vn, yahoo.com, cisco.com, microsoft.com, hcmuns.edu.vn. Anh/Chị hãy ghi nhận lại các thông tin về địa chỉ name server, địa chỉ mail server, địa chỉ web server của các miền trên.
6. Dùng máy tính bên cạnh làm secondary name server để backup cơ sở dữ liệu của primary name server, sau đó kiểm tra tính năng dự phòng của máy.
7. Cấu hình DDNS cho phép máy trạm khi đăng nhập mạng có thể đăng ký RR trực tiếp vào DDNS Server hoặc đăng ký RR thông qua DHCP Server.

Bài tập 01.2



Cho sơ đồ mạng như hình vẽ, hệ thống có đường mạng chính là 192.168.10.0/24, hệ thống tên miền được tổ chức như sau:

Miền chính csc.edu.vn có một số thông tin cụ thể như sau:

- Primary name server có tên dns1 có địa chỉ IP: 192.168.10.200+A1
- Secondary name server có tên sdns có địa chỉ IP: 192.168.10.200+A2
- Máy server1 là máy chủ www, ftp, mail, proxy địa chỉ IP: 192.168.10.200+A3
- Máy Client có địa chỉ : 192.168.10.200+A4

Miền con hbc.cscXX.edu.vn được uỷ quyền từ miền cha có một số thông tin cụ thể như sau:

- Primary name server có tên dns-hbc có địa chỉ IP: 192.168.10.200+B1
- Secondary name server có tên sdns-hbc có địa chỉ IP: 192.168.10.200+B2
- Máy dns1 là máy chủ www, ftp, mail, proxy
- Máy Client có địa chỉ : 192.168.10.200+B3

Miền con hitech.cscXX.edu.vn được uỷ quyền từ miền cha có một số thông tin cụ thể như sau:

- Primary name server có tên dns-hitech có địa chỉ IP: 192.168.10.200+C1
- Secondary name server có tên sdns-hitech có địa chỉ IP: 192.168.10.200+C2
- Máy dns-hbc là máy chủ www, ftp, mail, proxy.

- Máy Client có địa chỉ : 192.168.10.200+C3

Ta đăng ký một domain name là "cscXX.edu.vn". Sau đó, ta cung cấp cho mỗi vùng một subdomain có tên miền: hitech.netXX.com và hbc.netXX.com.

Chú ý:

- ***XX là số thứ tự nhóm.***
- ***A1,A2,A3,A4,B1,B2,B3,C1,C2,C3 là số thứ tự máy.***

Yêu cầu : 6 máy lập thành một nhóm để hoàn thành bài tập này, 2 máy quản lý một subdomain.

- ***Miền chính cscXX.edu.vn do hai máy có tên dns1 và sdns quản lý***

1. Cấu hình dns1 (máy thứ 1) là một Primary Name Server cho domain name cscXX.edu.vn của mình với những dữ liệu đã cho.
2. Cấu hình dns1 ủy quyền hai subdomain hitech.cscXX.edu, hbc.cscXX.edu cho hai server dns-hitech và dns-hbc quản lý.
3. Cấu hình sdns (máy thứ 2) là một Secondary Name Server cho miền chính cscXX.edu.vn, miền con hbc.cscXX.edu.vn, miền con hitech.cscXX.edu.vn.
4. Kiểm tra sự phân giải của domain vừa cấu hình và sự liên thông với những domain khác.

- ***Miền con hbc.cscXX.edu.vn do hai máy kế tiếp có tên dns-hbc và sdns-hbc quản lý***

1. Cấu hình dns-hbc (máy thứ 3) là một Primary Name Server cho subdomain hbc.cscXX.edu.vn của mình với những dữ liệu đã cho.
2. Cấu hình sdns-hbc (máy thứ 4) là một Secondary Name Server cho subdomain hbc.cscXX.edu.vn.
3. cấu hình forwarders cho máy dns-hbc để chuyển yêu cầu phân giải miền ngoài lên máy dns1.
4. Kiểm tra sự phân giải của domain vừa cấu hình và sự liên thông với những domain khác.

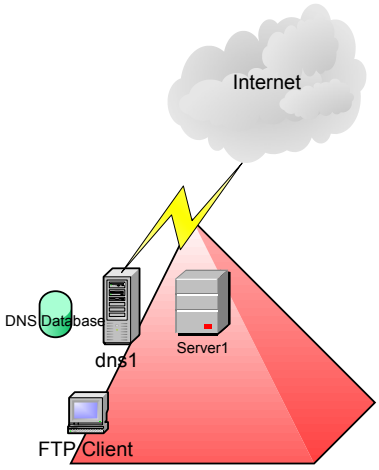
- ***Miền con hitech.cscXX.edu.vn do hai máy kế tiếp có tên dns-hitech và sdns-hitech quản lý***

1. Cấu hình dns-hitech (máy thứ 5) là một Primary Name Server cho subdomain hitech.cscXX.edu.vn của mình với những dữ liệu đã cho.
2. Cấu hình sdns-hitech (máy thứ 6) là một Secondary Name Server cho subdomain hitech.cscXX.edu.vn.
3. cấu hình forwarders cho máy dns-hitech để chuyển yêu cầu phân giải miền ngoài lên máy dns1.
1. Kiểm tra sự phân giải của domain vừa cấu hình và sự liên thông với những domain khác.

Bài 02
Dịch Vụ FTP

Bài tập 02.1

Mô hình kết nối mạng của Trung Tâm Tin Học có tên miền cscXX.edu.vn như sau (trong đó XX là số thứ tự của máy tính đang ngồi)



cscXX.edu.vn

Tên máy	Địa chỉ IP	Hệ điều hành sử dụng	Chức năng
Dns1	192.168.100.200+XX/24	Windows 2003 Server	Primary name server.
server1	192.168.100.200+XX/24	Windows 2003 Server	FTP Server.

1. Cài đặt và cấu hình DNS trên dns1 là Primary name server của miền cscXX.edu.vn, và ftp.cscXX.edu.vn là alias của server1.cscXX.edu.vn.
2. Cài đặt FTP Service trên máy chủ Server1, sau đó thực hiện các yêu cầu sau:
   a. Tạo một Public FTP site(sử dụng chế độ **"do not isolation user"**) với FTP home directory C:\inetpub\ftproot.
   b. Dùng trình tiện ích computer management , tạo user "ftpuser". Cấu hình cho phép kết nối vô danh (anonymous connection) và bỏ tùy chọn "Allow only anonymous connection". Kiểm tra việc truy cập dùng user anonymous và user "ftpuser".
   c. Chọn tuỳ chọn chỉ cho phép kết nối vô danh "Allow only anonymous connection", thử truy cập bằng user vô danh anonymous, và dùng ftpuser.
   d. Tạo các thông điệp Welcome:" xin chào các bạn đã đến FTP server của chúng tôi " và thông điệp Exit: "Hẹn gặp lại lần sau" .

e. Cấm máy bên cạnh có địa chỉ IP 192.168.100.200+XX/24 truy cập vào FTP server của mình. Kiểm tra kết quả bằng cách truy cập từ máy bên cạnh.

f. Tạo thư mục c:\SOFT, ánh xạ thành thư mục ảo trên FTP server với alias là "*download*", cho phép mọi người dùng bên ngoài truy xuất FTP Server qua anonymous user.

g. Tạo thư mục c:\pub, ánh xạ thành thư mục ảo trên FTP server với alias là "upload", cho phép mọi người dùng có thể upload tài nguyên thông qua anonymous user.

h. Dùng các tập lệnh của FTP client để, sau đó dùng lệnh get, mget, prompt, lcd…để thực hiện quá trình download một vài file từ thư mục download của FTP server về máy cục bộ.

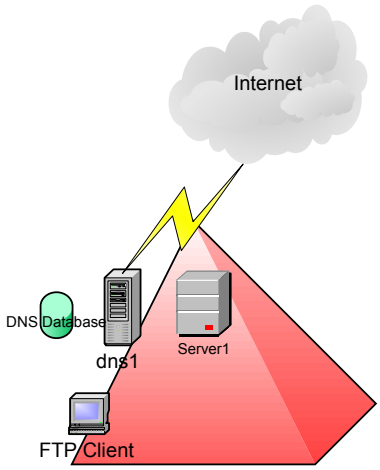
i. Dùng Winword tạo một file *.doc sau đó dùng lệnh put, mput, lcd,… để upload tập tin này lên thư mục upload của FTP Server.

j. Sử dụng các phần mềm làm FTP Client như: IE, Windows Commander, cutftp để truy xuất vào FTP server.

k. Tạo thư mục ảo /data trong FTP site trỏ đến D:\Webdata. Gán quyền sao cho nhóm Webmasters có quyền đọc ghi trong thư mục FTP, mọi user còn lại chỉ có quyền đọc. Thử lại bằng FTP client bằng user anonymous và user thuộc nhóm Webmasters (tạo một số user thuộc nhóm Webmasters trước khi kiểm tra).

l. Kiểm tra xem kết nối giữa FTP Server và FTP Client theo cơ chế gì?

Bài tập 02.2



cscXX.edu.vn

Tên máy	Địa chỉ IP	Hệ điều hành sử dụng	Chức năng
Dns1	192.168.100.200+XX/24	Windows 2003 Server	Primary name server.
server1	192.168.100.200+XX /24	Windows 2003 Server	FTP Server.

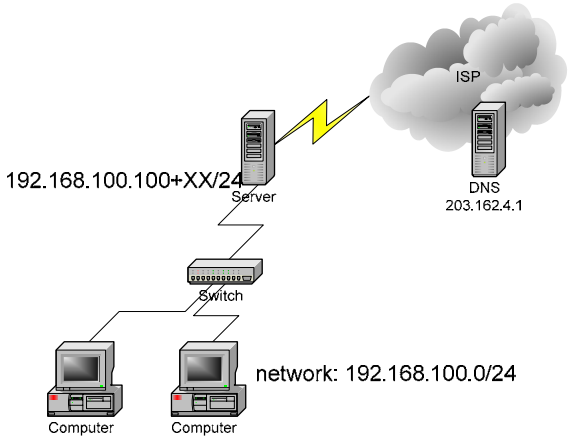
Mô hình kết nối mạng của Trung Tâm Tin Học có tên miền cscXX.edu.vn như sau (trong đó XX là số thứ tự của máy tính đang ngồi)

1. Trên Server1 tạo thêm địa chỉ IP: 172.16.XX.1
2. Cài đặt và cấu hình DNS trên dns1 là Primary name server của miền cscXX.edu.vn với:
   - ftp.cscXX.edu.vn. Alias (CNAME) server1.cscXX.edu.vn.
   - vftp.cscXX.edu.vn Host (A) 172.16.XX.1
3. Cài đặt FTP Service trên máy chủ Server1, sau đó thực hiện các yêu cầu sau:
   a. Tạo một Public FTP site có tên ftp.cscXX.edu.vn với FTP home directory C:\inetpub\ftproot. (sử dụng chế độ **"do not isolation user"**).
   b. Tạo FTP Site mới có tên vftp.cscXX.edu.vn sử dụng chế độ "Isolation User"
      - home directory: d:\ftpnet.
      - FTP Permission : Read + Write.
      - Tạo FTP home directory cho từng người dùng trong hệ thống, sau đó cấp quyền sao cho mỗi người dùng chỉ được phép truy xuất FTP home directory của mình.

4. Dùng Windows Commander để kiểm tra.

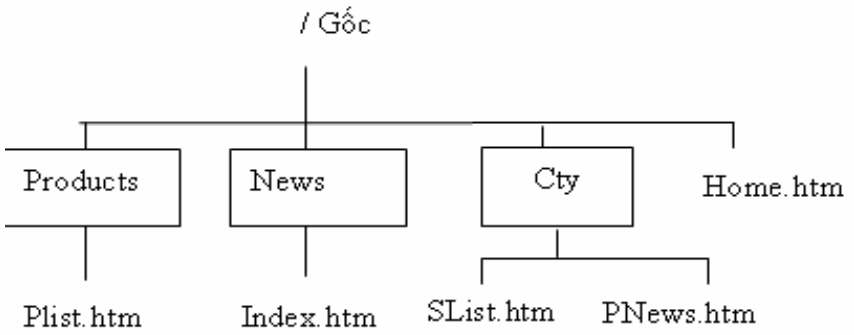
Bài 03
Dịch Vụ Web

Bài tập 03.1



*Bạn là người quản trị cho một mạng máy tính của **công ty XX** kết nối lên Internet như hình vẽ. Máy chủ cài Win2k3 server và máy làm phục vụ dịch vụ DNS, Mail, Web, FTP cho công ty. Công ty thuê một tên miền "**ctyXX.com.vn".***

1. **Tổ chức Web server.**
   a. **Tạo Web site cho công ty ctyXX theo cấu trúc sau:**



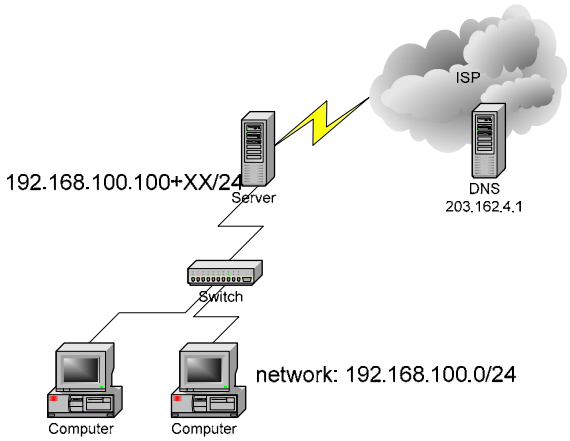
   - Trong đó gốc là thư mục C:\web, *Products là thư mục ảo* (Virtual Directory) chỉ đến thư mục **C:\PRO**.

   b. Cấp một số quyền hạn truy xuất Web site theo yêu cầu:
   - Các user có quyền *browsing* trên thư mục Products.
   - Cấu hình sử dụng tập tin default cho 2 thư mục / và /News. (/ là ***home.htm***; /News là ***index.htm***)
   - Trang Web **home.htm** có liên kết đến 2 trang **plist.htm** và **index.htm**
   - Trong trang plist.htm có link có nội dung " **Contact : nvlinh@ctxx.com** " và dùng để gởi mail liên hệ với công ty.
   - Các trang **Plist.htm** và **Index.htm** có liên kết nội dung "**Về Trang Chủ**" chỉ đến trang chủ.

2. cấp quyền truy xuất cho Website cho người dùng

a. Giả sử có các tổ chức người dùng: Nhóm QL(admin, manager, gd, webmaster), nhóm NV có các Users(nv1, nv2),
b. Các tập tin trong thư mục Cty chỉ cho các user của công ty truy xuất (không cho user Anonymous truy xuất), tập tin /Cty/Slist.htm chỉ cho user administrator và gd xem.
c. Tạo một thư mục ảo có tên **tailieu** ánh xạ về thư mục thật d:\soft, cho phép mọi người trong công ty có quyền truy xuất tài nguyên này nhưng chỉ có user webmaster mới có quyền Upload tài nguyên.
d. Không cho phép tất cả các máy trong đường mạng 192.168.12.0 truy xuất webserver.

Bài tập 03.2

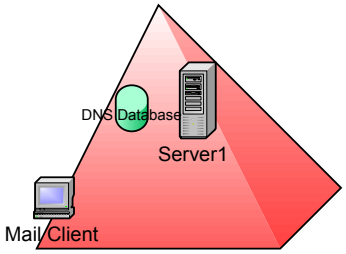


*Bạn là người quản trị cho một mạng máy tính của **công ty XX** kết nối lên Internet như hình vẽ. Máy chủ cài Win2k3 server và máy làm phục vụ dịch vụ DNS, Mail, Web, FTP cho công ty. Công ty thuê một tên miền "**ctyXX.com.vn**"*

1. Tìm hiểu cấu hình cơ chế quản trị Web site, FTP site(Administration Web Site) thông qua trình duyệt web.
2. Download tập tin sf2k_v34_051.zip từ \\192.168.11.1\soft (hoặc download từ Web site: http://ovh.dl.sourceforge.net/sourceforge/sf2k/sf2k_v34_05.zip), cấu hình cho phép người dùng có thể sử dụng Forum thông qua địa chỉ **http://www.ctyXX.com.vn/forum**.
3. Giả sử Web server này hosting cho một Web site của các công ty con có tên truy xuất www.cna.ctyXX.com.vn. Cấu hình Web site này cùng hoạt động với Web site www.Ctyxx.com.vn. Giả sử trang web chủ cho Web site www.cna.ctyXX.com.vn có tên index.htm, Dữ liệu Web được lưu trữ tại thư mục C:\WebDH.
4. Cấp quyền cho Webmaster có quyền cập nhật Web site cho trang www.cna.ctyXX.com.vn thông qua dịch vụ FTP.

Bài 04
Dịch Vụ Mail

Bài tập 04.1



cscXX.edu.vn

Bạn là người quản trị cho một mạng máy tính cho trung tâm đào tạo tin học (có sơ đồ kết nối như hình vẽ). Máy chủ Server1 cài Win2k3 server và máy làm phục vụ dịch vụ DNS, Mail, Web, FTP cho công ty. Công ty thuê một tên miền "**cscXX.edu.vn",** cấu hình máy chủ Server1 này theo yêu cầu sau.

1. Nâng cấp Server1 thành domain controller để quản lý cơ sở dữ liệu cho miền cscXX.edu.vn, trong quá trình nâng cấp cho phép hệ thống cài DNS tự động sao đó hiệu chỉnh lại một số thông tin cho dịch vụ DNS tương ứng với các dữ liệu sau:

Mailbox	Host(A)	172.168.10.100+XX
Server1	Host(A)	172.168.10.100+XX
www	Alias(CNAME)	Server1.cscXX.edu.vn.
ftp	Alias(CNAME)	Server1.cscXX.edu.vn.
cscXX.edu.vn	MailExchanger(MX)	mailbox.cscXX.edu.vn.

2. Cài đặt Exchange trên Server1 để cung cấp hệ thống thư điện tử (E-mail) cho miền "cscXX.edu.vn". Sau khi cài đặt hoàn tất ta tạo các group mail sau:
   - Nhóm **Admins** bao gồm các user sau:
     - Nvbinh (Nguyễn Văn Bình)
     - Dcphung (Đặng Công Phụng)
   - Nhóm **Phongmay** bao gồm các user sau:
     - nqhuy (Nguyễn Quang Huy)
     - ndcan (Nguyễn Đình Can)
     - bvquy (Bùi Văn Quý)

- Nhóm **Vanphong** bao gồm các user sau:
  - ntcthuy (Nguyễn Thị Cẩm Thuý)
  - nttdung (Nguyễn Thị Thuỳ Dung)
  - ntmthao (Nguyễn Thị Mai Thảo)
- Nhóm **Nhanvien** bao gồm các user sau:
  - (Admins, Phongmay,Vanphong)
- Nhóm **Giamdoc** bao gồm các user sau:
  - Ndchinh (Nguyễn Đình Chinh)
  - Ltcan (La Thanh Cần)

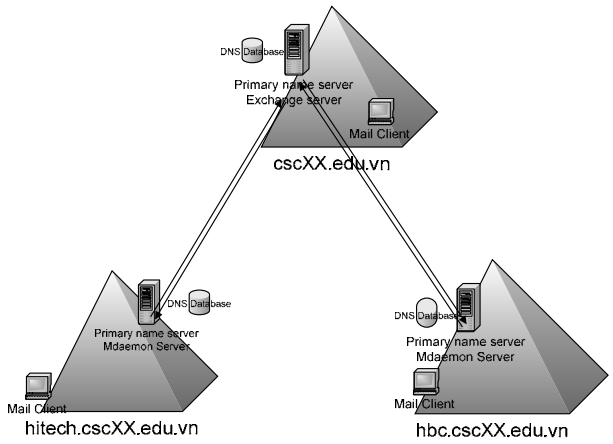
Tạo các Alias Mail như sau:

- Admins có alias banquantrimang
- Dcphung có alias webmaster
- Dcphung có alias admin

3. Sử dụng mail thông qua Web hoặc qua POP Client
   - Dùng trình duyệt web để gởi nhận mail bằng Webmail bằng cách truy xuất mail thông qua địa chỉ http://<IIS_Web>/exchange
   - Dùng services tool để khởi động một số services liên quan tới exchange như MS Exchange POP3, MS Exchange IMAP4, … để cho phép mọi người dùng có thể sử dụng mail thông qua MS Outlook Express, Eudora.
4. Sử dụng MS Outlook Express để làm POP3 Client hoặc IMAP Client để soạn thảo và nhận thư từ máy trạm.
5. Sử dụng tập lệnh SMTP & POP3 để thực hiện quá trình send/receive mail thông qua dòng lệnh.

Bài tập 04.2

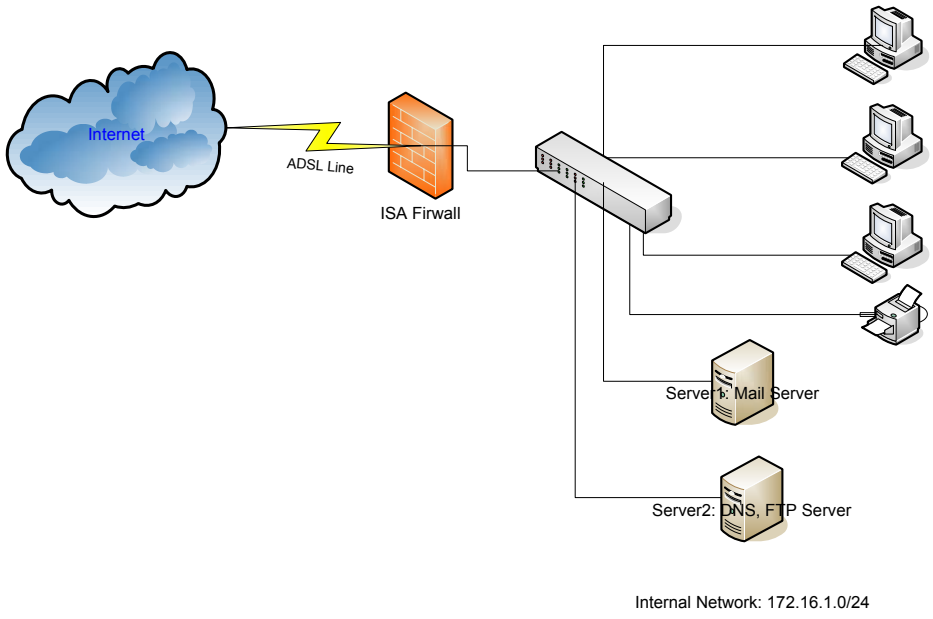
1. Cài đặt Exchange trên Server1 để cung cấp hệ thống thư điện tử (E-mail) cho miền "cscXX.edu.vn". Sau khi cài đặt hoàn tất ta tạo các group mail sau:
2. Cấp một số quyền hạn sau:
   - Mỗi hộp thư của tài khoản có dung lượng tối đa cho phép là 20M.
   - Chỉ cho phép các tài khoản trong nhóm Admins và Giamdoc trên được sử dụng Web mail, OMA, POP3, IMAP. Các user còn lại chỉ sử dụng Webmail, POP3.
   - Dung lượng tối đa của **Public Folder** được lưu trên server 100M, cho phép mọi người dùng có thể sử dụng **Public Folder**.
   - Ngăn địa chỉ mail abc@yahoo.com gởi mail vào miền nội bộ, chặn tất cả email từ miền nội bộ gởi tới người dùng có địa chỉ mlbadmail@yahoo.com
   - Ngăn chặn địa chỉ mạng 192.168.10.0 không được connect và mail server.
   - Khai báo Smart host có địa chỉ mail.hcm.vnn.vn để chỉ định mail gateway cho mail server nội bộ.
   - Cấu hình relay mail cho tất cả các miền bên ngoài gởi mail vào miền nội bộ, chỉ không relay cho máy trong mạng 172.29.0.0/16.
3. Cài đặt Mdaemon sau đó tìm hiểu cơ chế tổ chức và quản lý hệ thống mail thông qua Mdaemon (cài đặt trên server khác) sau đó thực hành lại bài tập 2,3,4 và tìm hiểu một số tùy chọn nâng cao khác.
4. Tổ chức mail cho ba miền sau có thể trao đổi mail với nhau.



Bài 05
Dịch Vụ Proxy

Bài tập 01

Bạn là người quản trị cho một mạng máy tính cho trung tâm đào tạo tin học (có sơ đồ kết nối như hình vẽ). Máy chủ Server1 cài Win2k3 Server và cung cấp dịch vụ Mail Server. Server2 là DNS, FTP Server cho công ty, công ty thuê một tên miền "**cscXX.edu.vn"** sau đó dùng phần mềm ISA để triển khai Firewall và cung cấp dịch vụ Proxy để protect hệ thống mạng nội bộ.



1. Cài đặt ISA Firewall trên máy tính chủ có ít nhất hai card mạng để tổ chức hệ thống kết nối như trên sơ đồ.
2. Cấu hình ISA Firewall theo các yêu cầu sau:
    - Cấu hình trên ISA Firewall như một Proxy Server sao cho có thể chia sẻ kết nối Internet cho các máy tính trong Internal network (sử dụng cổng 8080)
    - Cấm các máy tính trong mạng 192.168.XX.0/24 truy xuất Internet.
    - Cho phép tất cả các máy tinh trong mạng được truy xuất Internet nhưng trong giờ hành chánh không được truy xuất vào các trang như: *.yahoo.com, *.vnn.vn, *.vnexpress.net.
    - Chỉ cho phép các máy trong mạng nội **ping** tới ISA Firewall.

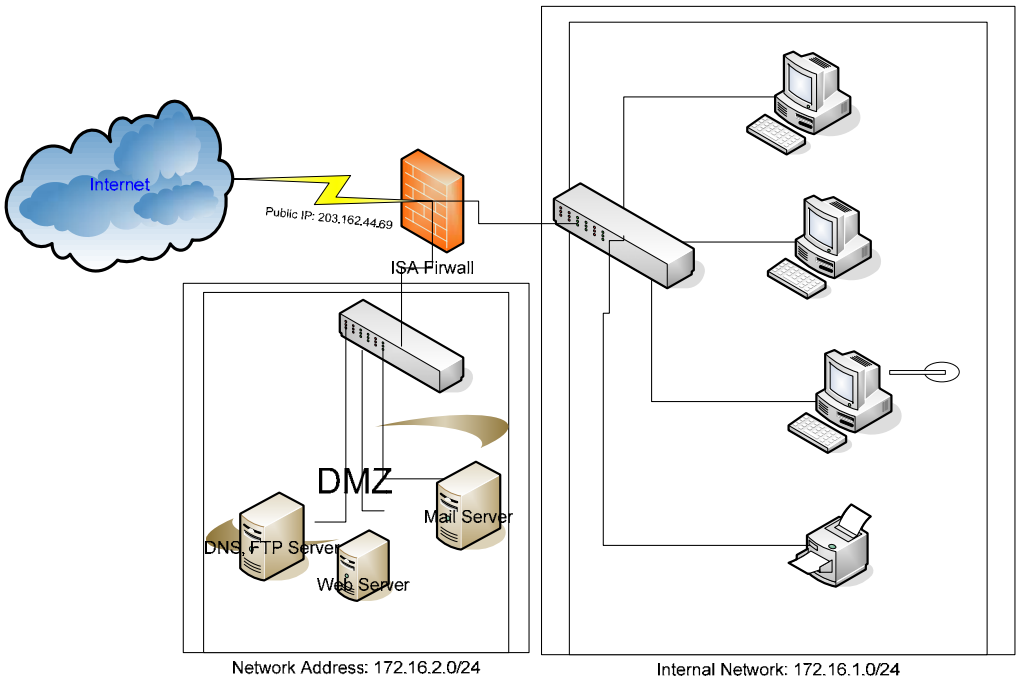
- Cho phép một số máy trong mạng nội bộ có thể truy xuất Internet thông qua cơ chế NAT được cung cấp trên ISA Firewall.
- Cấu hình **route uptream** lên proxy cha có địa chỉ 192.168.11.1
- Proxy dùng kết nối dial-up lên VNN theo thông tin account dial-up.

3. Cấu hình Caching:
   - Cấu hình Cache memory size : 100MB
   - Tạo rule cache cho ISA proxy để theo dõi và quản lý các cache objects
4. Khai báo Proxy server là máy Server1 cho máy trạm để tiến hành kiểm tra.

Bài tập 05.2

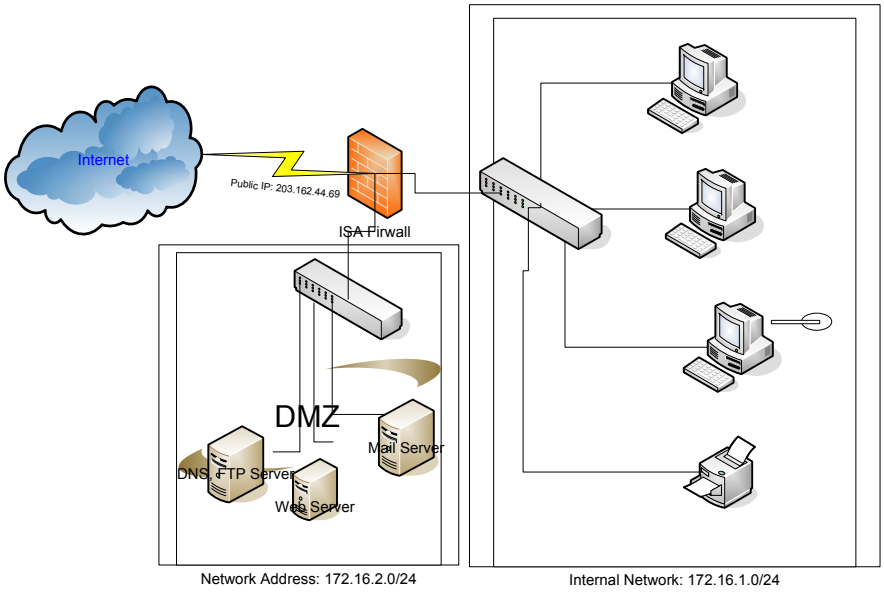
Bạn là người quản trị cho một mạng máy tính cho trung tâm đào tạo tin học (có sơ đồ kết nối như hình vẽ trong **Bài tập 05.1**). Máy chủ Server1 cài Win2k3 Server và cung cấp dịch vụ Mail Server. Server2 là DNS, FTP Server cho công ty, công ty thuê một tên miền "**cscXX.edu.vn"** sau đó dùng phần mềm ISA để triển khai Firewall và cung cấp dịch vụ Proxy để protect hệ thống mạng nội bộ.

1. Publishing Server:
    - Tổ chức trong mạng nội bộ một hoặc vài máy chủ cung cấp dịch vụ DNS, WWW, FTP, Mail,…
    - Dùng cơ chế Publish Server trên ISA Firewall để publish các Server trên để cho phép bên ngoài Internet có thể sử dụng các dịch vụ được cung cấp trong mạng nội bộ.
2. Theo dõi Web log và xử lý sự cố lỗi:
    - Thiết lập luật cảnh báo cho các dịch vụ được cung cấp trong mạng nội bộ.
    - Cấu hình cho phép ta có thể theo dõi và quản lý Web log qua giao diện được cung cấp trong ISA Firewall.
3. Một số công cụ bảo mật:
    - Cài đặt chương trình download security để thực thi một số phương thức bảo mật cho dịch vụ proxy như:
        - Cấm download các file có phần mở rộng là *.exe, *.zip.
        - Cấm download các file có kích thước >1MB.
        - Kiểm tra virus cho các file download từ internet.
    - Cài đặt chương trình Surfcontrol Web Filter để thực thi một số thao tác giới hạn truy xuất Web cho mạng nội bộ như:
        - Không cho phép mạng nội bộ sử dụng **Web mail** trên internet trong giờ hành chánh.
        - Không cho phép **chat** trong giờ hanh chánh.
4. Tìm hiểu cơ chế tổ chức hệ thống ISA Firewall theo mô hình Tri-home như sau:


Internet
Public IP: 203.162.44.69
ISA Firwall
DMZ
Mail Server
DNS, FTP Server
Web Server
Network Address: 172.16.2.0/24
Internal Network: 172.16.1.0/24

Bài Tập Ôn Tập Cuối Môn

Cho sơ đồ kết nối mạng của Trung tâm đào tạo công nghệ thông tin như sau:



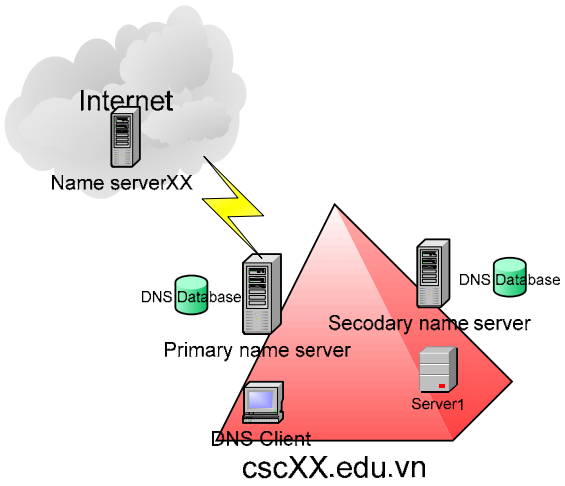
Trung tâm đào tạo thuê một tên miền "**cscXX.edu.vn**" từ VNNIC (XX là số thứ tự nhóm), trung tâm này muốn tổ chức mạng nội bộ có sơ đồ như hình trên. Trong mạng nội bộ có cung cấp đầy đủ các dịch vụ như Mail Server (Dùng Exchange Server), Web, FTP, DNS. Học viên có thể dùng 1 máy ServerXX nào đó để tổ chức các dịch vụ như: WWW, FTP, Mail, DNS theo các yêu cầu sau:

1. DNS quản lý tên miền "csc.edu.vn" sao cho có thể phân giải được tất cả các tên của các máy cung cấp các dịch vụ trong vùng DMZ.
2. Cấu hình dịch vụ FTP sao cho có thể cung cấp 1 FTP site chung cho mọi người dùng có thể truy xuất tài nguyên thông qua Anonymous, 1 FTP Site cung cấp riêng cho từng người dùng có thể lưu trữ và sử dụng tài nguyên thông qua dịch vụ FTP.
3. Dùng MS Frontpage XP để tạo một Web page cho cơ quan (dùng bộ template có sẵn trong Frontpage), sau đó publish nội dung này lênh Web Server để cho phép người dùng có thể truy xuất Web, Trên Web Site phải cung cấp forum cho người dùng có thể thảo luận.
4. Cài đặt và tổ chức hệ thống Mail nội bộ (dùng **Exchange** hoặc Mdaemon) để cung cấp E-mail cho người dùng. Người dùng có thể sử dụng mail thông qua POP, IMAP, OWA, OMA.
5. Cài đặt và tổ chức hệ thống Firewall cho mạng nội bộ để bảo mật hệ thống và cung cấp dịch vụ Proxy cho phép chia sẻ kết nối Internet cho mạng nội bộ.
6. Publish các server trong vùng DMZ để cho phép người dùng bên ngoài có truy xuất vào các dịch vụ được cung cấp trong mạng nội bộ.

Phần Hướng Dẫn Giải

Bài 01
Dịch Vụ DNS

Bài tập 01.1



1. **Bài 1:**

Cài đặt dịch vụ DNS trên máy chủ dns1

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (Chương 1 – phần VII.1 – trang 20).

2. **Bài 2:**

Cấu hình dns1 là một Primary Name Server cho domain name của mình với những dữ liệu đã cho. Có 2 cách cấu hình

Cấu hình DNS khi cấu hình AD (tích hợp DNS với AD)

Cấu hình DNS riêng

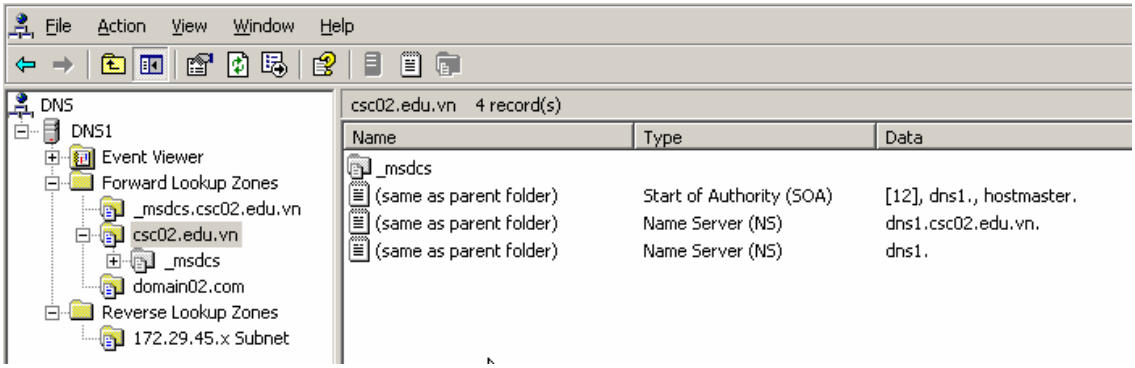
a. Cài đặt DNS

Do ở câu 7 của bài tập này có sử dụng DDNS nên trong phần hướng dẫn sẽ thực hiện theo cách tích hợp với AD. Bạn chỉ cần cài đặt AD trên máy dns1, với tên miền là "csc02.edu.vn", trong quá trình cài đặt, chọn máy tính tự động cài đặt DNS.

Chú ý:

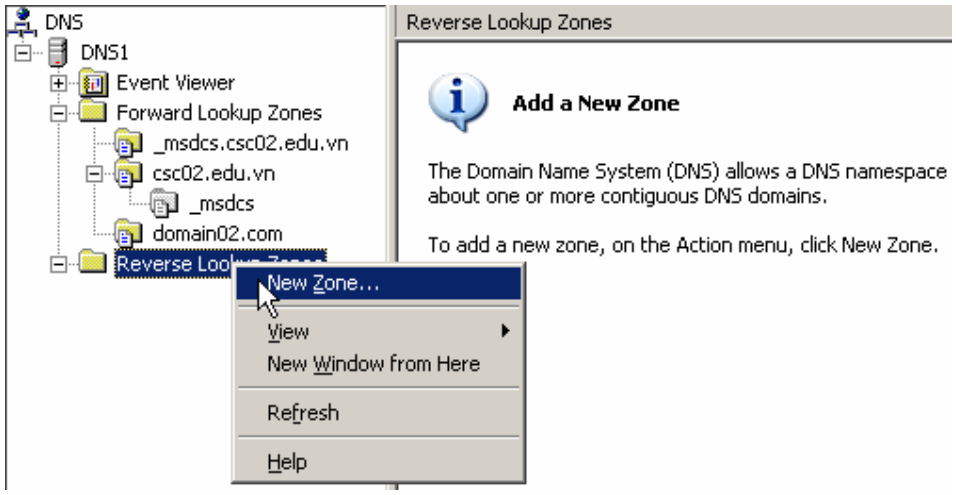
Nên đặt Preferred DNS Server là địa chỉ của máy dns1.

Giao diện DNS sau khi đã cài đặt xong:

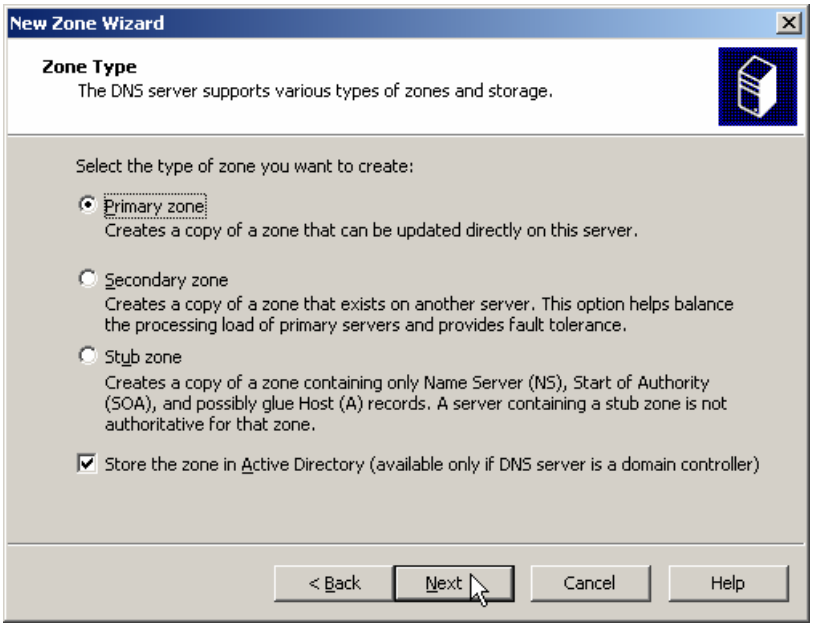


Sau khi cài đặt xong, bạn cần kiểm tra xem mình đã có Reverse Lookup Zones chưa, nếu chưa có thì bạn có thể cài đặt theo các bước sau:

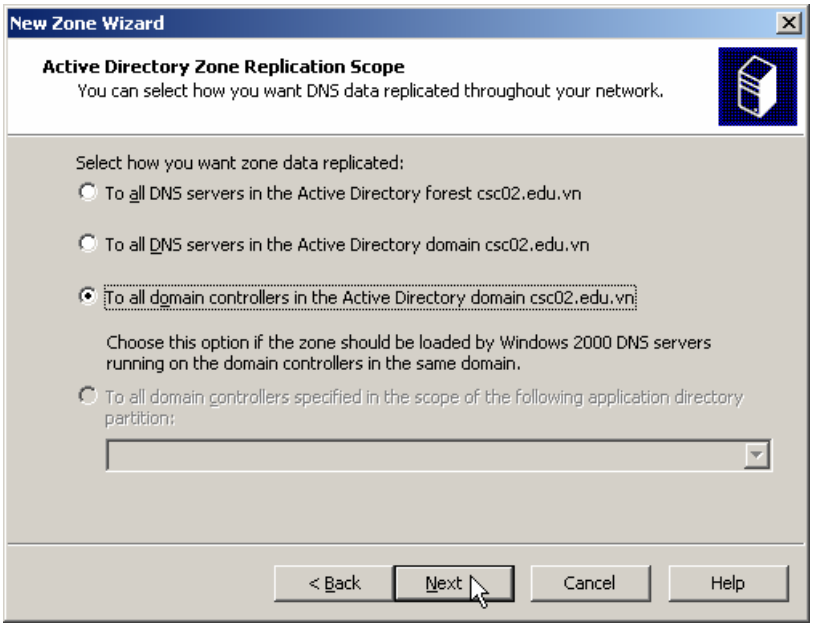
Bước 1: kích chuột phải vào Reverse Lookup Zones, chọn New Zone



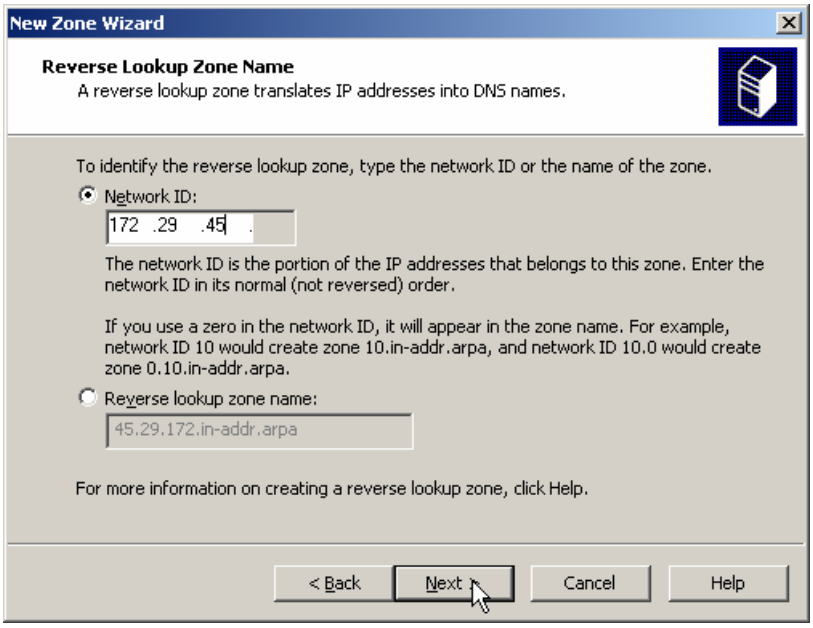
Bước 2: hộp thoại "Welcome to the New Zone Wizard", chọn Next để tiếp tục. Hộp thoại Zone Type hiện ra, bạn chọn kiểu Primary zone, sau đó chọn Next để tiếp tục



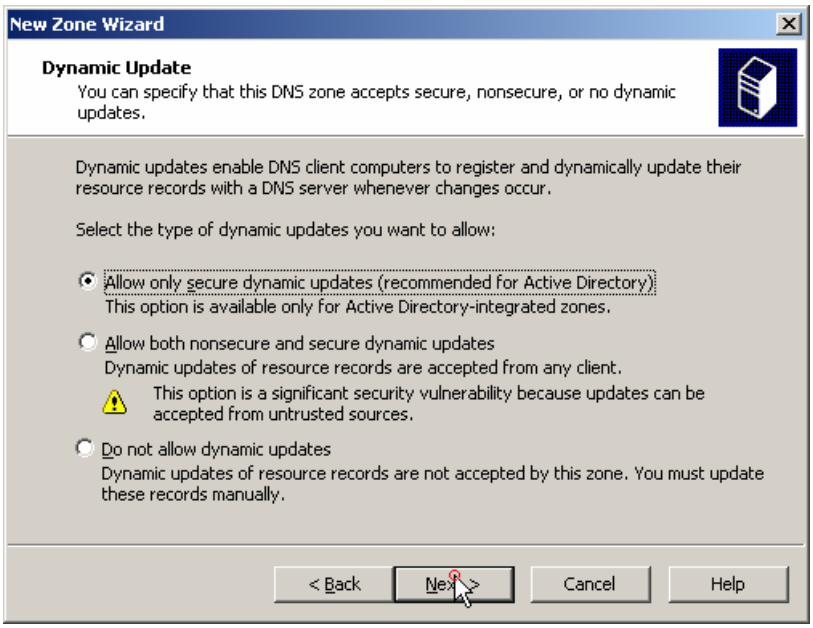
Bước 3: trong hộp thoại "Active Directory Zone Replication Scope". Bạn chọn "To all domain controllers in the Active Directory domain csc02.edu.vn" (bản sao sẽ được chuyển đến các máy Domain Controller trong AD).



Bước 4: trong hộp thoại "Reverse Lookup Zone Name", tại mục "Network ID" bạn chọn đường mạng là 172.29.45.* (bạn đang thực hiện phân giải từ địa chỉ IP của các máy trong đường mạng 172.29.45.0/24 sang tên máy).



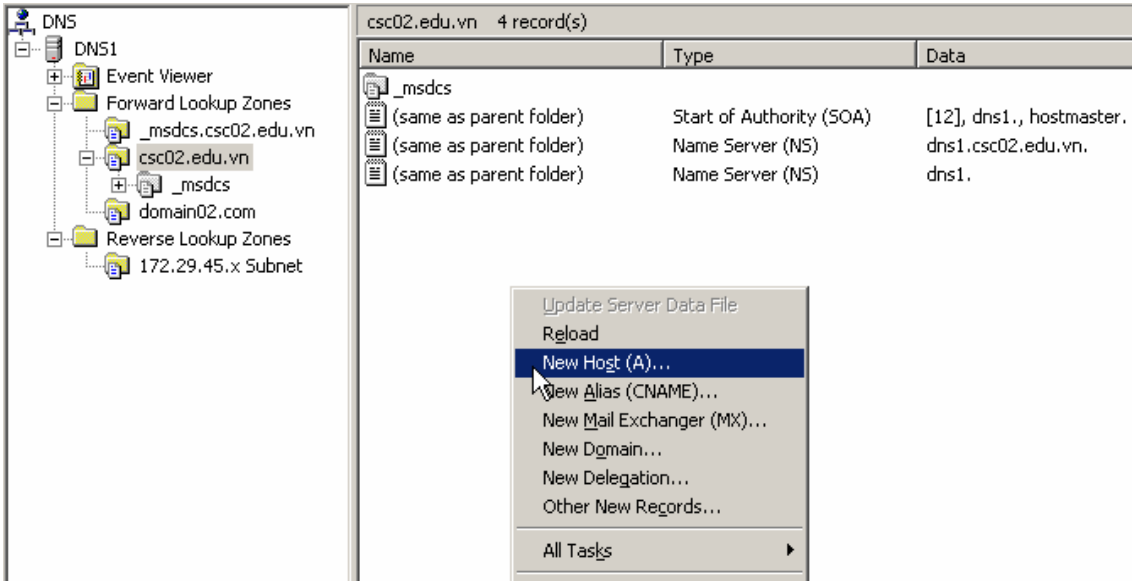
Bước 5: bạn chọn kiểu Dynamic update phù hợp với yêu cầu. Trong trường hợp muốn bảo mật thì chọn "Allow only secure dynamic updates"



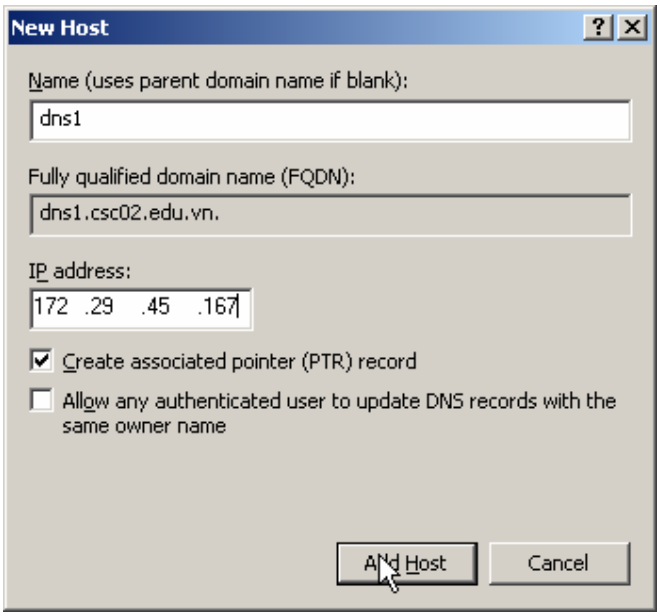
Bước 6: đến đây bạn đã kết thúc việc thiết lập Reverse Lookup Zones.

b. Cài đặt thông tin

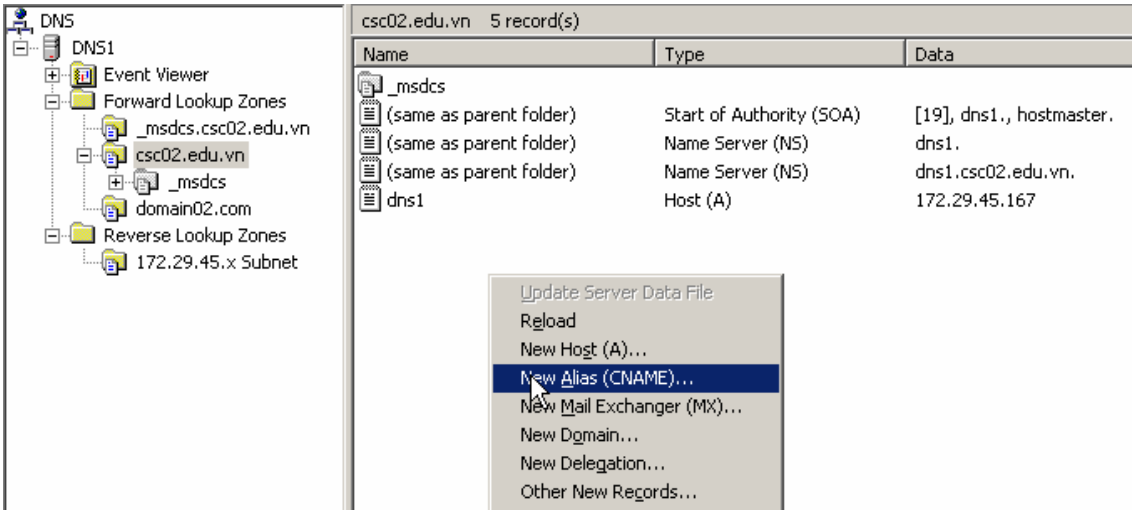
Bước 1: trước tiên, tạo một Resoure Record A, bạn kích chuột phải và chọn New Host (A)



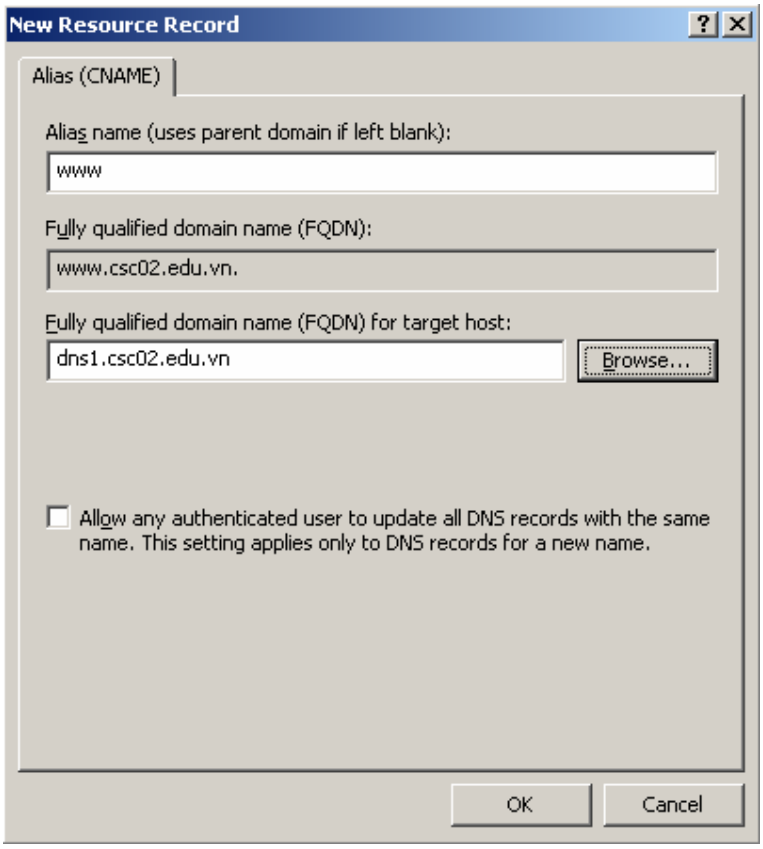
Bước 2: trong mục Name, bạn nhập tên của Host, trong mục IP Address, bạn điền địa chỉ IP của Host. Nếu muốn tạo luôn PTR record thì bạn chọn vào mục "**Create associated pointer (PRT) record**". Sau khi điền đầy đủ thông tin thì bạn chọn vào nút **Add Host** để tạo một Host mới.



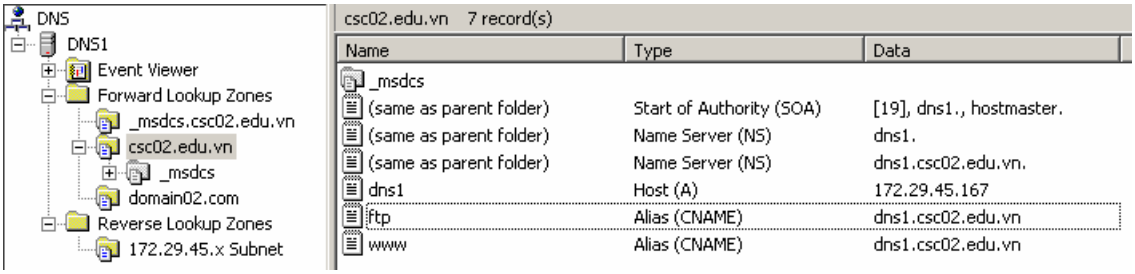
Bước 3: sau đó, tạo 2 Alias (ftp và www): chọn Forward Lookup Zones, csc02.edu.vn. Kích chuột phải và chọn New Alias (CNAME) (như hình sau):



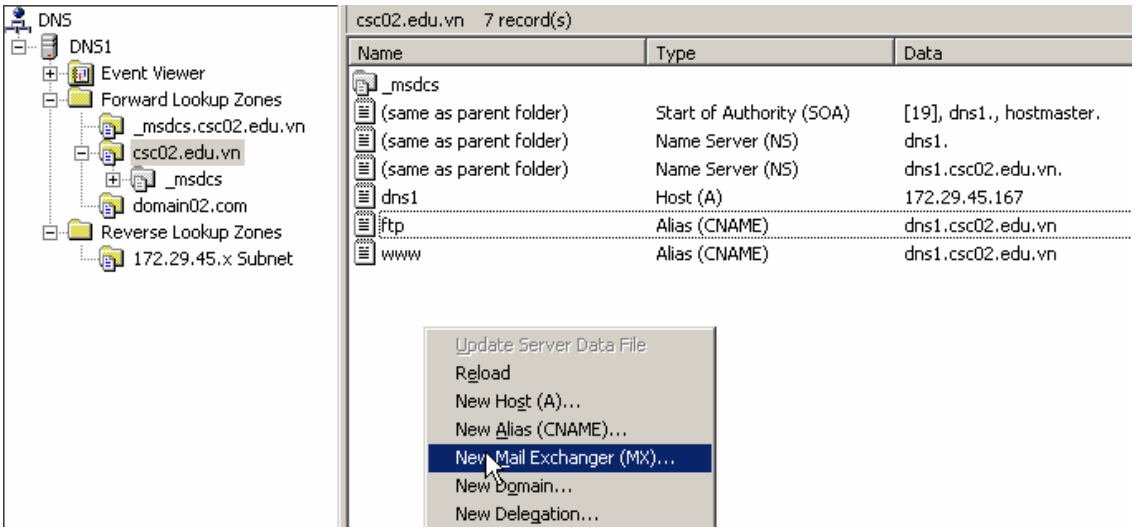
Bước 4: trong mục Alias name, bạn điền tên Alias mà bạn muốn tạo, trong mục FQDN thì bạn chọn Host tương ứng với tên đó.



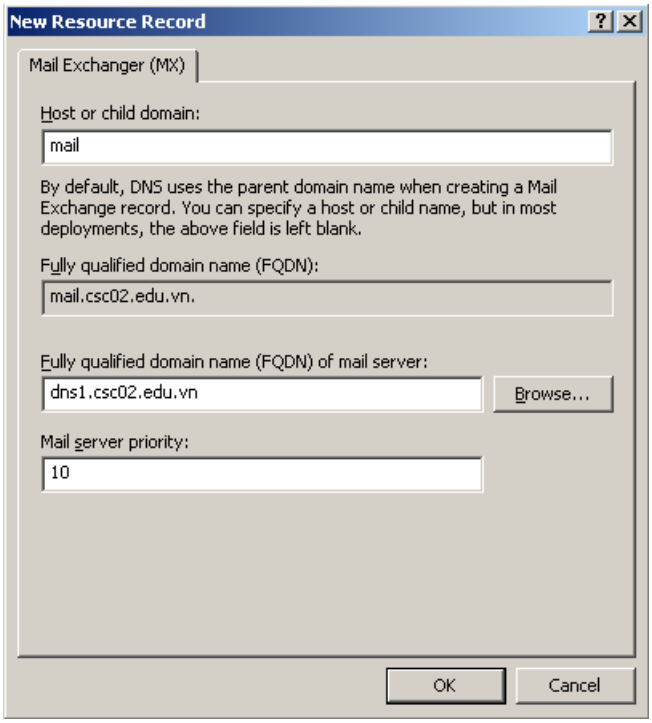
Bước 5: thực hiện tương tự đối với ftp, bạn sẽ có bảng sau:



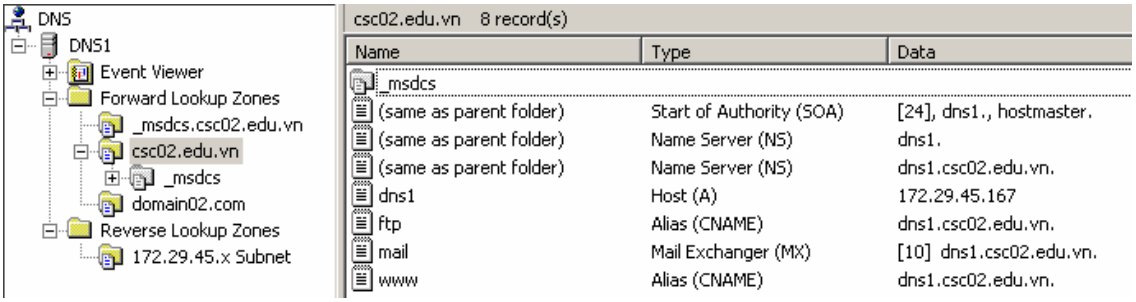
Bước 6: tạo một MX Record (dùng cho mail), bạn kích chuột phải vào chọn vào mục New Mail Exchange (MX)…



Bước 7: điền các thông số sau

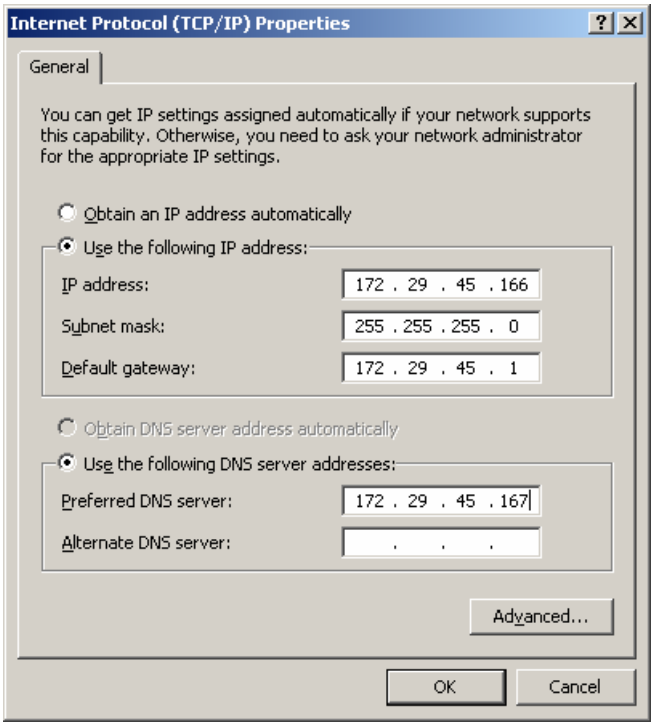


Bước 8: kết quả sau khi bạn tạo ra sẽ như sau:



3. Bài 3: sử dụng DNS Client để kiểm tra lại quá trình phân giải

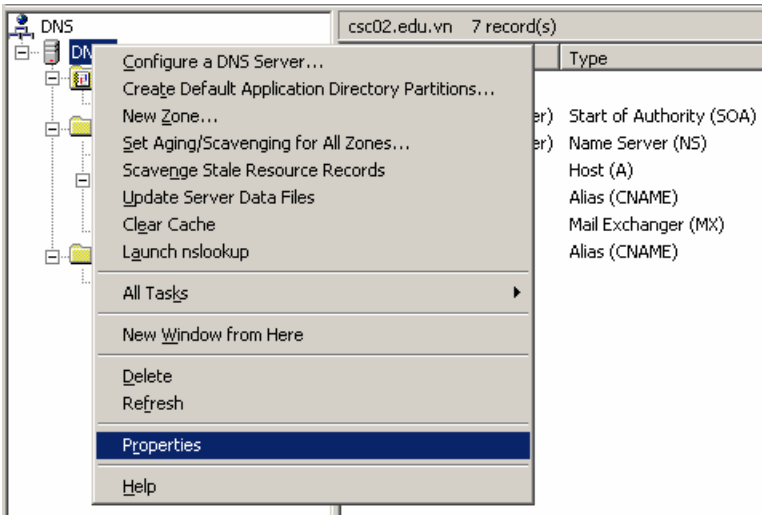
Tại máy Client, bạn cần khai báo DNS Server là máy dns1 (trong minh họa này là IP 172.29.45.167), bạn cần khai báo địa chỉ này trong mục “Preferred DNS server”



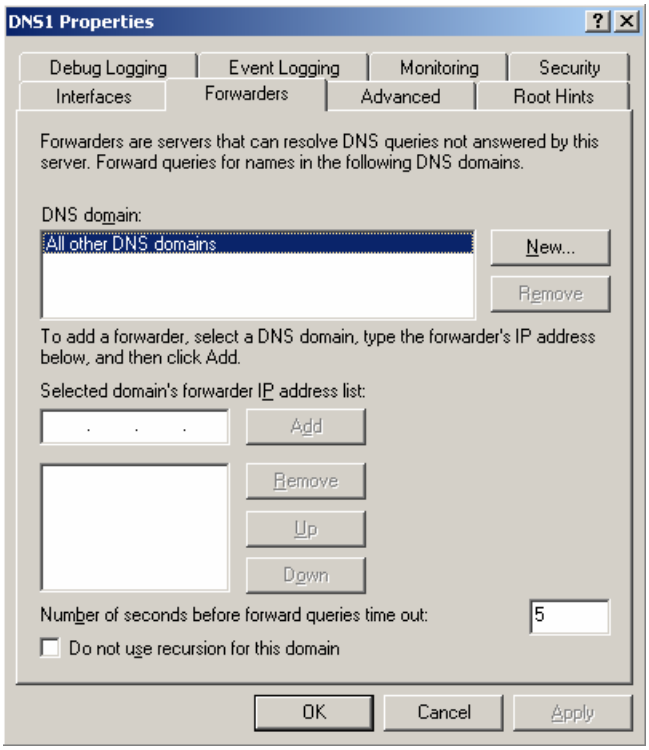
Sau đó, tại máy Client mở chương trình Command Prompt lên, chạy nslookup để kiểm tra.

4. Bài 4: cấu hình forwarders lên server 203.162.4.1

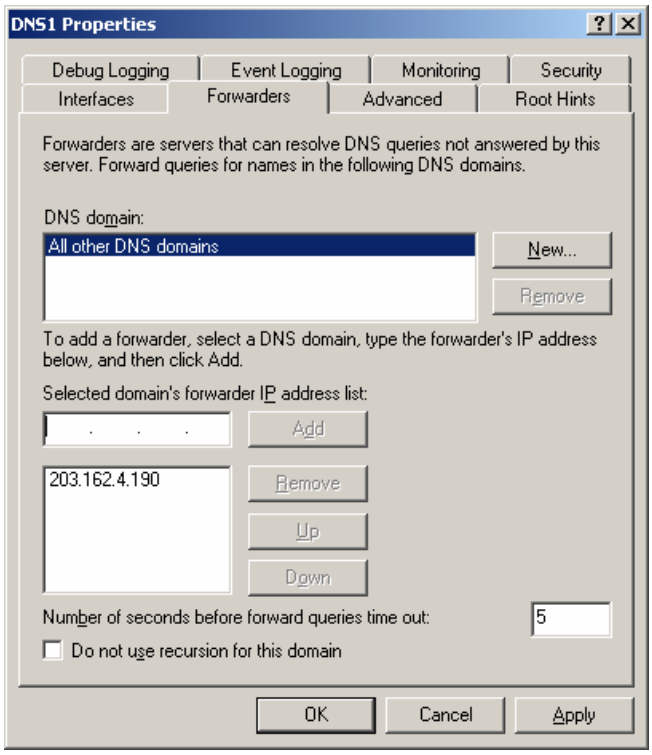
Bước 1: kích chuột phải vào tên máy (dns1), chọn Properties



Bước 2: chọn Tab Forwarders

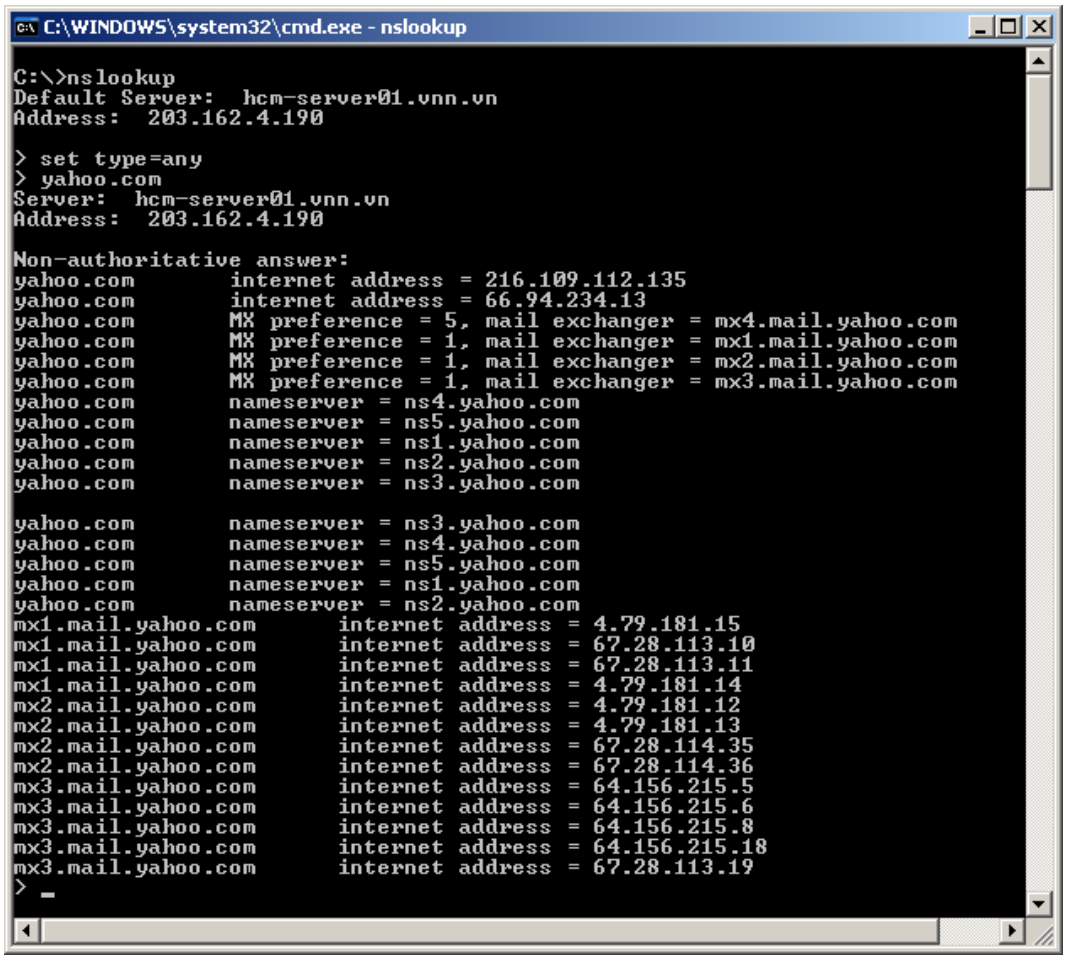


Bước 3: điền địa chỉ IP vào trong mục "**Selected domain's forwarder IP address list**", sau đó chọn Add, (trong hình sau bạn sẽ thấy add vào địa chỉ 203.162.4.190):

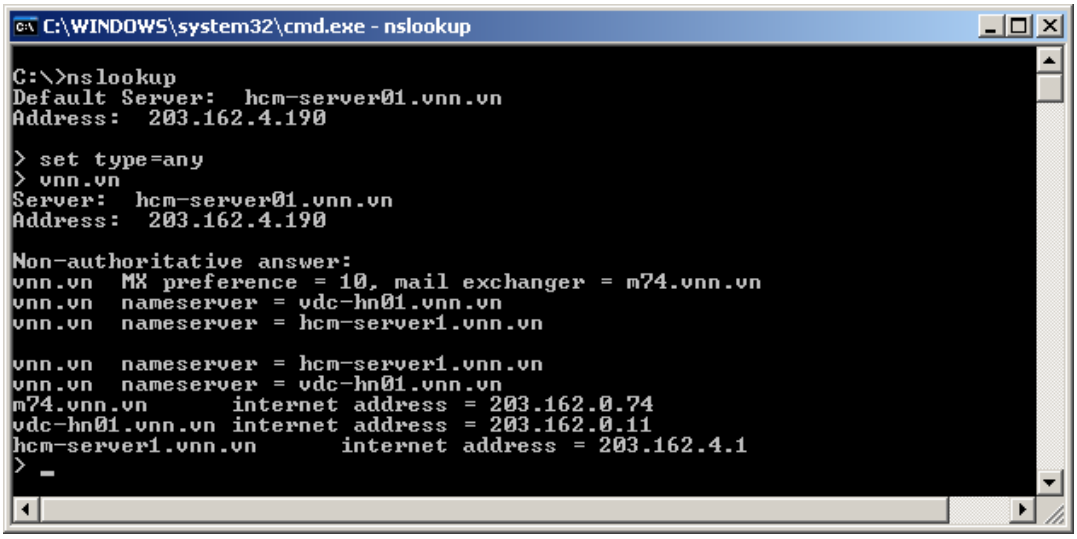


5. Bài 5: dùng tiện ích nslookup để phân giải các tên miền quốc tế

Phân giải tên miền yahoo.com



Phân giải địa chỉ vnn.vn

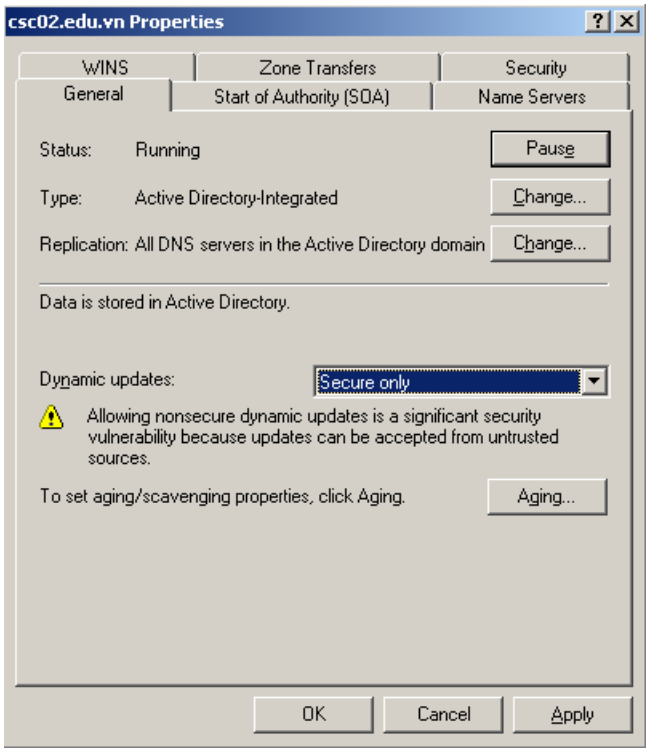


6. Bài 6: dùng máy tính bên cạnh làm secondary name server

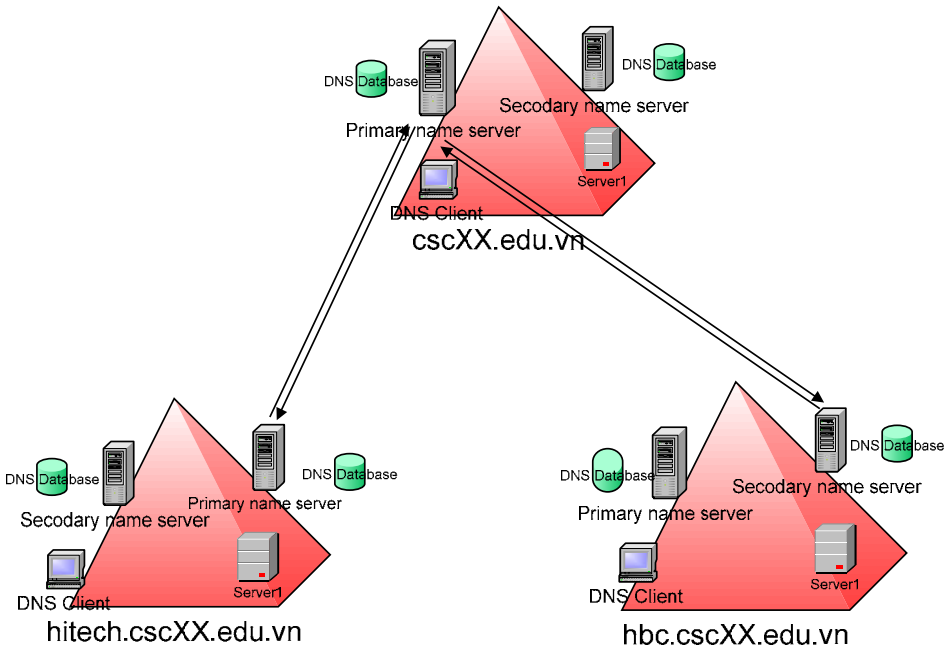
Tham khảo giáo trình “Dịch vụ mạng Windows 2003” (chương 1 – phần VII.2.7 – trang 34)

7. **Bài 7: cấu hình DDNS cho phép máy trạm khi đăng nhập mạng có thể đăng ký RR trực tiếp vào DDNS Server hoặc đăng ký RR thông qua DHCP Server.**

Tham khảo giáo trình “Dịch vụ mạng Windows 2003” (chương 1 – phần VII.2.9 – mục 2 – trang 43)



Bài tập 01.2



- ***Miền csc02.edu.vn***

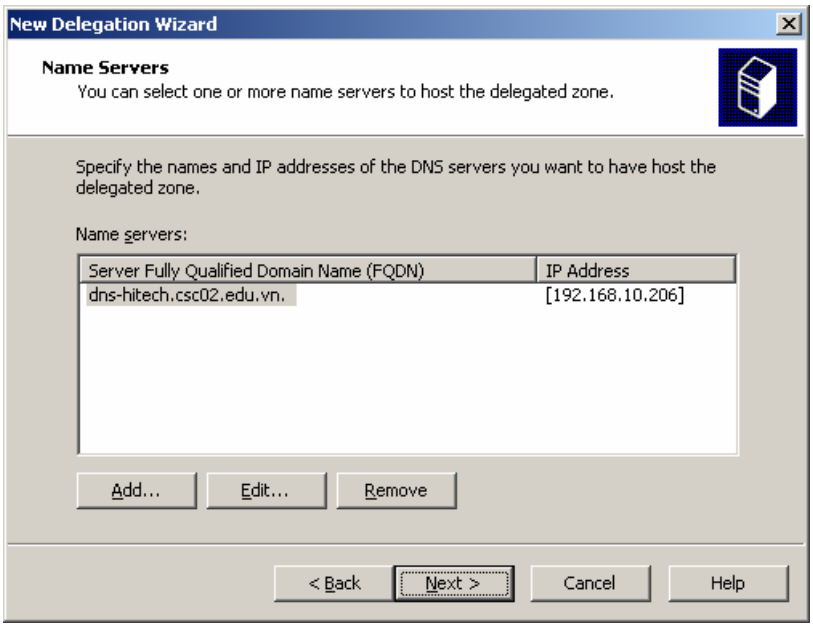
1. Bài 1: trên máy dns1

Trên máy dns1 tạo 2 zone mới (hitech và hbc), sau đó uỷ quyền cho cả 2 máy này. Minh họa thực hiện cho hitech (Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 1 – phần VII.2.5 – trang 32))

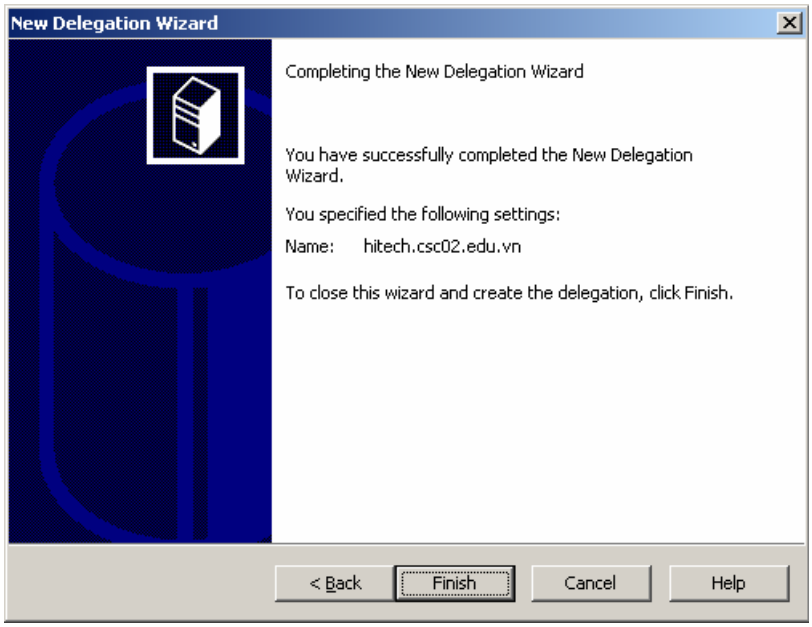
Chú ý:

máy dns-hitech này phải được khai báo trong DNS Server (máy dns1) quản lý miền csc02.edu.vn. Nếu không thì máy dns1 không thể biết được chính xác vị trí của máy quản lý miền con hitech.csc02.edu.vn

Bước 1: sau khi đã chọn máy dns-hitech, bạn chọn ok thì kết quả sẽ như sau:



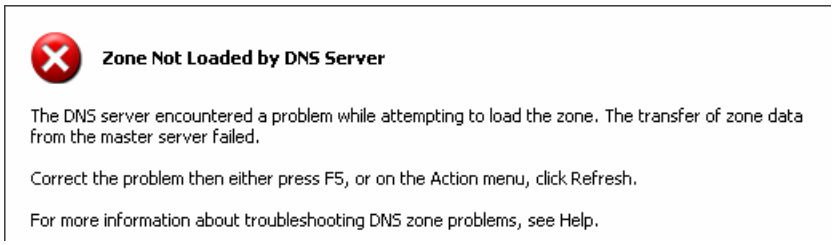
Bước 2: chọn Next để tiếp tục, bạn sẽ gặp hộp thoại kết thúc việc ủy quyền. Bạn chỉ cần chọn Finish để kết thúc việc thiết lập.



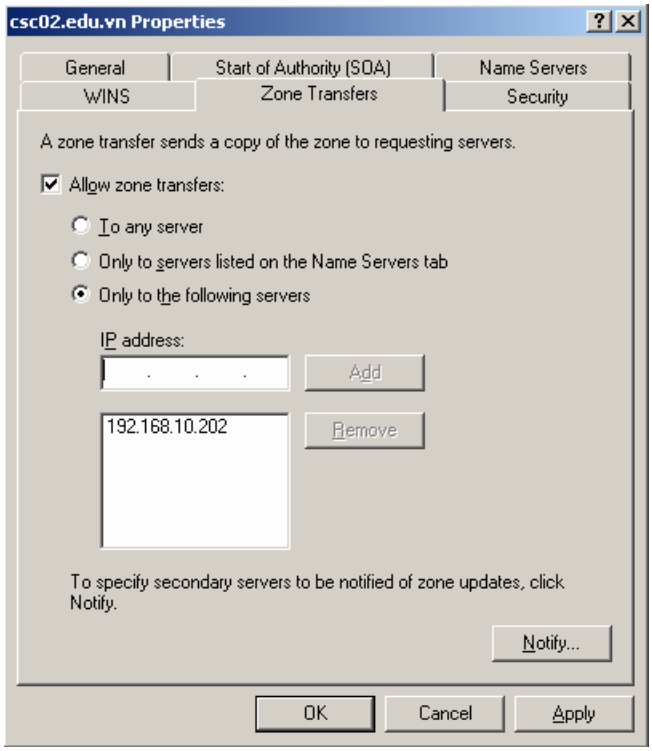
2. **Bài 2: cấu hình sdns là Secondary name server cho miền csc02.edu.vn, hbc.csc02.edu.vn, hitech.csc02.edu.vn**

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 1 – phần VII.2.7 – trang 34)

Chú ý: Nếu gặp thông báo lỗi sau:



Thì bạn cần kiểm tra trong Primary DNS, kích chuột phải vào zone, chọn Properties, sau đó chọn Tab Zone transfers (như hình sau), và nhập địa chỉ IP của Secondary name Server vào



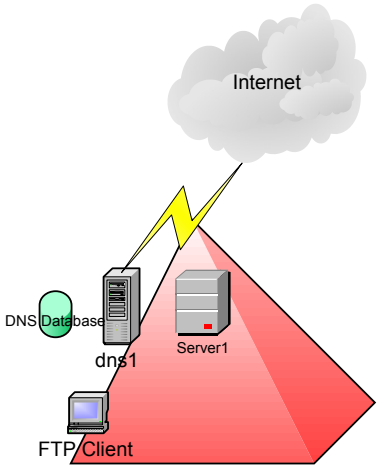
- ***Miền con hitech.csc02.edu.vn.***

1. **Bài 1: thực hiện tương tự bài tập 01.1**

Bài 02
Dịch Vụ FTP

Bài tập 02.1

Mô hình kết nối mạng của Trung Tâm Tin Học có tên miền cscXX.edu.vn như sau (trong đó XX là số thứ tự của máy tính đang ngồi)



cscXX.edu.vn

Tên máy	Địa chỉ IP	Hệ điều hành sử dụng	Chức năng
Dns1	192.168.100.200+XX/24	Windows 2003 Server	Primary name server.
server1	192.168.100.200+XX/24	Windows 2003 Server	FTP Server.

1. **Bài 1:**

Tham khảo bài tập 01.1

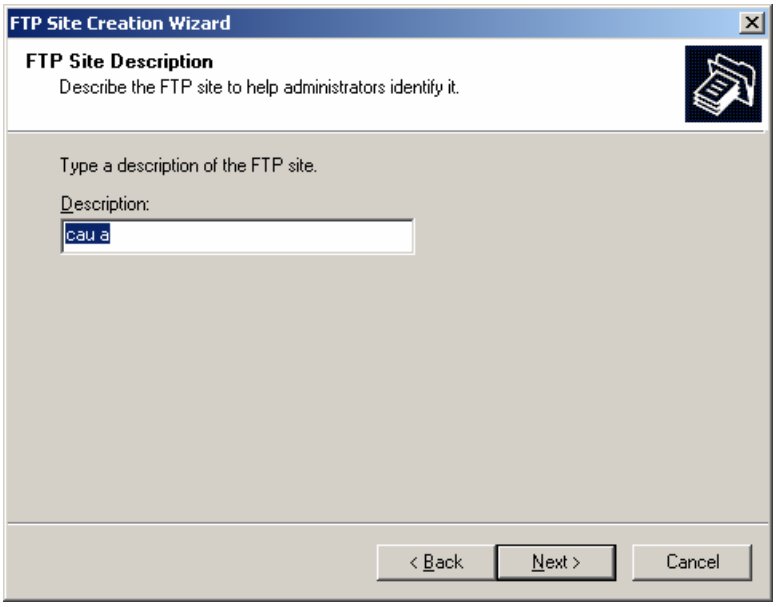
2. **Bài 2:**

Cài đặt FTP Service trên máy chủ Server1, sau đó thực hiện các yêu cầu sau (Để vào FTP Service, chọn **Administrator Tool**, chọn **Internet Information Services Manager**):

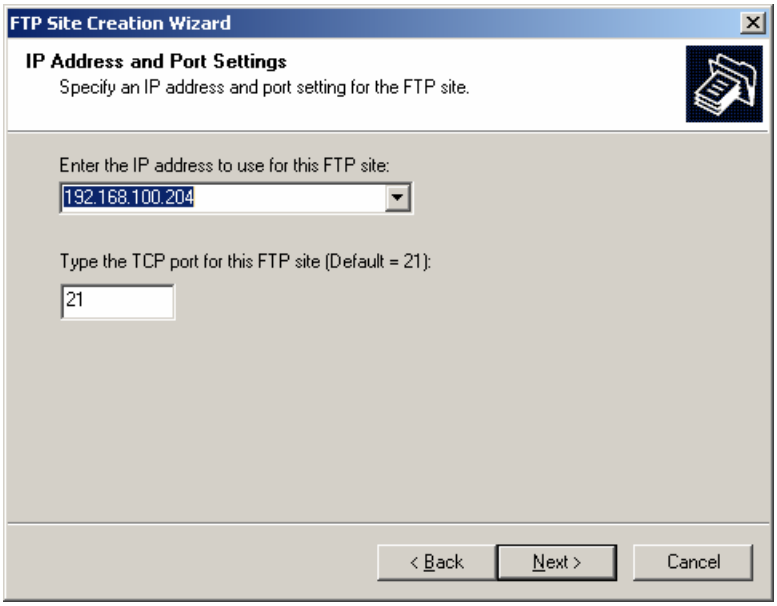
a. Tạo một Public FTP site (sử dụng chế độ **"do not isolation user"**) với FTP home directory C:\inetpub\ftproot.

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 2 – phần III.2.1 – trang 56)

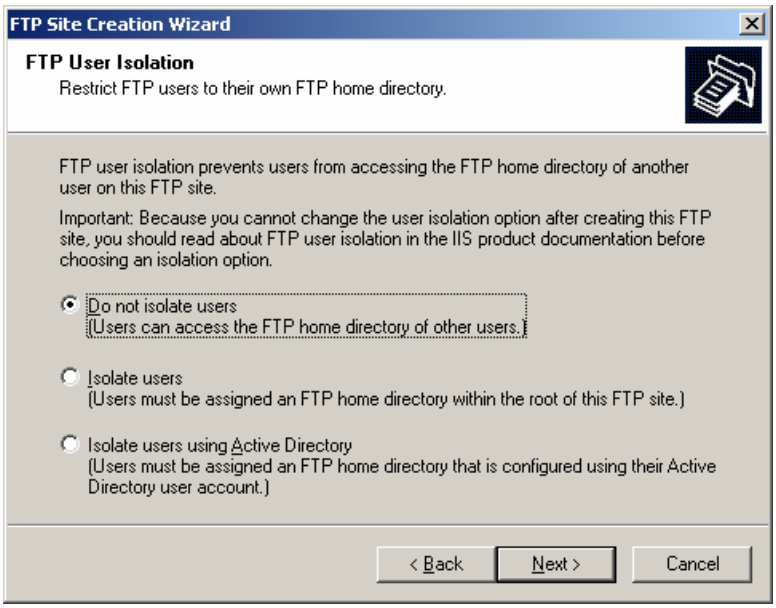
Bước 1: bạn vào IIS Manager, kích chuột phải vào thư mục FTP Sites, chọn New, FTP Site, bạn sẽ thấy hộp thoại "Welcome to the FTP Site Creation Wizard". Chọn Next để tiếp tục. Hộp thoại "FTP Site Description" sẽ hiện ra. Ở mục Description, bạn sẽ nhập tên "diễn giải" cho FTP Site. Ví dụ là "cau a", sau đó chọn Next



Bước 2: trong hộp thoại "IP Address and Port Settings", bạn cần cho hệ thống biết bạn sẽ sử dụng địa chỉ IP và Port bao nhiêu để làm FTP Server. Trong hình minh họa bên dưới thể hiện hệ thống sẽ sử dụng địa chỉ 192.168.100.204, Port 21 làm FTP Server. Sau khi nhập xong thông tin, bạn chọn Next để tiếp tục



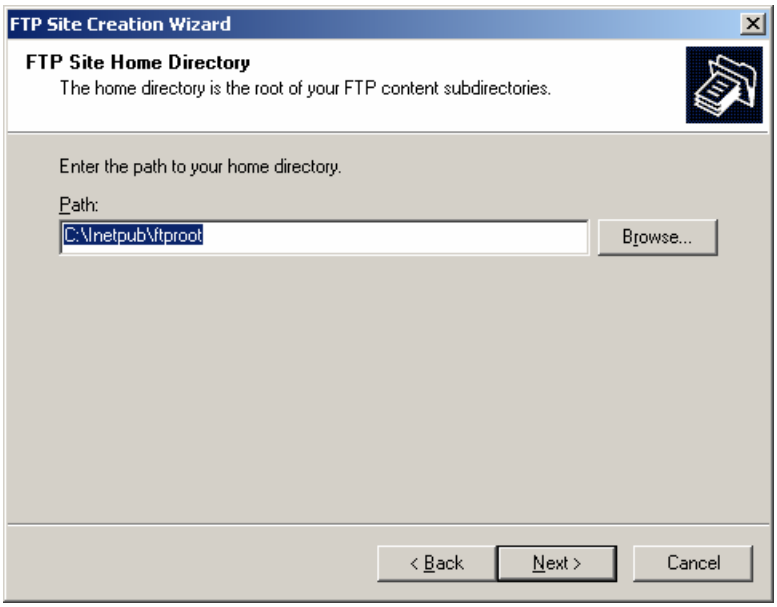
Bước 3: trong hộp thoại "FTP User Isolation", bạn chọn kiểu "Do not isolate Users". Sau đó, chọn Next để tiếp tục



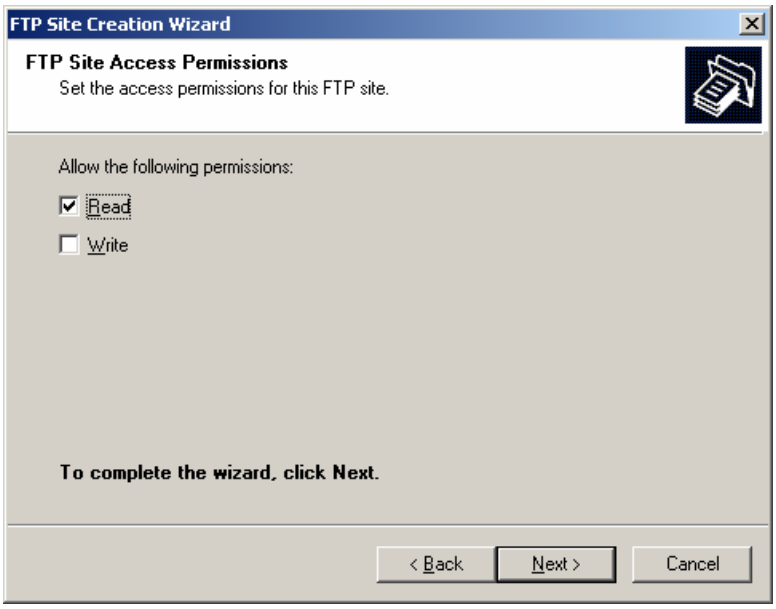
Chú ý:

Bạn có thể xem thêm về các mode ở trang 57 trong giáo trình Dịch vụ mạng Windows 2003.

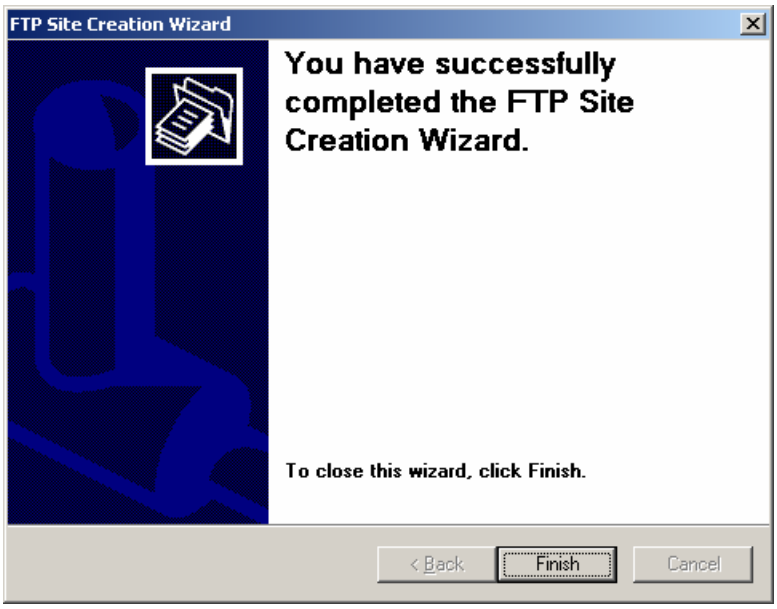
Bước 4: trong hộp thoại "FTP Sites Home Directory", bạn chọn đường dẫn để làm thư mục gốc cho FTP Server. Sau đó chọn Next để tiếp tục



Bước 5: trong hộp thoại "FTP Site Access Permissions", bạn chọn quyền của các user khi truy cập vào FTP Site. Trong hình minh họa ở dưới, user chỉ có quyền Read. Chọn Next để tiếp tục

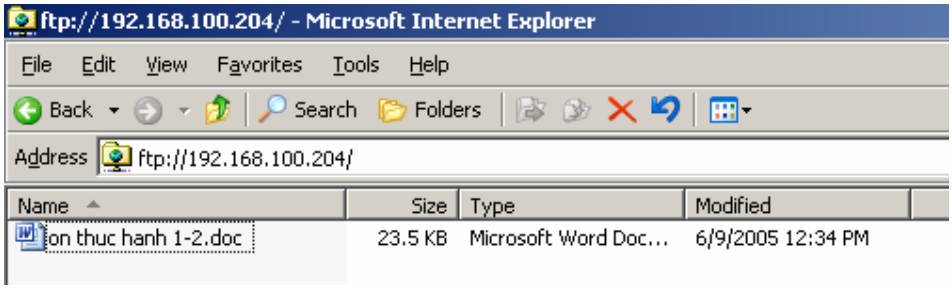


Bước 6: bạn chọn Finish để kết thúc quá trình cài đặt



Kiểm tra lại:

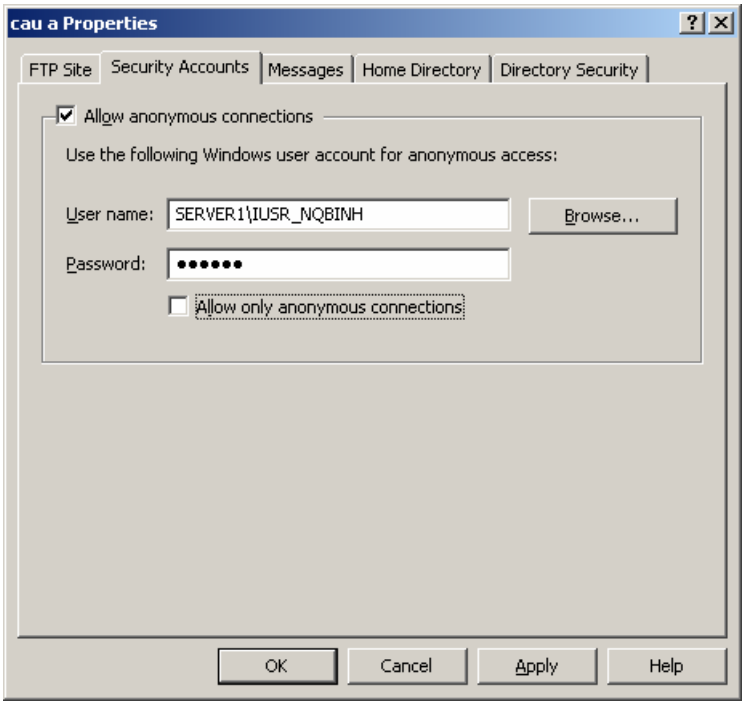
Ở máy Client, bạn sử dụng IE để truy cập FTP.



b. Dùng trình tiện ích computer management , tạo user "ftpuser". Cấu hình cho phép kết nối vô danh (anonymous connection) và bỏ tùy chọn "Alow only anonymous connection". Kiểm tra việc truy cập dùng user anonymous và user "ftpuser".

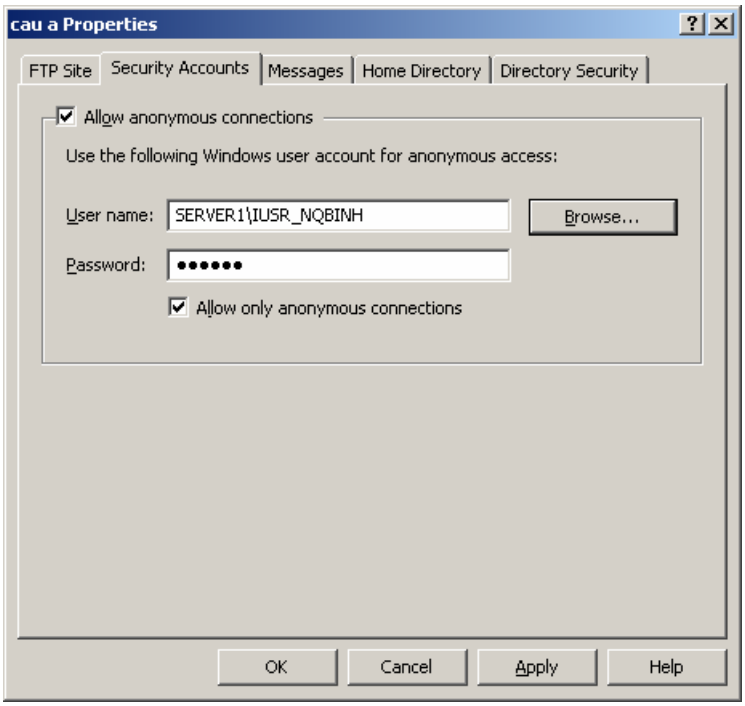
Tạo user ftpuser: tham khảo "giáo trình quản trị windows"

Kích chuột phải vào FTP Site (cau a), và chọn Properties, chọn Tab Security Accounts và bạn cấu hình như hình sau:



Trong trường hợp này thì user ftpuser và anonymous đều truy cập được

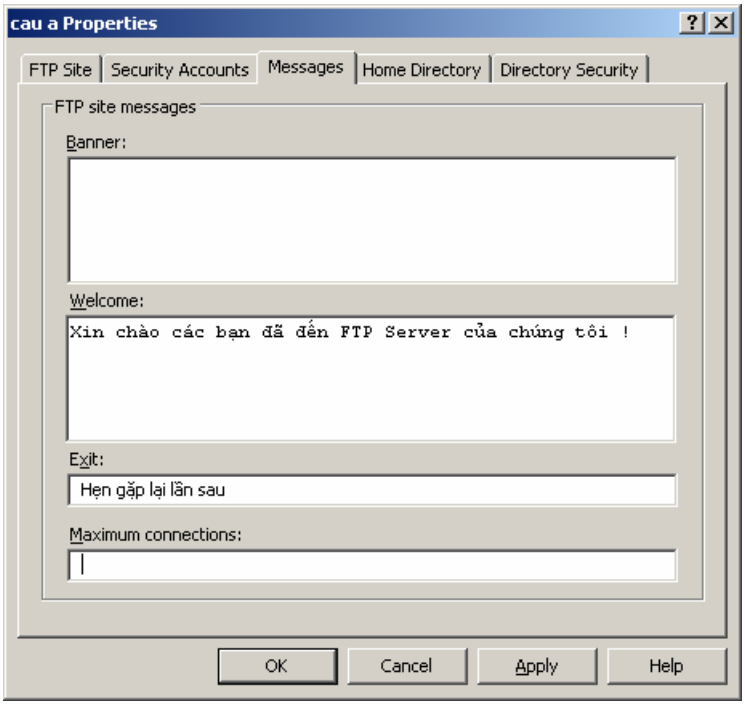
c. Chọn tuỳ chọn chỉ cho phép kết nối vô danh "Alow only anonymous connection", thử truy cập bằng user vô danh anonymous, và dùng ftpuser.



Trong trường hợp này thì chỉ có user anonymous có thể truy cập được

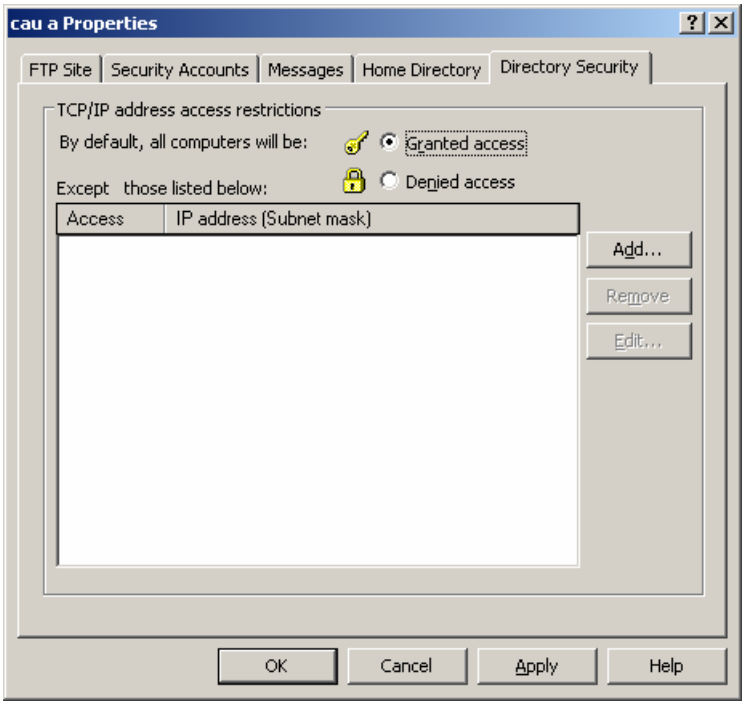
d. Tạo các thông điệp Welcome:" xin chào các bạn đã đến FTP server của chúng tôi " và thông điệp Exit: "Hẹn gặp lại lần sau" .

Thay vì chọn Tab Security, bạn chọn Tab Messages.

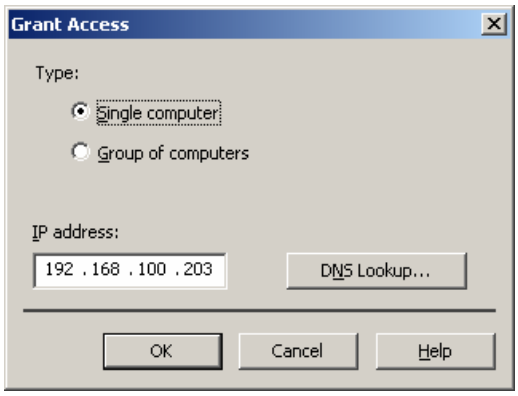


e. Cấm máy bên cạnh có địa chỉ IP 192.168.100.200+XX/24 truy cập vào FTP server của mình. Kiểm tra kết quả bằng cách truy cập từ máy bên cạnh.

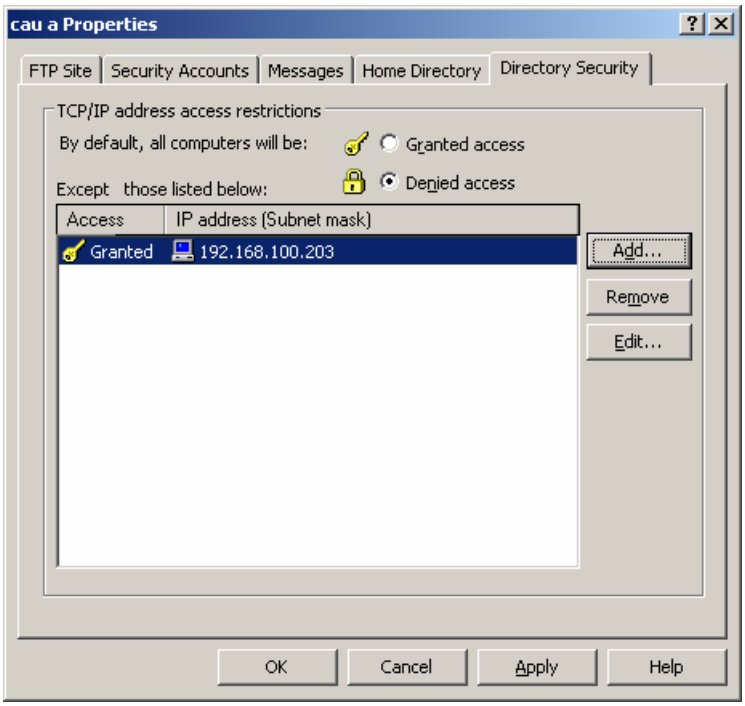
Bước 1: kích chuột phải vào FTP Site "cau a", chọn Properties, chọn Tab Directory Security



Bước 2: chọn mục "**Denied Access"**, sau đó chọn Add để thêm địa chỉ 192.168.100.203



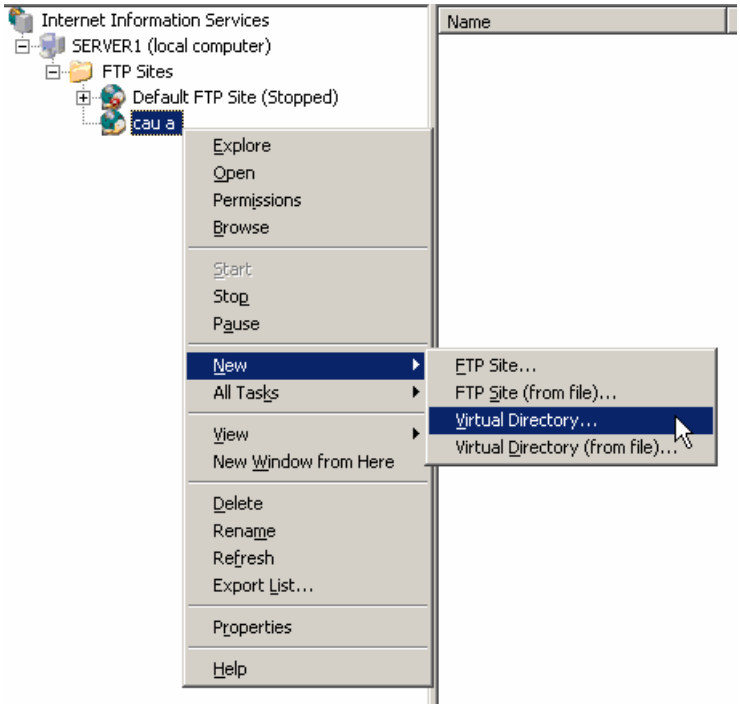
Bước 3: chọn Ok



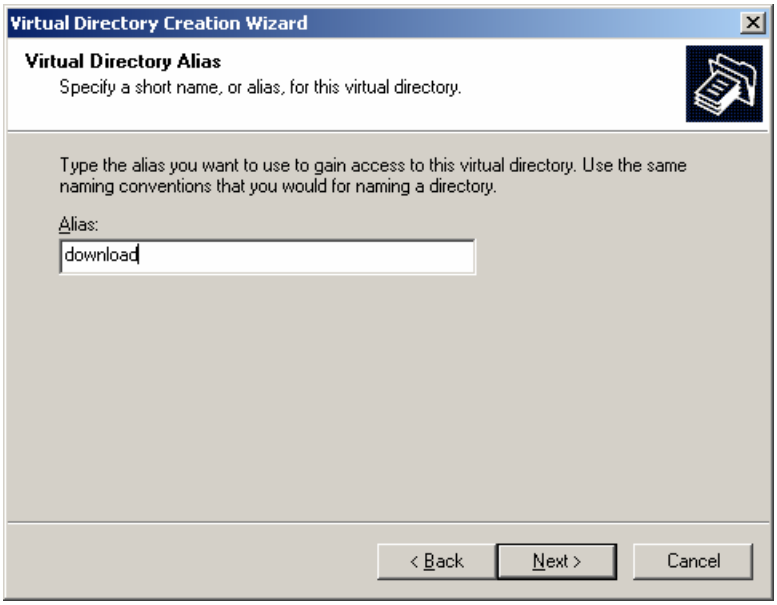
f. Tạo thư mục c:\SOFT, ánh xạ thành thư mục ảo trên FTP server với alias là "download", cho phép mọi người dùng bên ngoài truy xuất FTP Server qua anonymous user.

Với thiết lập như câu c, bạn chỉ cần tạo thêm một Virtual Directory

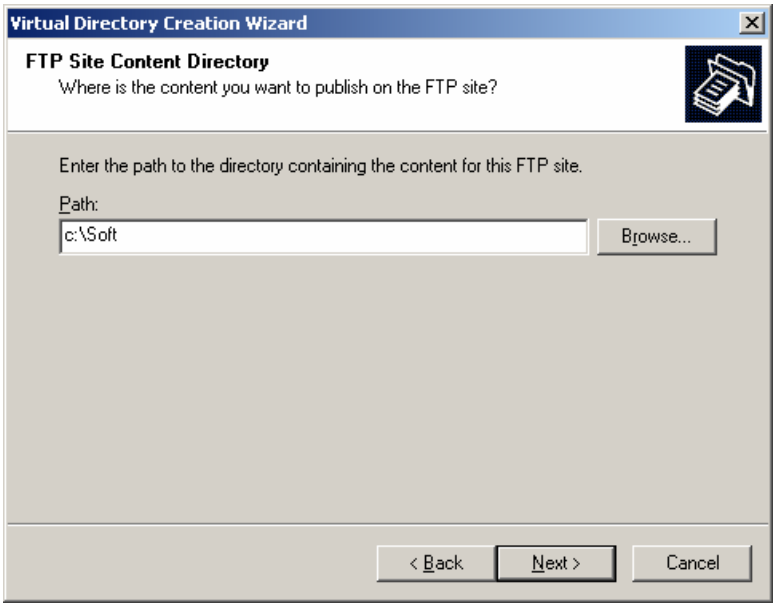
Bước 1: kích chuột phải lên FTP Site mới tạo ra, chọn New, Virtual Directory.



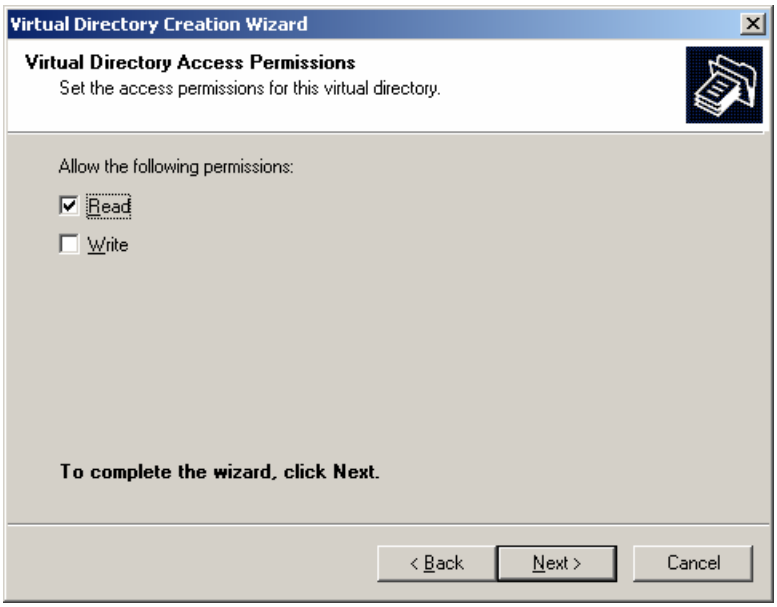
Bước 2: bảng Virtual Directory hiện ra, chọn Next để tiếp tục. Hộp thoại "Virtual Directory Alias" hiện ra, trong mục Alias, bạn điền tên thư mục "ảo". Ví dụ là download.



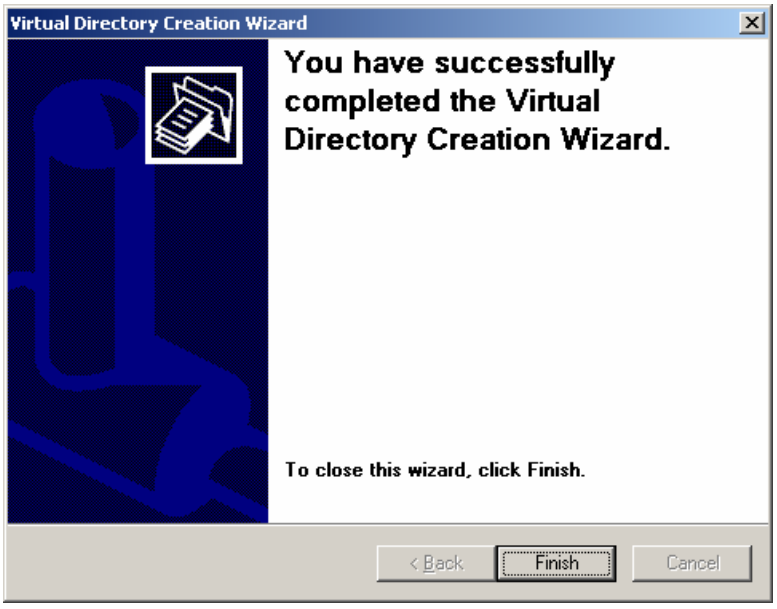
Bước 3: trong hộp thoại "FTP Site Content Directory", trong mục Path, bạn chọn đường dẫn thực sự trên máy tính. Ví dụ là thư mục "C:\Soft" Chọn Next



Bước 4: trong hộp thoại "Virtual Directory Access Permissions", bạn chọn quyền cho User khi truy cập vào thư mục này.

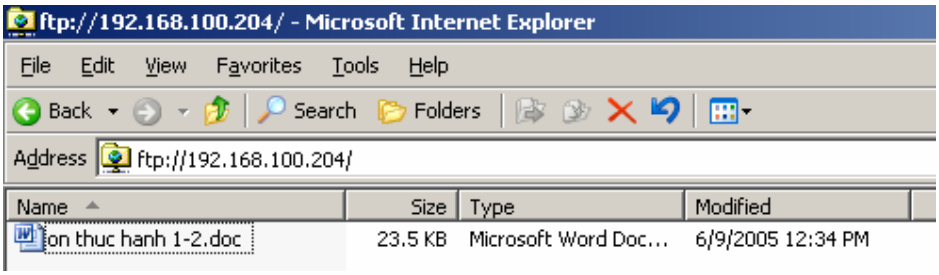


Bước 5: chọn Finish để kết thúc quá trình cài đặt Virtual Directory.

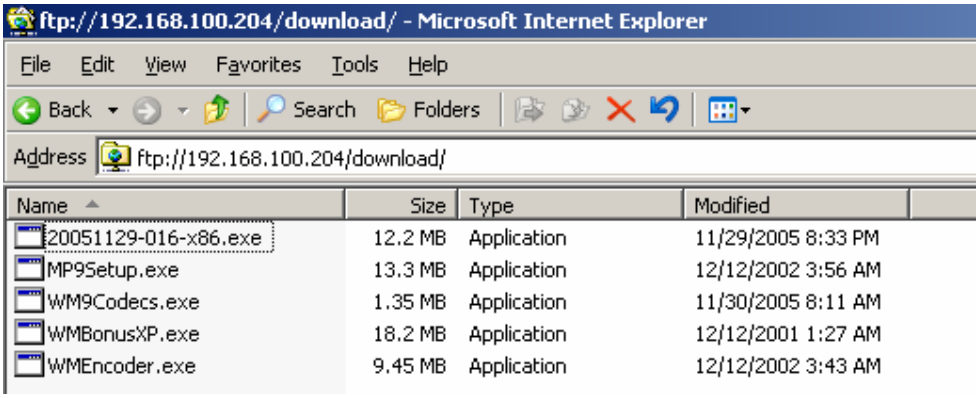


Kiểm tra lại:

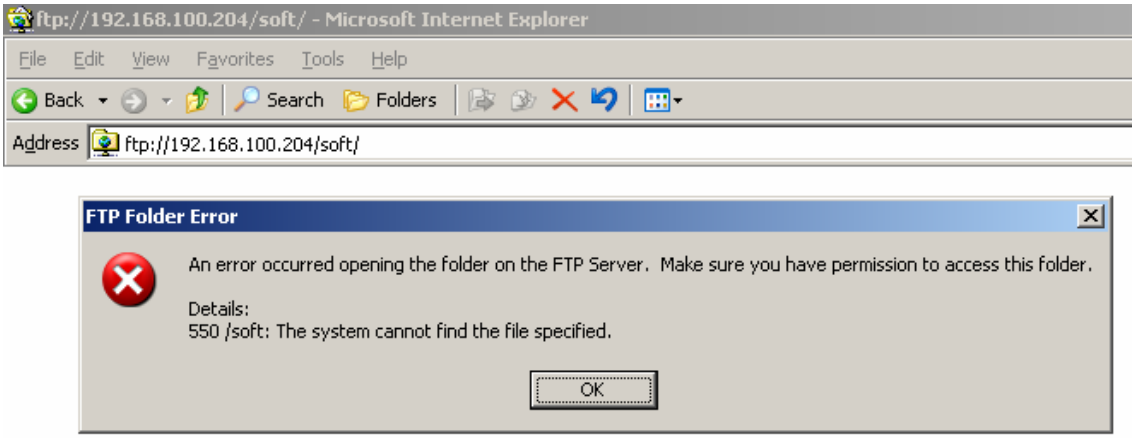
Ở máy Client, bạn sử dụng IE để truy cập vào Virtual Directory. Khi truy cập vào **ftp://192.168.100.204**, bạn thấy như sau:



Khi truy cập vào **ftp://192.168.100.204/download**, bạn thấy như sau:

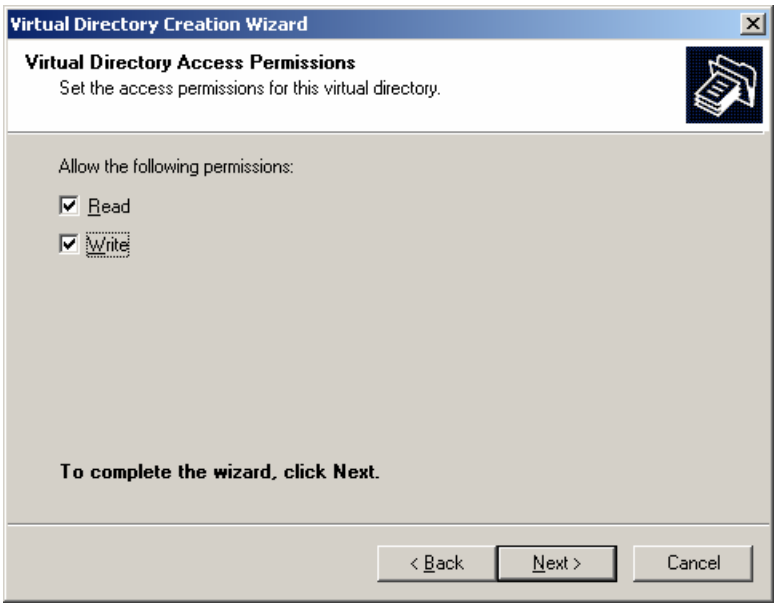


Khi truy cập vào **ftp://192.168.100.204/soft**, bạn thấy như sau:



g. Tạo thư mục c:\pub, ánh xạ thành thư mục ảo trên FTP server với alias là "upload", cho phép mọi người dùng có thể upload tài nguyên thông qua anonymous user.

Vẫn thực hiện giống như câu f, nhưng ở bước 4, bạn chọn lựa thêm quyền Write



Đồng thời, trong thư mục trên ổ cứng (tương ứng với Virtual Directory, cụ thể trong trường hợp này là c:\pub), bạn cần thiết lập quyền Security, cho phép Everyone có quyền Full (bạn tham khảo thêm trong giáo trình Quản trị mạng Windows 2003 về cách thiết lập quyền Security trên thư mục).

h. Dùng các tập lệnh của FTP client để, sau đó dùng lệnh get, mget, prompt, lcd…để thực hiện quá trình download một vài file từ thư mục download của FTP server về máy cục bộ.

Tham khảo mạng cơ bản

i. Dùng Winword tạo một file *.doc sau đó dùng lệnh put, mput, lcd,… để upload tập tin này lên thư mục upload của FTP Server.

Tham khảo mạng cơ bản

j. Sử dụng các phần mềm làm FTP Client như: IE, Windows Commander, cutftp để truy xuất vào FTP server.

Tham khảo mạng cơ bản

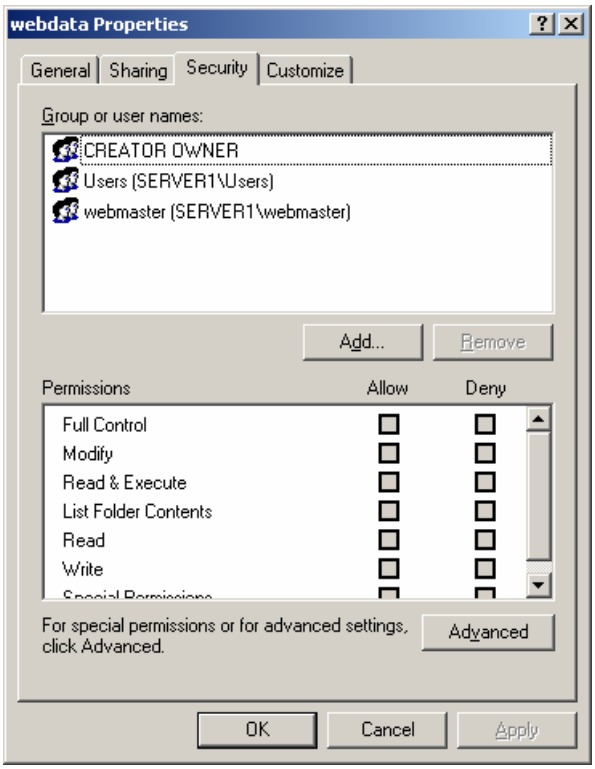
k. Tạo thư mục ảo /data trong FTP site trỏ đến D:\Webdata. Gán quyền sao cho nhóm Webmasters có quyền đọc ghi trong thư mục FTP, mọi user còn lại chỉ có quyền đọc. Thử lại bằng FTP client bằng user anonymous và user thuộc nhóm Webmasters (tạo một số user thuộc nhóm Webmasters trước khi kiểm tra).

Bạn thiết lập một Virtual Directory (có quyền Read và Write), nhưng quyền tại thư mục Webdata của ổ D: thì hơi khác biệt (tham khảo quản trị windows):

- Chỉ có nhóm Webmasters mới có quyền ghi

- Các user còn lại có quyền đọc

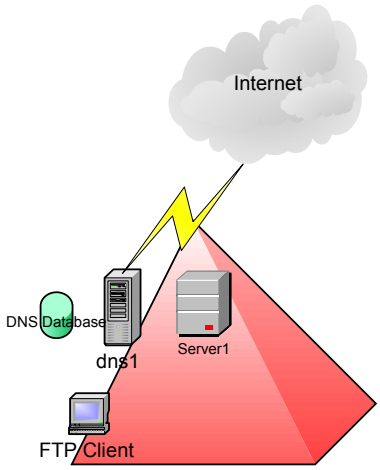
Tham khảo hình sau:



I. Kiểm tra xem kết nối giữa FTP Server và FTP Client theo cơ chế gì?

Sử dụng lệnh netstat -rn

Bài tập 02.2



cscXX.edu.vn

Tên máy	Địa chỉ IP	Hệ điều hành sử dụng	Chức năng
Dns1	192.168.100.200+XX/24	Windows 2003 Server	Primary name server.
server1	192.168.100.200+XX /24	Windows 2003 Server	FTP Server.

Mô hình kết nối mạng của Trung Tâm Tin Học có tên miền cscXX.edu.vn như sau (trong đó XX là số thứ tự của máy tính đang ngồi)

1. **Bài 1: trên Server1 tạo thêm địa chỉ IP: 172.16.XX.1**

Đặt thêm một địa chỉ cho card mạng (tham khảo mạng cơ bản)

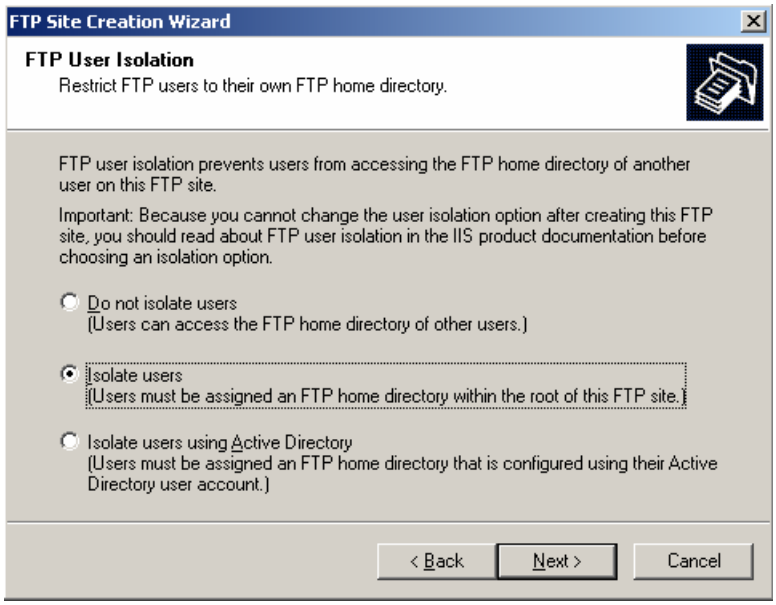
2. **Bài 2: cài đặt và cấu hình DNS trên dns1 là Primary name server của miền cscXX.edu.vn với:**
   - ftp.cscXX.edu.vn. Alias (CNAME) server1.cscXX.edu.vn.
   - vftp.cscXX.edu.vn Host (A) 172.16.XX.1

Tạo Resource Record A vftp.csc02.edu.vn và CNAME ftp.csc02.edu.vn

3. **Bài 3: cài đặt FTP Service trên máy chủ Server1, sau đó thực hiện các yêu cầu sau:**
   a. Tạo một Public FTP site có tên ftp.cscXX.edu.vn với FTP home directory C:\inetpub\ftproot. (sử dụng chế độ "do not isolation user").
   b. Tạo FTP Site mới có tên vftp.cscXX.edu.vn sử dụng chế độ "Isolation User"

- home directory: d:\ftpnet.
- FTP Permission : Read + Write.
- Tạo FTP home directory cho từng người dùng trong hệ thống, sau đó cấp quyền sao cho mỗi người dùng chỉ được phép truy xuất FTP home directory của mình.

Tạo FTP Site, chọn mode Isolate Users

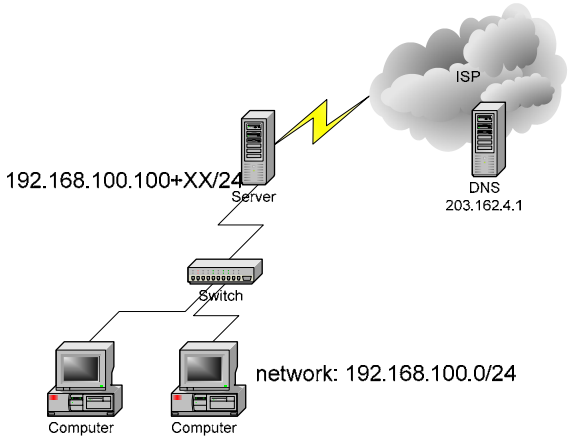


Tạo các home directory cho từng người dùng. Sau đó gán quyền Security cho từng người dùng.

4. Bài 4: dùng Windows Commander để kiểm tra.

Bài 03
Dịch Vụ Web

Bài tập 03.1



*Bạn là người quản trị cho một mạng máy tính của **công ty XX** kết nối lên Internet như hình vẽ. Máy chủ cài Win2k3 server và máy làm phục vụ dịch vụ DNS, Mail, Web, FTP cho công ty. Công ty thuê một tên miền "**ctyXX.com.vn**".*

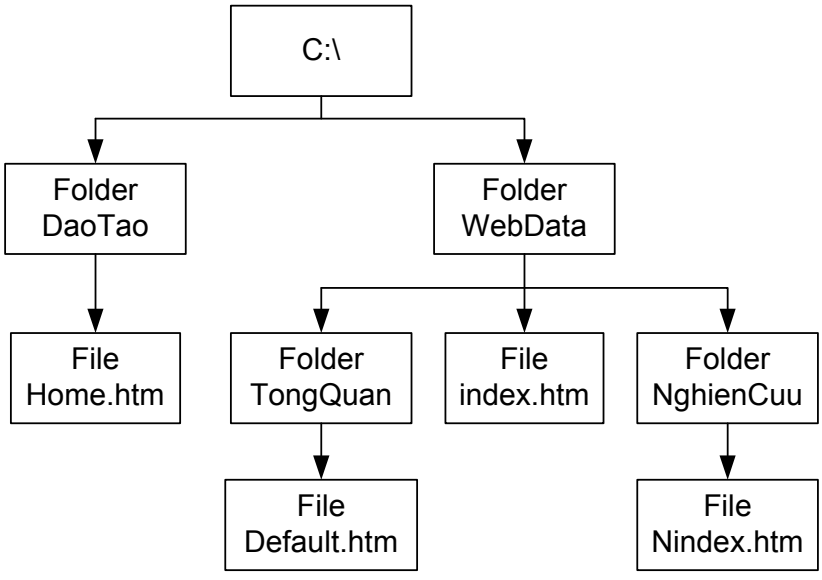
1. **Bài 1: tổ chức Web server.**
   a. Cài đặt IIS, DNS

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 3 – phần IV.1 - trang 82).

Sau đó, cài đặt Alias www đến WebServer

b. Tổ chức Web Site

Bạn tạo cấu trúc thư mục trên ổ cứng như sau:



Sau đó sử dụng FrontPage để tạo các trang Web như yêu cầu

2. Bài 2: cấp quyền truy xuất cho Website cho người dùng

a. Truy xuất theo địa chỉ

Tổ chức phân giải www

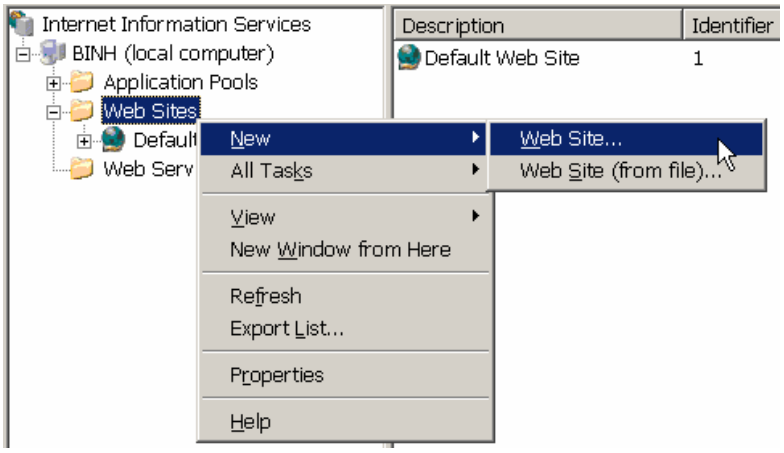
b. Cấu hình sử dụng tập tin Default

Các bước tạo Site

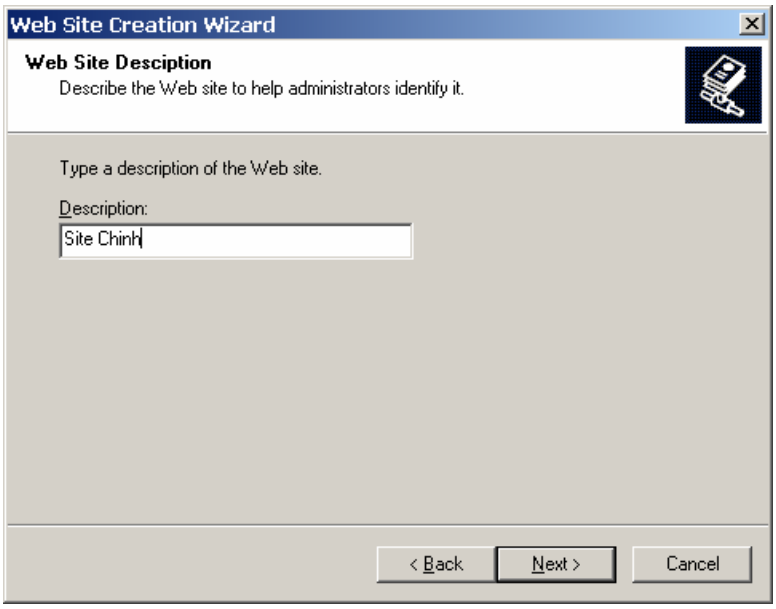
- Yêu cầu 1: Tạo Site chính, chỉ định index.htm là file Default
- Yêu cầu 2: Tạo thư mục ảo DaoTao, chỉ định home.htm là file Default

Yêu cầu 1:

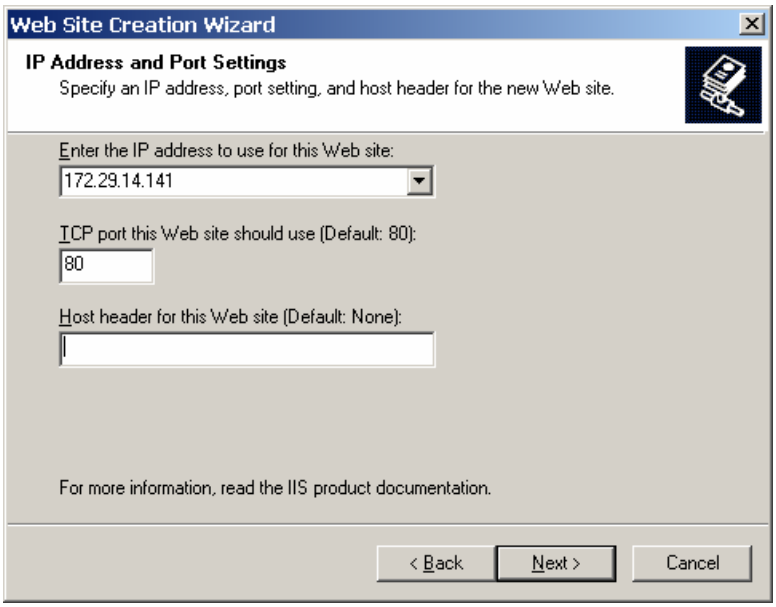
Bước 1: bạn chạy IIS Manager, kích chuột phải vào thư mục Web Sites, chọn New, Web Site.



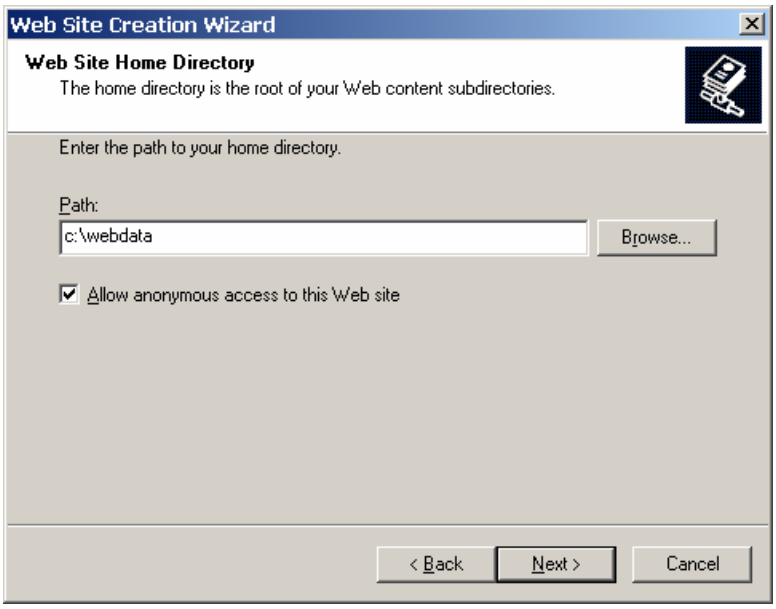
Bước 2: hộp thoại "Welcome to the Web Site Creation Wizard", bạn chọn Next để tiếp tục. Sau đó, hộp thoại Web Site Description, bạn nhập tên "diễn giải" cho Web Site. Sau đó chọn Next để tiếp tục



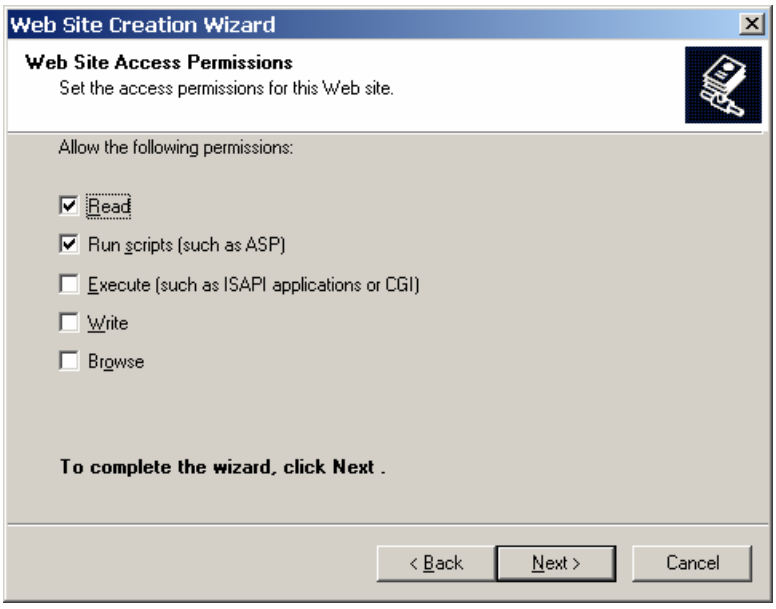
Bước 3: trong hộp thoại "IP Address and Port Settings", bạn cho hệ thống biết hệ thống sẽ dùng địa chỉ IP và IP bao nhiêu cho Web server. Trong hình minh họa bên dưới, hệ thống sẽ sử dụng địa chỉ 172.29.14.141, Port 80 cho Web server.



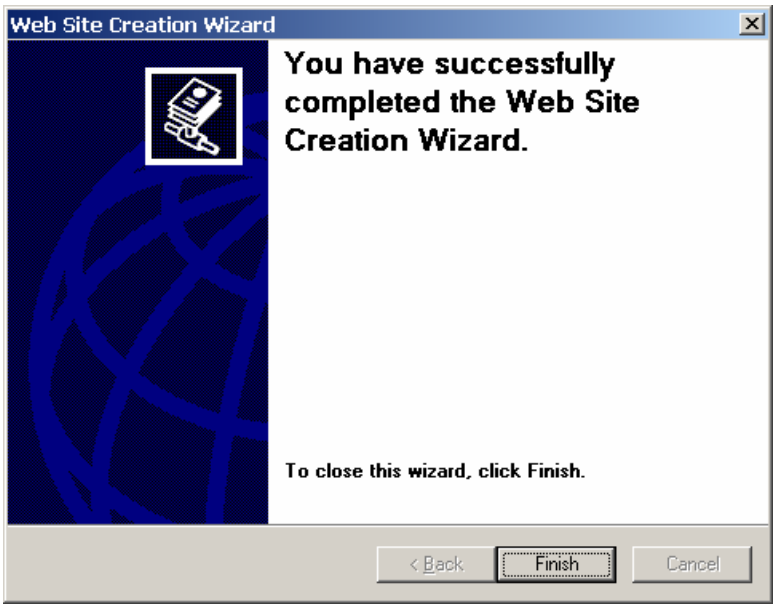
Bước 4: trong hộp thoại "Web Site Home Directory", trong phần Path, bạn chỉ ra thư mục trên ổ cứng, nơi lưu trữ các trang Web.



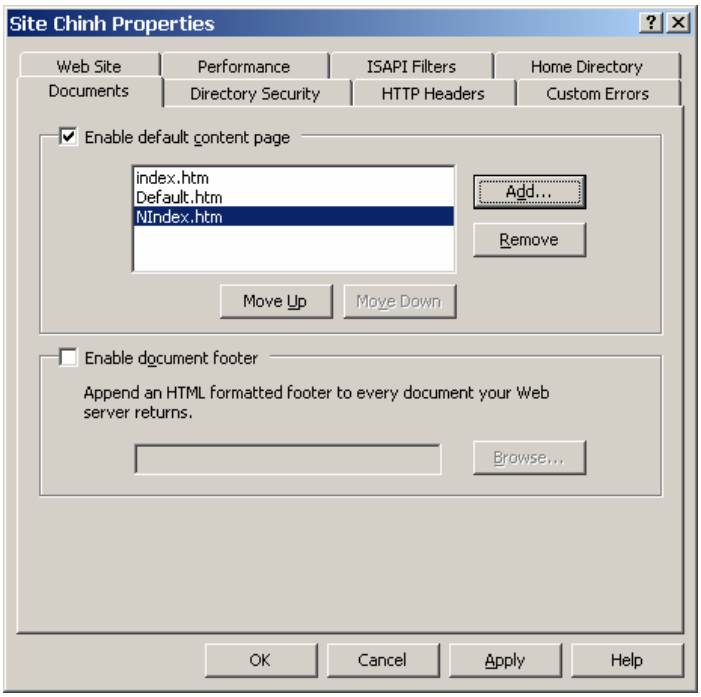
Bước 5: trong hộp thoại "Web Site Access Permissions", bạn chọn lựa các quyền mà user được phép khi đăng nhập thông qua Web Server.



Bước 6: bạn chỉ việc chọn Finish để kết thúc quá trình cài đặt.



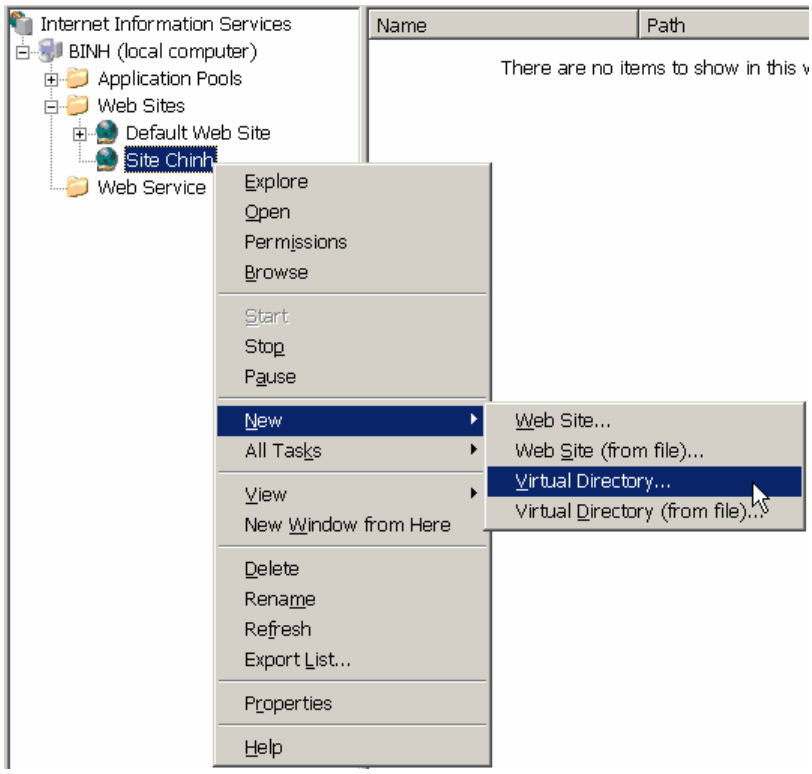
Để trang Default có thể tự động hiện lên, bạn phải cho hệ thống biết là sẽ chọn lựa các trang Default từ đâu ? có tên là gì ?. Để làm được điều này, bạn chọn Properties của Site Chinh, chọn Tab Documents. Bạn Remove file Default.asp trong mục Enable Default content page, và thêm NIndex.htm



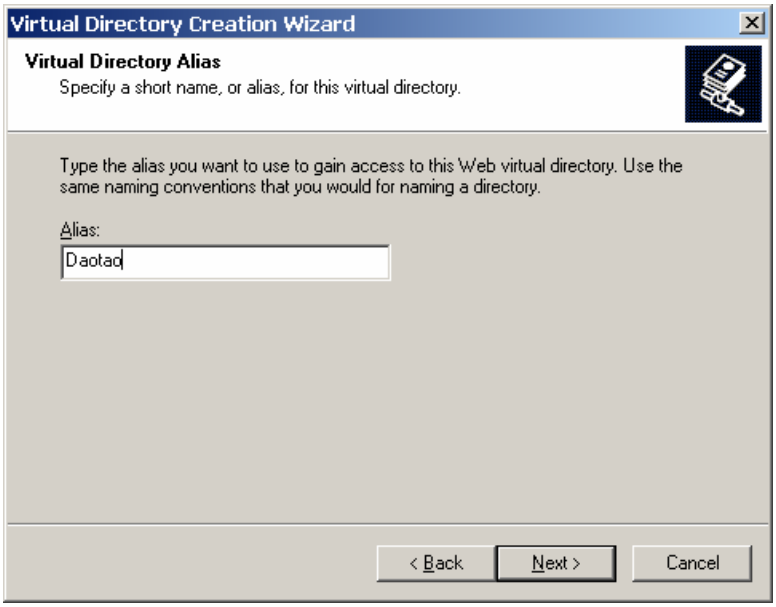
Với thông tin như hình trên, thì hệ thống sẽ ưu tiên cho file index.htm làm trang Default, nếu không có file index.htm thì hệ thống sẽ chọn Default.htm, nếu không có Default.htm thì hệ thống sẽ chọn file Nindex.htm làm trang Default. Nếu không có tập tin nào thì hệ thống sẽ không hiển thị nội dung (trừ khi user có quyền Browse thư mục này).

Yêu cầu 2: Tạo Virtual Directory

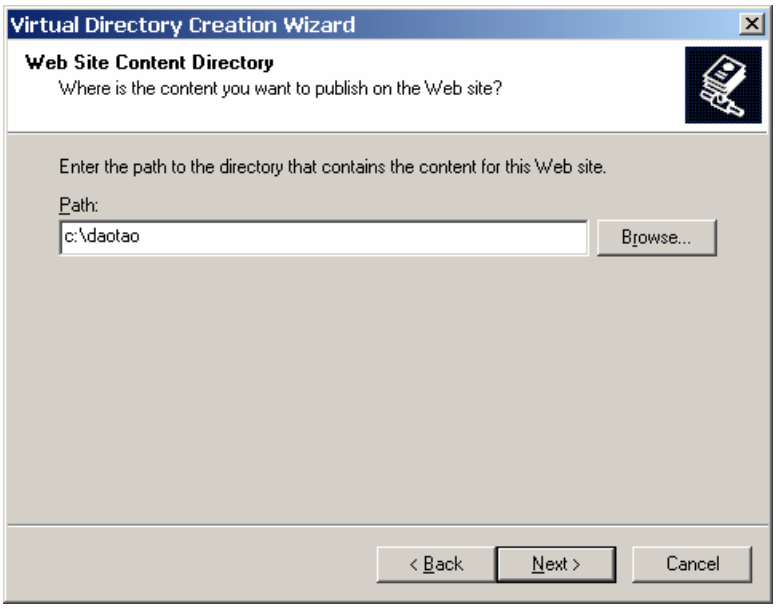
Bước 1: kích chuột phải vào "Site Chinh", chọn New, chọn Virtual Directory



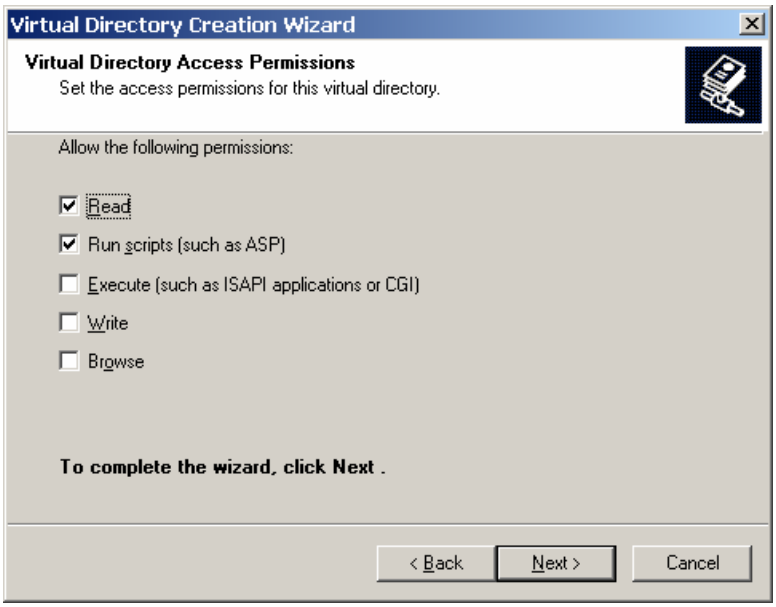
Bước 2: hộp thoại "Welcome to the Virtual Directory Creation Wizard" hiện lên, bạn chỉ cần chọn Next để tiếp tục. Trong hộp thoại "Virtual Directory Alias", bạn nhập tên "diễn giải" cho thư mục, nói cách khác, bạn nhập tên thư mục ảo.



Bước 3: trong hộp thoại "Web Site Content Directory", trong mục Path, bạn chọn đường dẫn thực trên ổ đĩa, nơi lưu trữ các trang Web của thư mục ảo.



Bước 4: trong hộp thoại "Virtual Directory Access Permissions", bạn chọn quyền của các User khi đăng nhập vào thư mục ảo đó.



Bước 5: chọn Finish để kết thúc việc thiết lập Virtual Directory.

Chỉ định Site Default cho DaoTao, bạn thực hiện tương tự ở trên (thêm file Home.htm vào Default content page)

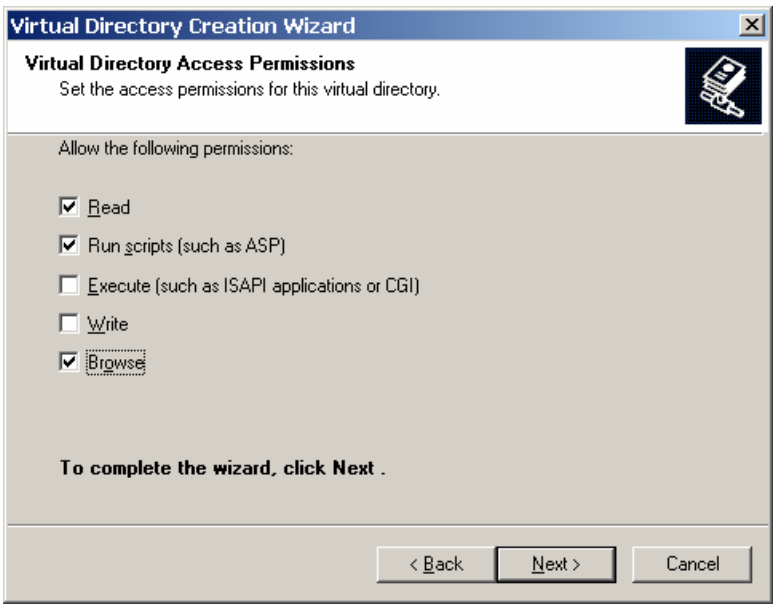
a. Tổ chức các nhóm

Tạo Group và User theo yêu cầu (tham khảo Quản trị mạng 2003)

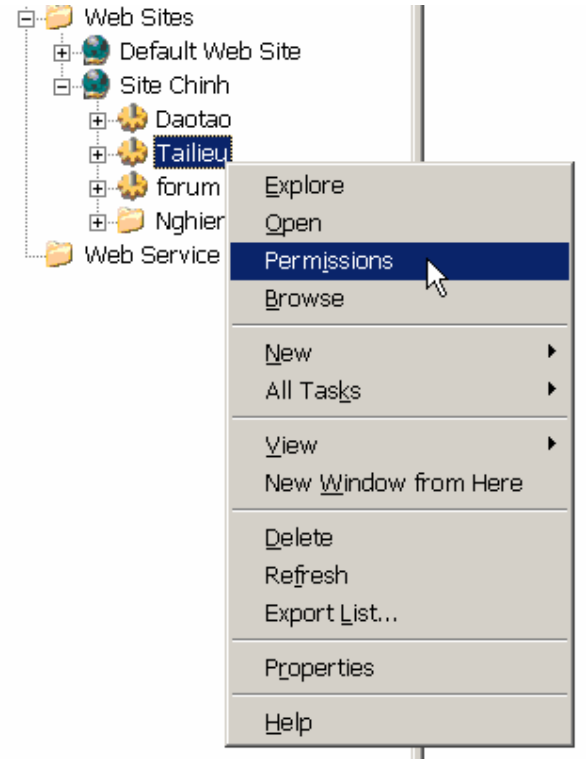
b. Tạo một thư mục ảo có tên tailieu ánh xạ về thư mục thật D:\Soft

Tạo một Virtual Directory (tên là Tailieu) chỉ về thư mục D:\Soft (tham khảo câu 2b)

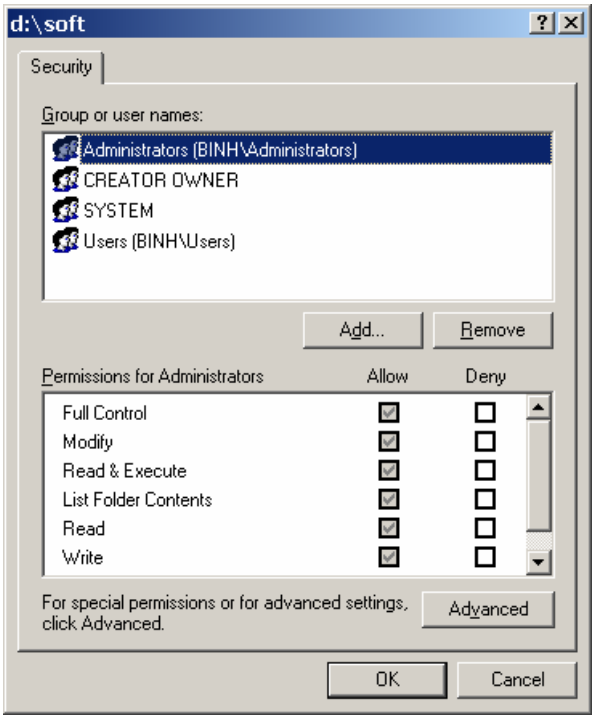
Chú ý:



Chọn Permissions

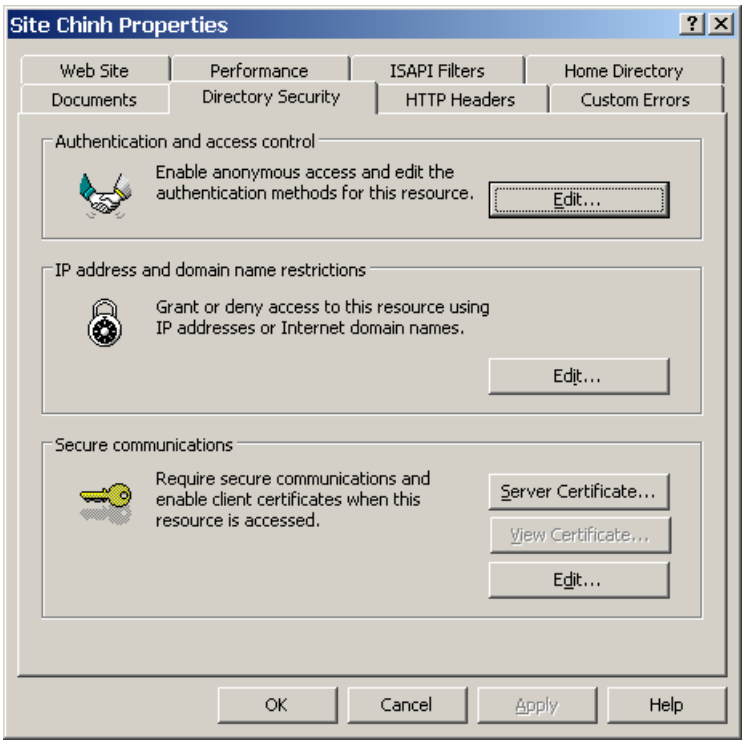


Sau đó bạn chỉnh sửa theo yêu cầu (chỉ có nhóm Webmaster mới có quyền chỉnh sửa và Upload (Full), các user còn lại chỉ có quyền Read (Read)

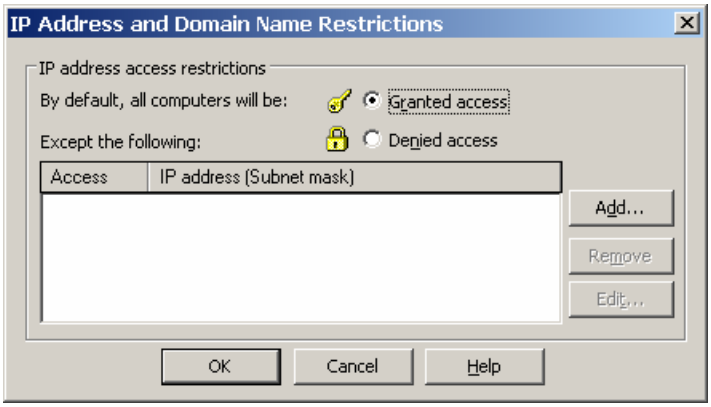


c. Không cho phép các máy trong đường mạng 192.168.12.0 truy xuất Web Server

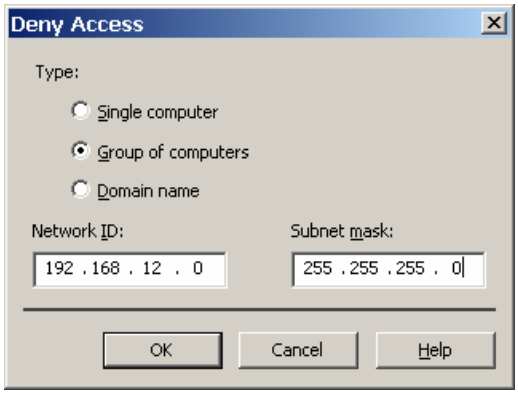
Bước 1: chọn Properties của "Site Chinh"



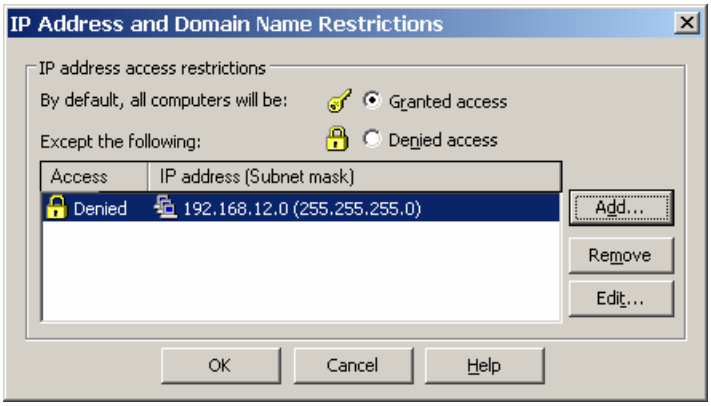
Bước 2: tab Directory Security, chọn Edit



Bước 3: chọn mục Granted access, chọn Add

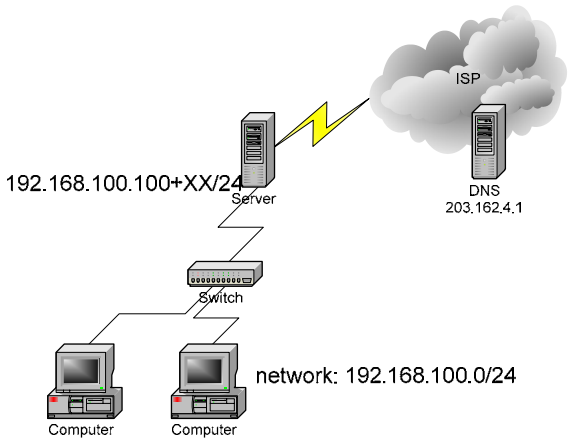


Bước 4: chọn mục Group of computers, nhập đường mạng 192.168.12.0/24, sau đó chọn Ok



Chọn Ok, sau đó Apply để thực thi

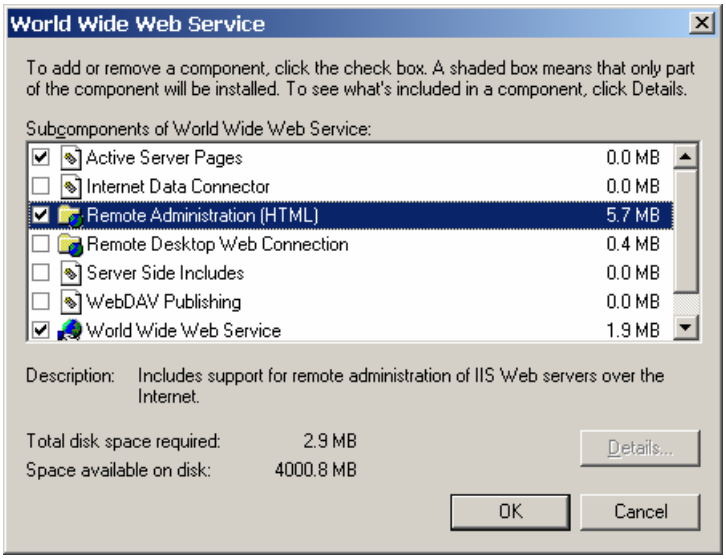
Bài tập 03.2



*Bạn là người quản trị cho một mạng máy tính của **công ty XX** kết nối lên Internet như hình vẽ. Máy chủ cài Win2k3 server và máy làm phục vụ dịch vụ DNS, Mail, Web, FTP cho công ty. Công ty thuê một tên miền "**ctyXX.com.vn**"*

1. **Bài 1: tìm hiểu cấu hình cơ chế quản trị Web site, FTP site(Administration Web Site) thông qua trình duyệt web.**

Cài đặt thêm tính năng Remote Administrator trong IIS (tham khảo hình sau)

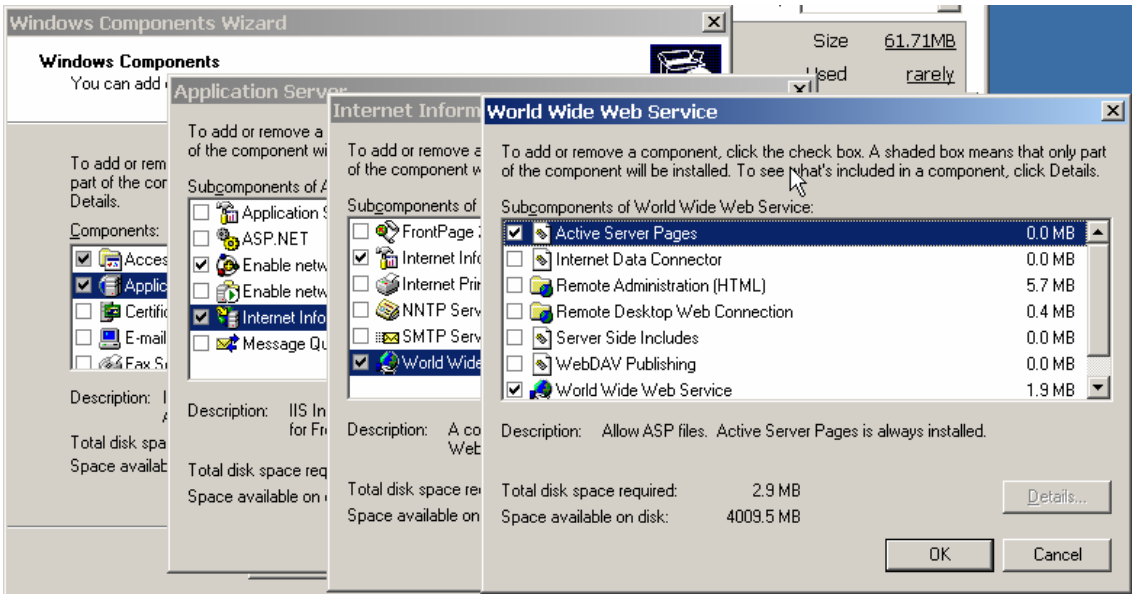


Sau đó sử dụng IIS để truy cập (tham khảo giáo trình "Dịch vụ mạng Windows 2003" – phần IV.2.7 – trang 98).

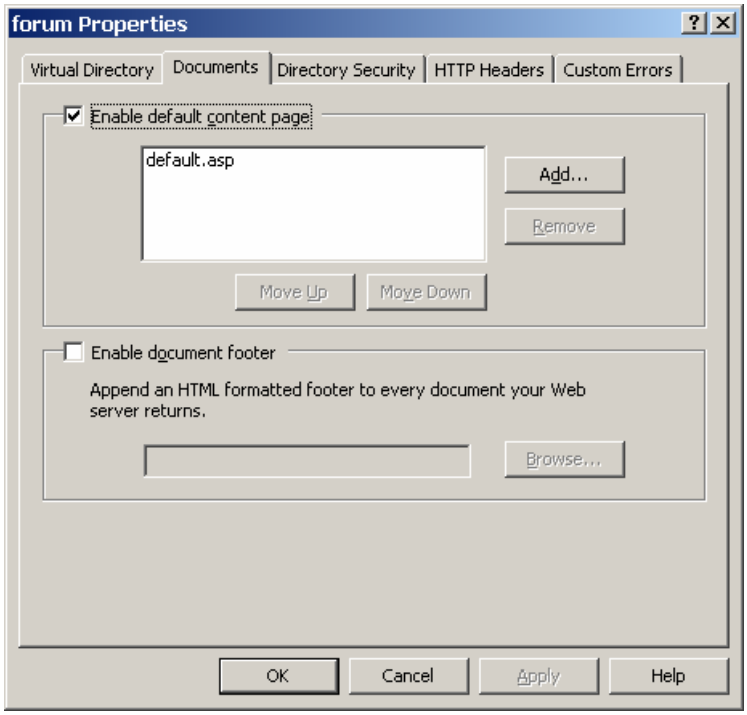
2. **Bài 2: tạo Forum**
   a. Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 3 – phần IV.2.10 – trang 103).

Chú ý:

Trong lúc cài đặt IIS, phải chọn thêm ASP, như hình sau



Phải hiệu chỉnh lại trang mặc định là default.asp



b. Cài đặt DNS để người dùng có thể truy xuất thông qua tên miền

3. Bài 3: Web Hosting

Sử dụng cách Host header (tham khảo giáo trình "Dịch vụ mạng Window 2003" – phần IV.2.6 – trang 96)

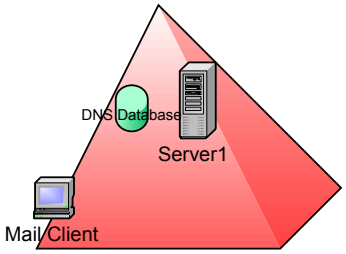
4. Bài 4: cấp quyền cho Webmaster có quyền cập nhật Web Site thông qua FTP.

Để đạt được điều này, bạn cần thực hiện 2 yêu cầu sau:

- Yêu cầu 1: Tạo user Webmaster
- Yêu cầu 2: Sử dụng FTP để tạo Virtual Directorry (chỉ đến thư mục chứa Web Site hbc.csc02.edu.vn, - C:\WebHosting).

Bài 04
Dịch Vụ Mail

Bài tập 04.1



cscXX.edu.vn

Bạn là người quản trị cho một mạng máy tính cho trung tâm đào tạo tin học (có sơ đồ kết nối như hình vẽ). Máy chủ Server1 cài Win2k3 server và máy làm phục vụ dịch vụ DNS, Mail, Web, FTP cho công ty. Công ty thuê một tên miền "**cscXX.edu.vn",** cấu hình máy chủ Server1 này theo yêu cầu sau.

1. **Bài 1:**

Tham khảo Bài tập 1 (Dịch vụ DNS)

2. **Bài 2:**

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (Chương 4 – phần VII.2 – trang 122)

Tạo các Alias Mail như sau: Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (Chương 4 – phần VII.2.2 – mục 2 – trang 126)

3. **Bài 3: sử dụng mail thông qua Web hoặc qua POP Client**

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.4.4 – trang 136)

4. **Bài 4: sử dụng MS Outlook Express để làm POP3 Client hoặc IMAP Client để soạn thảo và nhận thư từ máy trạm.**

Cài đặt Outlook express để gởi và nhận mail (tham khảo giáo trình "mạng cơ bản")

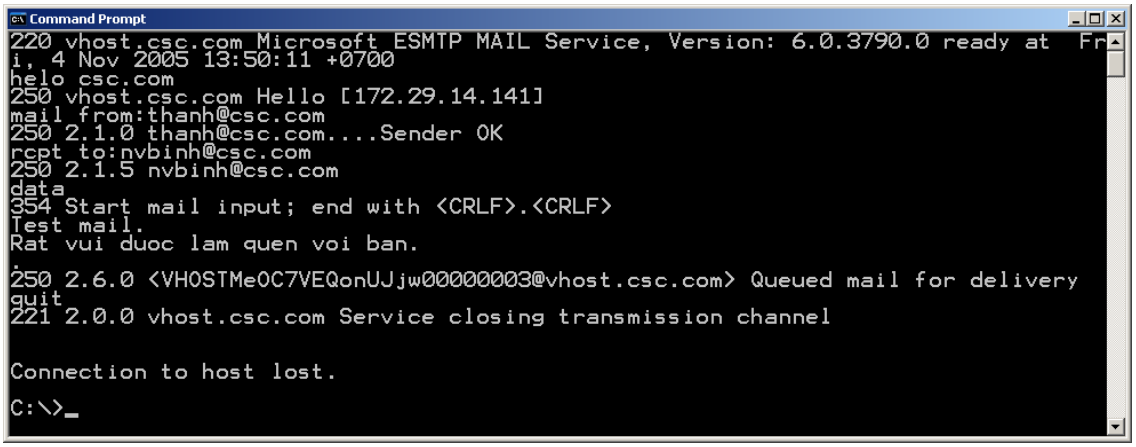
5. **Bài 5: sử dụng tập lệnh SMTP & POP3 để thực hiện quá trình send/receive mail thông qua dòng lệnh.**

Sử dụng Telnet để thực hiện Telnet vào địa chỉ của Mail Server, sau đó tham khảo tập lệnh ở trang 106 (chương 4 – phần I.1 – giáo trình Dịch vụ mạng Windows 2003). Để có thể sử dụng được Telnet thông qua SMTP, bạn cần để ý 2 điều sau:

a. Enable Service Telnet: mặc định, dịch vụ (service) Telnet ở Server đang ở trạng thái Disable. Do đó, bạn phải vào Administrator Tools, chọn Services, chọn Service có tên là Telnet và chuyển sang trạng thái Automatic (tự động kích hoạt khi máy khởi động lên) và chọn vào Start để dịch vụ Telnet được kích hoạt.

b. Telnet qua Port 25: do SMTP sử dụng Port 25, và mặc định Telnet sẽ kết nối thông qua Port 23. Nên để kết nối với dịch vụ SMTP thông qua Telnet thì bạn phải sử dụng Telnet thông qua Port 25. Hình dưới đây minh họa cách kết nối vào SMTP Server (địa chỉ 172.29.14.151) thông qua Port 25.

Đây là một ví dụ khi sử dụng Telnet để sử dụng địa chỉ thanh@csc.com gởi mail đến nvbinh@csc.com (nội dung là "Test mail, rat vui duoc lam quen voi ban")



Chú ý: Để kết thúc nội dung mail, bạn chỉ cần dấu "." ở 1 dòng riêng biệt.

Bài tập 04.2

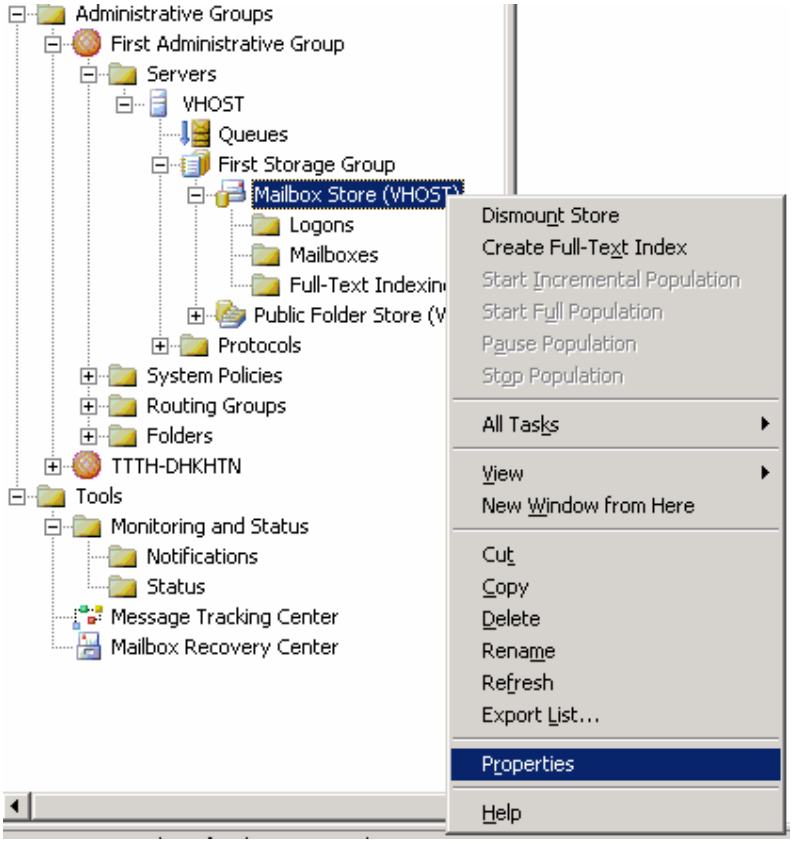
1. **Bài 1: cài đặt Exchange trên Server1 để cung cấp hệ thống thư điện tử (E-mail) cho miền "cscXX.edu.vn".**

Tham khảo bài 04.1.

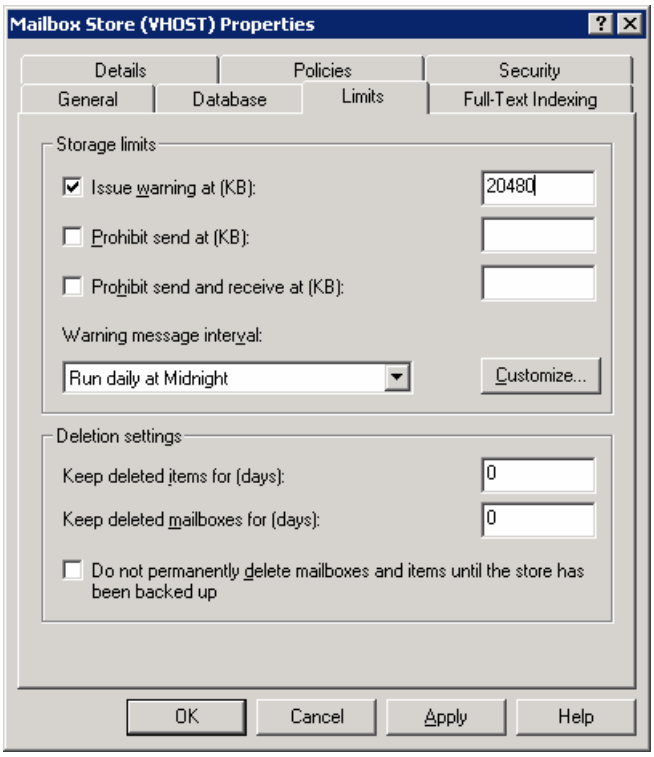
2. **Bài 2: cấp một số quyền hạn sau:**
   a. Mỗi hộp thư của tài khoản có dung lượng tối đa cho phép là 20M.

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.5.5 – trang 143)

Bước 1: bạn vào Exchange System Manager, chọn Administrator Groups, chọn First Administrative Group, chọn Servers, chọn VHOST, chọn First Storage Group, kích chuột phải vào Mailbox Store (VHOST) chọn Properties



Bước 2: chọn Tab Limits, trong mục "**Issue warning at (KB)**" chỉnh sửa lại kích thước theo yêu cầu, 20MB = 20480 KB. Sau đó chọn Apply, chọn Ok để kết thúc quá trình thiết lập.

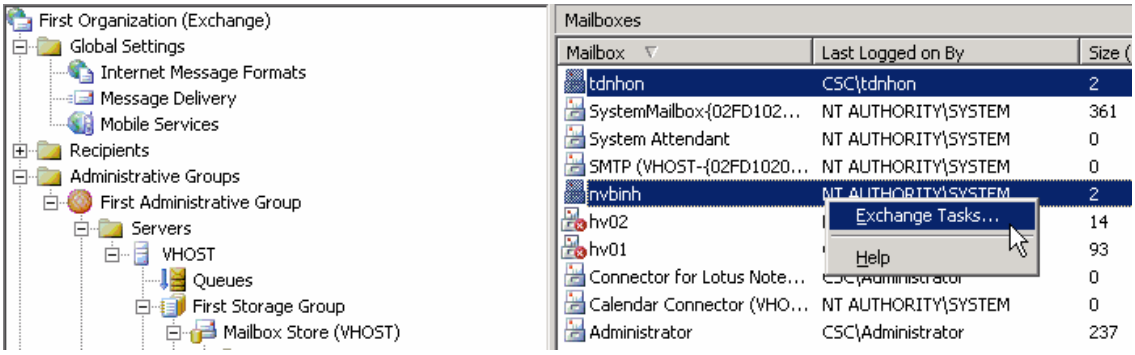


b. Chỉ cho phép các tài khoản trong nhóm Admins và Giamdoc trên được sử dụng Web mail, OMA, POP3, IMAP. Các user còn lại chỉ sử dụng Webmail, POP3.

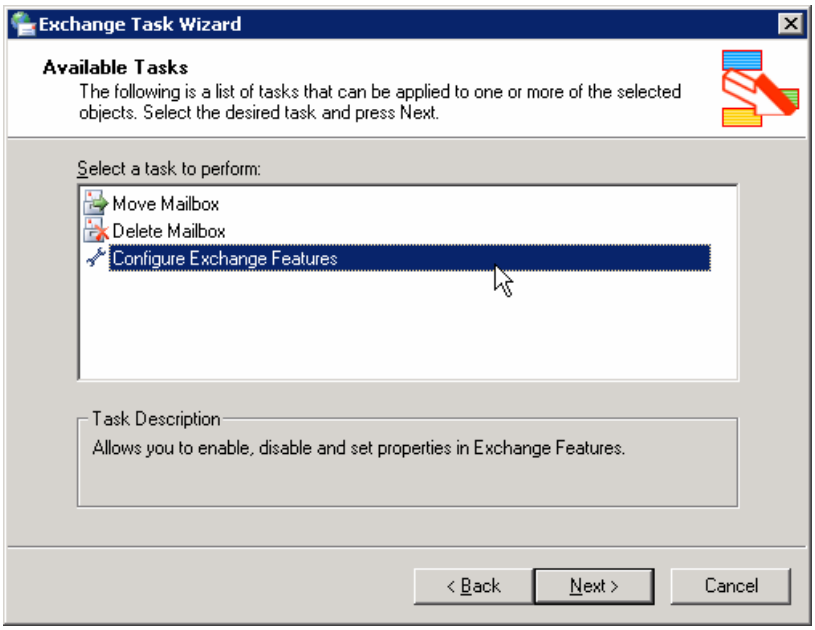
Có 2 cách:

Cách 1: Thực hiện trong Mailbox của Mail Exchange (chỉ có các user đã sử dụng mail).

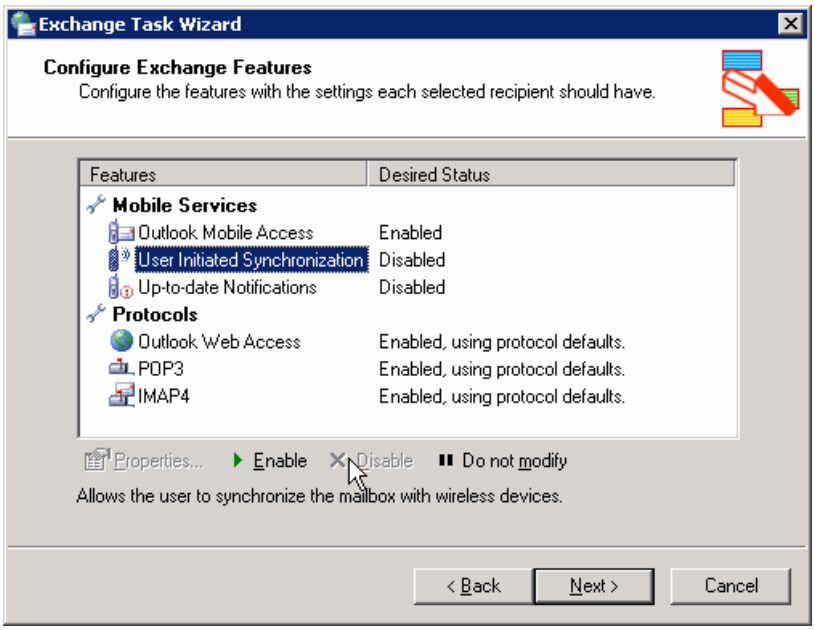
Bước 1: vào Mailbox Store, chọn user Account và chọn "Exchange Tasks…", nếu muốn chọn nhiều Account cùng một lúc thì giữ phím Ctrl và chọn tiếp Account khác.



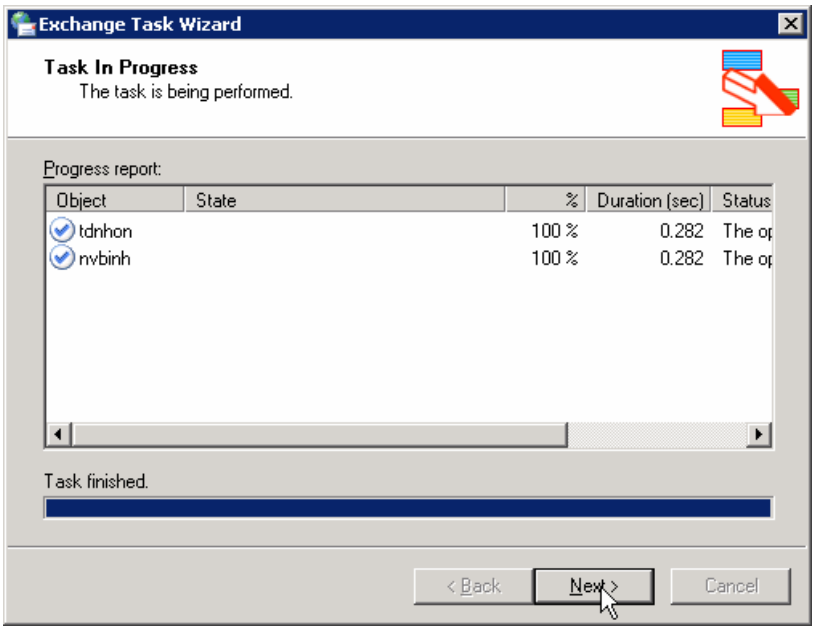
Bước 2: trong hộp thoại "Available Tasks", chọn Configure Exchange Features, sau đó chọn Next



Bước 3: trong hộp thoại "Configure Exchange Features", chọn tính năng, sau đó chọn Enable – Disable hay là "Do not modify" cho từng tính năng tương ứng. Đối với nhóm Admins và Giamdoc, sau khi chọn các tính năng bạn sẽ thấy như sau:



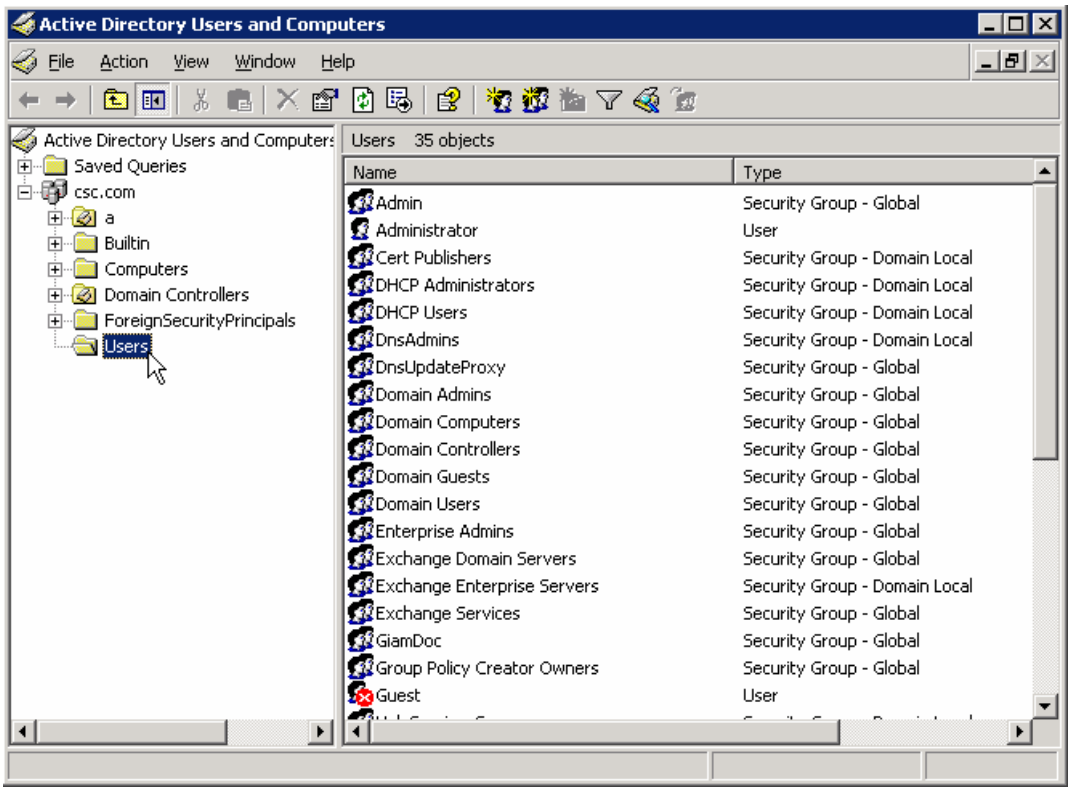
Bước 4: trong hộp thoại "Task In Progress", chọn Next



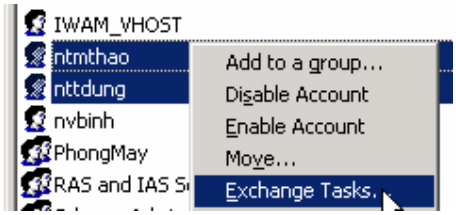
Bước 5: chọn Finish để kết thúc

Cách 2: Thay vì thao tác trong Mail Exchange, bạn có thể thực hiện đối với các Account trong Active Directory Users and Computers,

Bước 1: mở Active Directory Users and Computers, chọn mục Users



Bước 2: chọn các user cần thực thi, kích chuột phải và chọn "Exchange Task.."

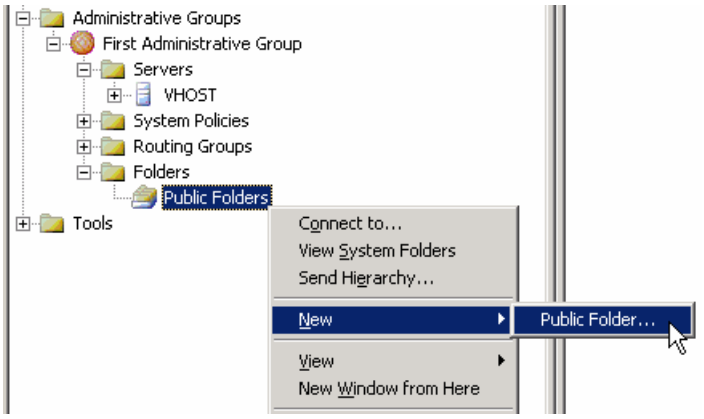


Bước 3: từ bước này trở đi, bạn thực hiện giống như từ Bước 2 của cách 1.

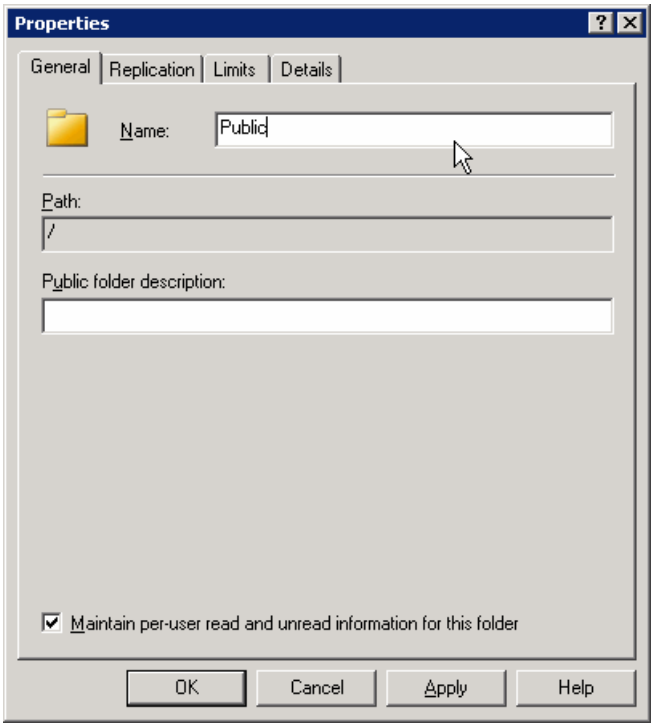
c. Dung lượng tối đa của Public Folder được lưu trên server 100M, cho phép mọi người dùng có thể sử dụng Public Folder.

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.6.2 – trang 145)

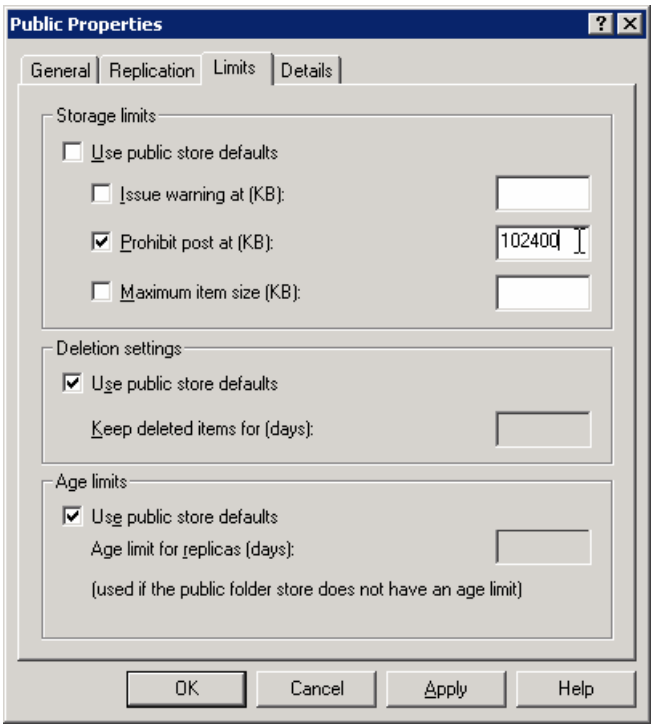
Bước 1: trước tiên, bạn tạo một Public Folder. Bạn vào Exchange System Manager, chọn Administrative Groups, chọn First Administrative Group, chọn mục Folder, kích chuột phải vào Public Folders, chọn New, chọn Public Folder…



Bước 2: trong Tab General, trong mục Name, bạn đặt tên cho thư mục này, ví dụ là Public



Bước 3: sau đó chọn Tab Limits, trong mục “Prohibit post at (KB)” bạn đặt 102400 (100MB). Sau đó chọn Ok để hoàn tất việc thiết lập

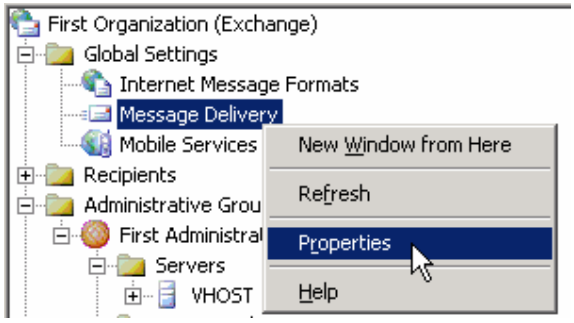


Để cho phép người dùng sử dụng, bạn làm theo hướng dẫn ở trang 147.

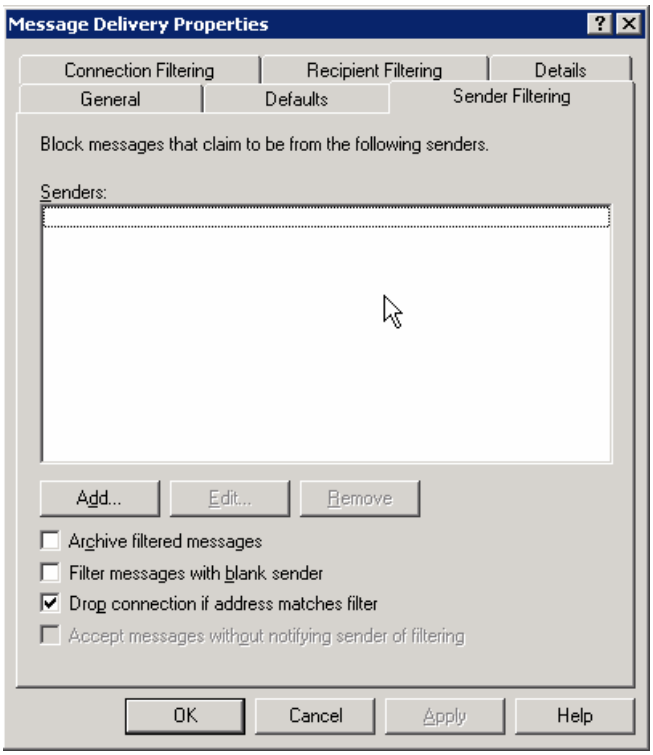
d. Ngăn địa chỉ mail abc@yahoo.com gởi mail vào miền nội bộ, chặn tất cả email từ miền nội bộ gởi tới người dùng có địa chỉ mlbadmail@yahoo.com

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.5.1 – trang 138)

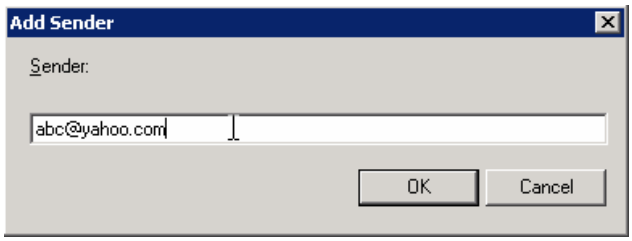
Bước 1: bạn mở Exchange System Manager, chọn First Organization, chọn Global Settings, kích chuột phải vào Message Delivery, chọn Properties



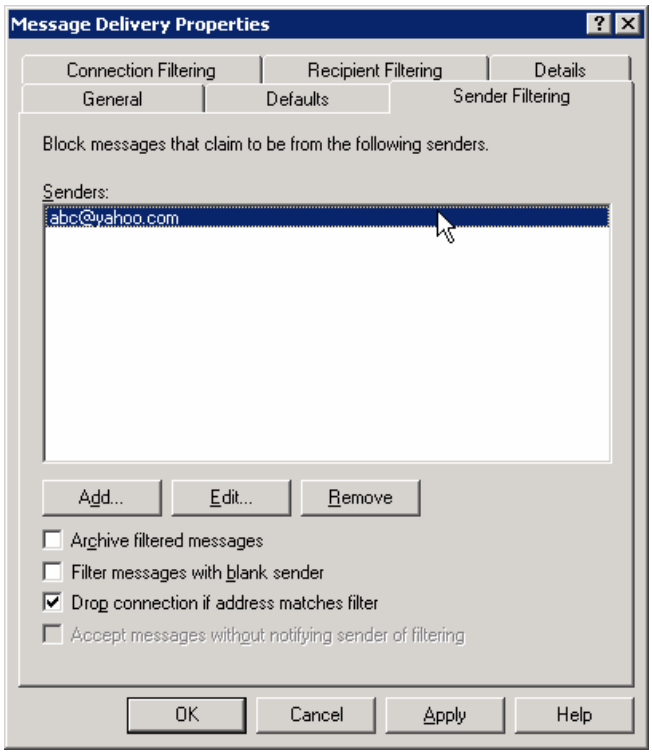
Bước 2: chọn Tab Sender Filtering



Bước 3: chọn Add, thêm địa chỉ abc@yahoo.com vào



Bước 4: chọn Ok để hoàn tất việc thêm địa chỉ abc@yahoo.com



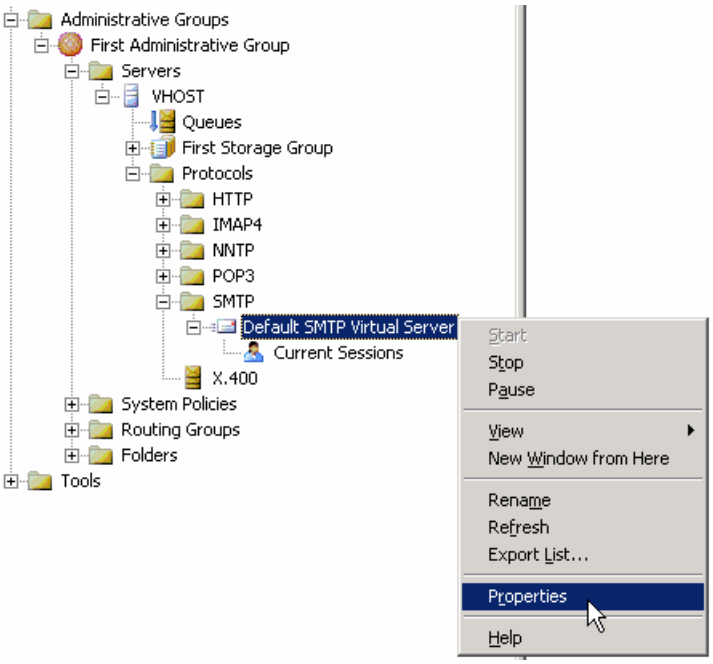
Bước 5: chọn Ok để hoàn tất việc thiết lập

Để ngăn người dùng nội bộ gởi mail đến mlbadmail@yahoo.com, bạn thực hiện tương tự như trên, nhưng đối với Tab Recipient Filtering.

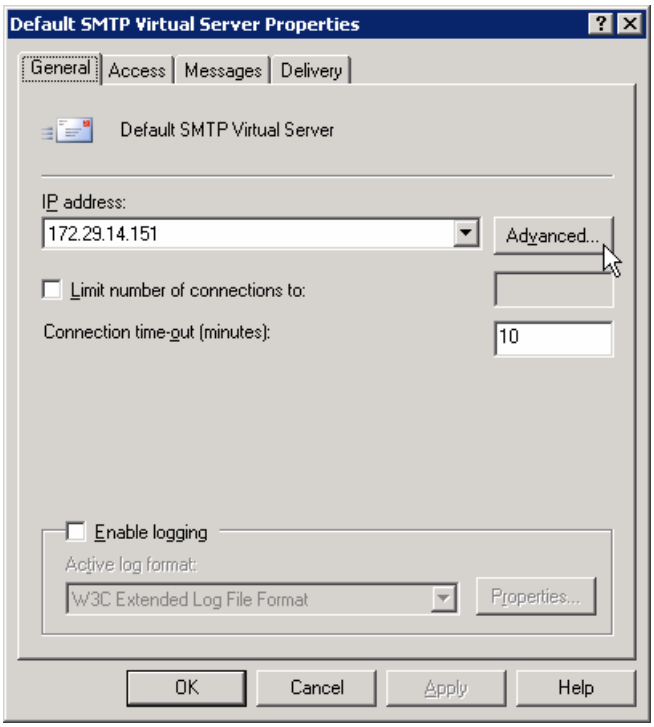
Chú ý:

Sau khi đã tạo xong thì bạn cần phải thực thi chính sách đó. Nếu không thì bạn vẫn không lọc được mail (dù bạn đã định nghĩa ở các bước trên)

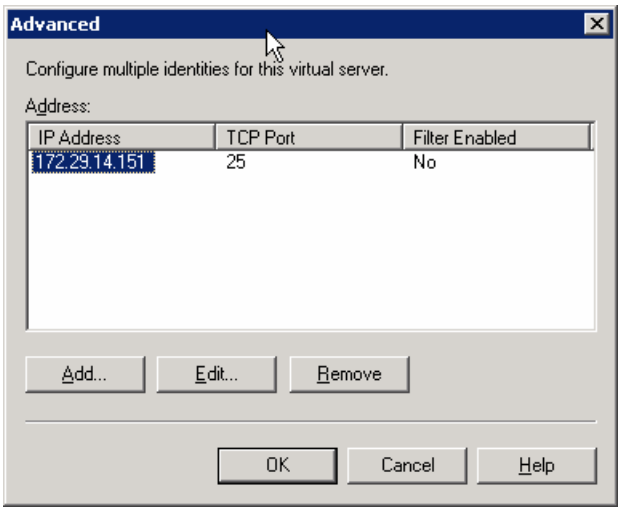
Bước 1: trước tiên, bạn vào Administrative Groups, First Administrative Groups, Servers, VHOST, Protocols, SMTP. Kích chuột phải vào Default SMTP Virtual Server, chọn Properties



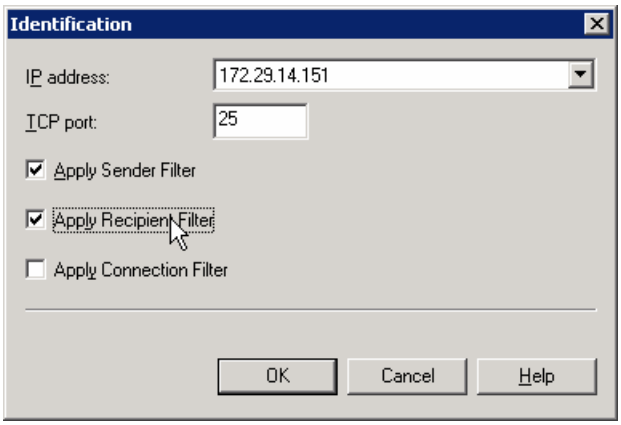
Bước 2: chọn Tab General



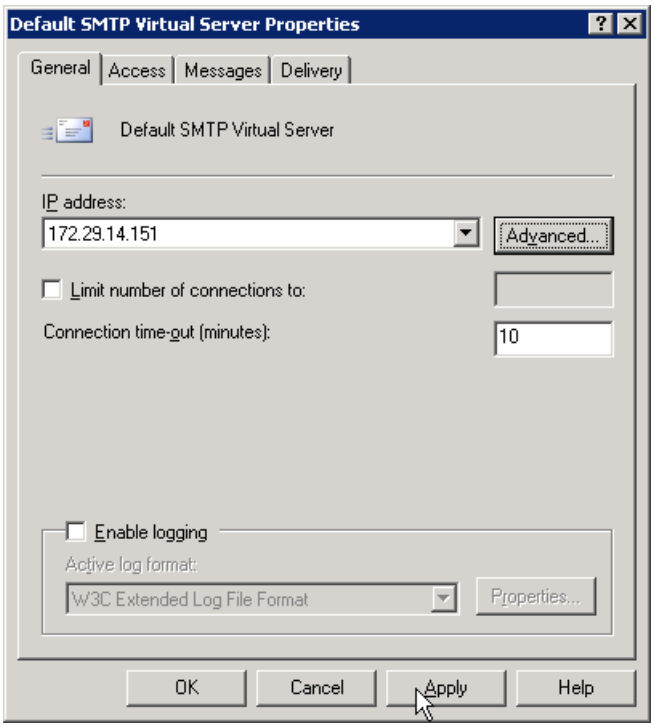
Bước 3: chọn nút Advanced



Bước 4: chọn địa chỉ 172.29.14.151, sau đó chọn vào nút Edit. Do bạn cần lọc mail dựa vào địa chỉ người gởi và người nhận nên bạn phải chọn vào mục "**Apply Sender Filter**" và mục "**Apply Recipeint Filter**". Sau đó chọn Ok để đóng hộp thoại lại



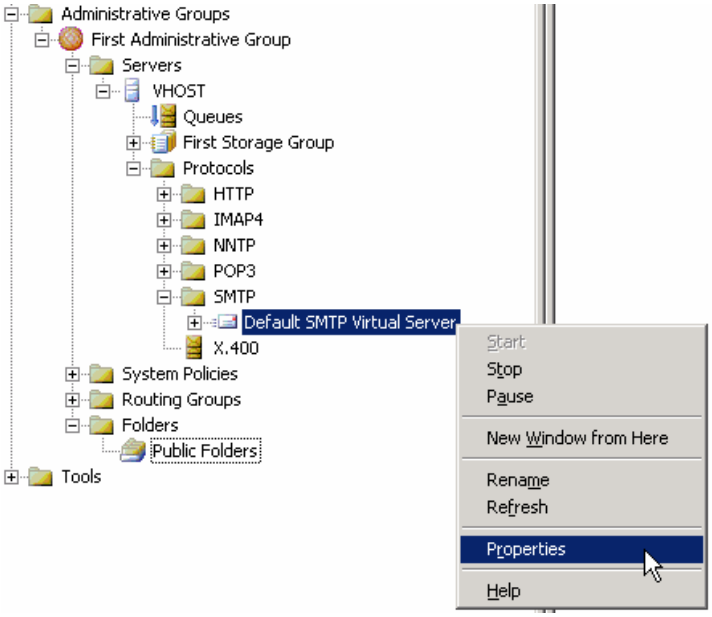
Bước 5: chọn Ok lần nữa để quay về hộp thoại Default SMTP Virtual Server Properties, sau đó bạn chọn Apply để cập nhật sự thay đổi. Rồi chọn Ok để hoàn tất việc lọc mail người gởi và người nhận.



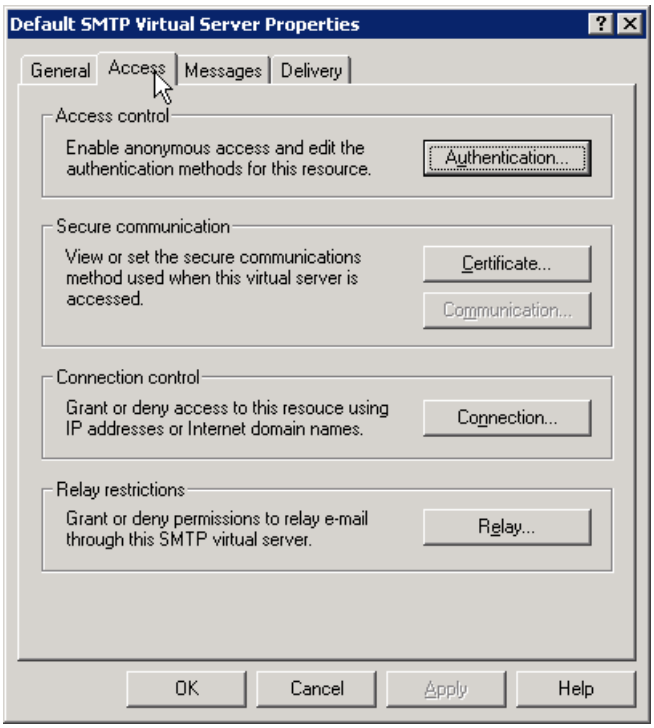
e. Ngăn chặn địa chỉ mạng 192.168.10.0 không được connect và mail server.

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.5.3 – trang 142)

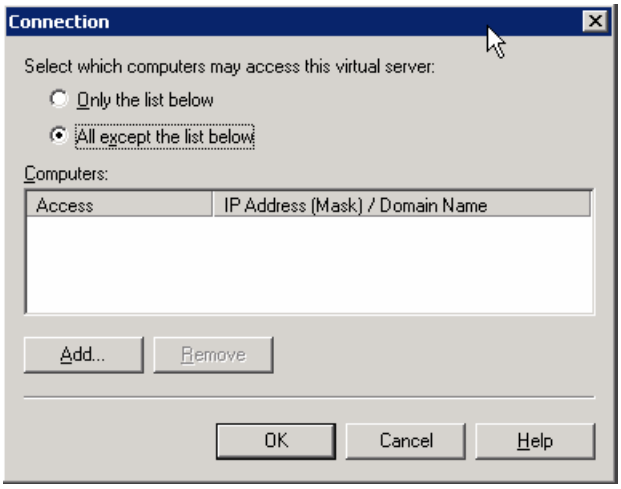
Bước 1: vào Properties của Default SMTP Virtual Server



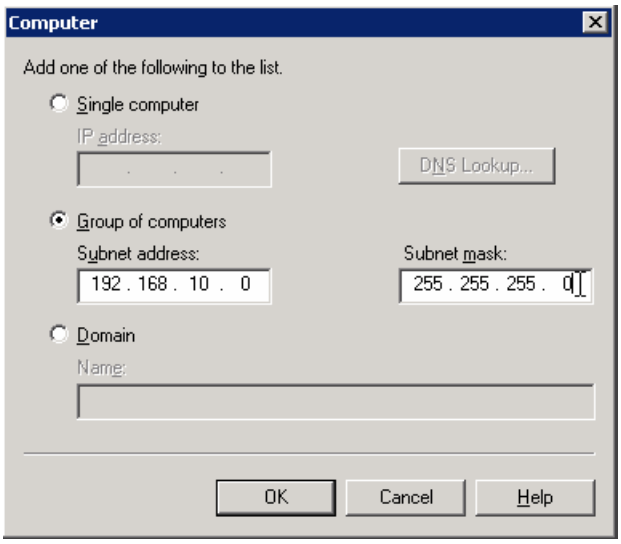
Bước 2: chọn Tab Access



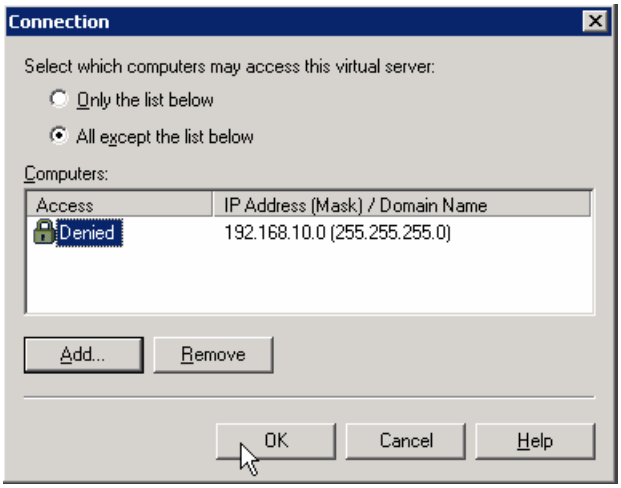
Bước 3: chọn nút Connection…, chọn mục All except the list below (chấp nhận tất cả các đường mạng, ngoại trừ các đường mạng được liệt kê ở bên khung dưới).



Bước 4: chọn mục Group of computers và điền giá trị đường mạng vào, sau đó chọn Ok



Bước 5: sau khi điền xong, bạn thấy như sau, chọn Ok để tắt bảng Connection.

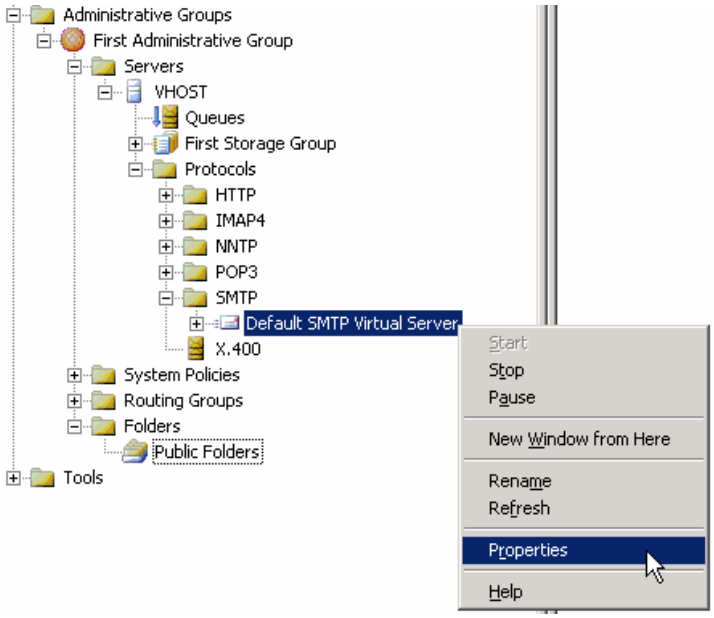


Bước 6: chọn Ok để hoàn tất việc thiết lập.

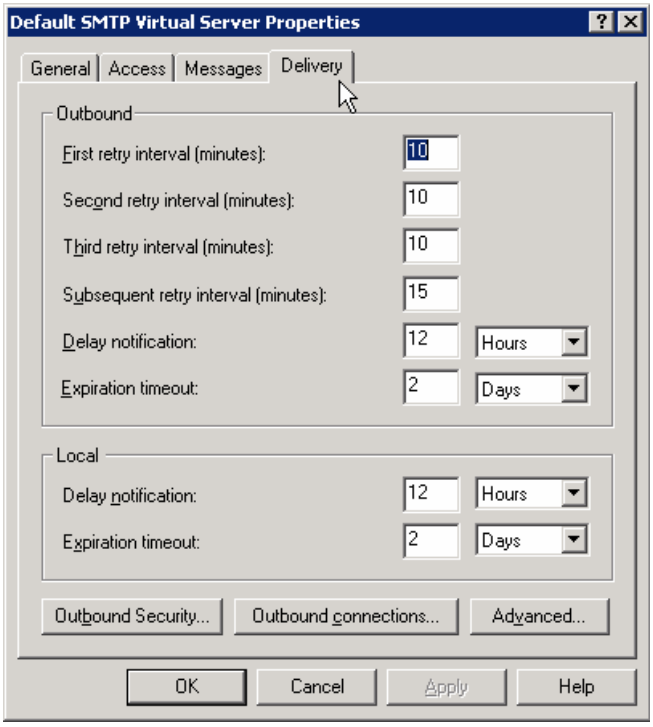
f. Khai báo Smart host có địa chỉ mail.hcm.vnn.vn để chỉ định mail gateway cho mail server nội bộ.

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.5.4 – trang 143)

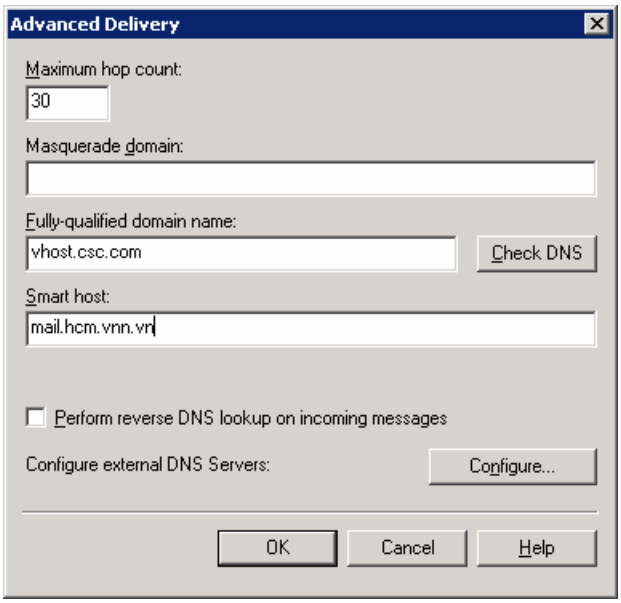
Bước 1: vào Properties của Default SMTP Virtual Server



Bước 2: chọn Tab Delivery



Bước 3: chọn nút Advanced…

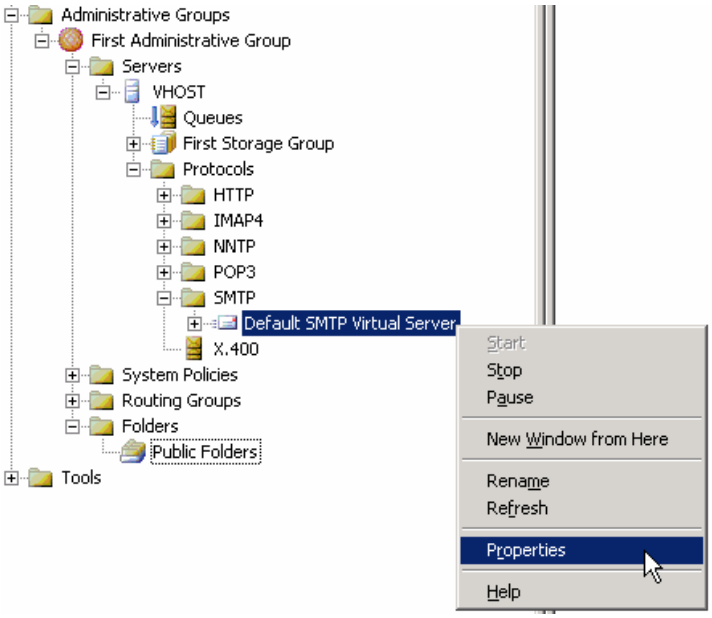


Điền địa chỉ mail.hcm.vnn.vn vào mục Smart host. Sau đó chọn Ok. Chọn Ok lần nữa để hoàn tất.

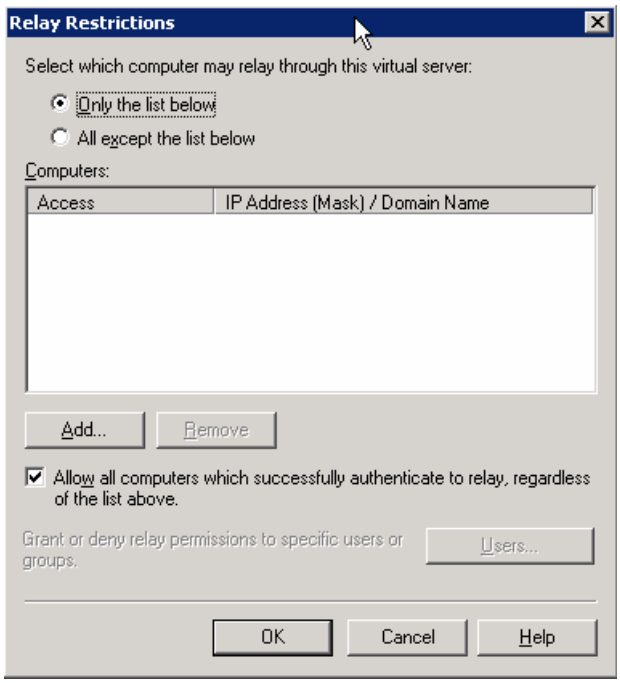
g. Cấu hình relay mail cho tất cả các miền bên ngoài gởi mail vào miền nội bộ, chỉ không relay cho máy trong mạng 172.29.0.0/16.

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 4 – phần VII.5.2 – trang 141)

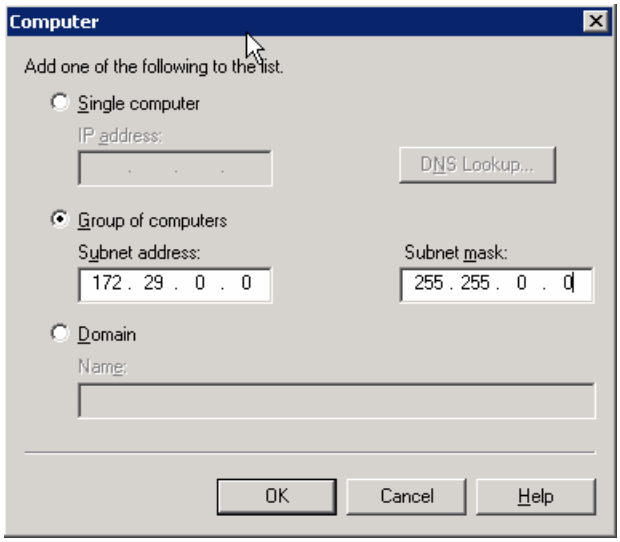
Bước 1: vào Properties của Default SMTP Virtual Server



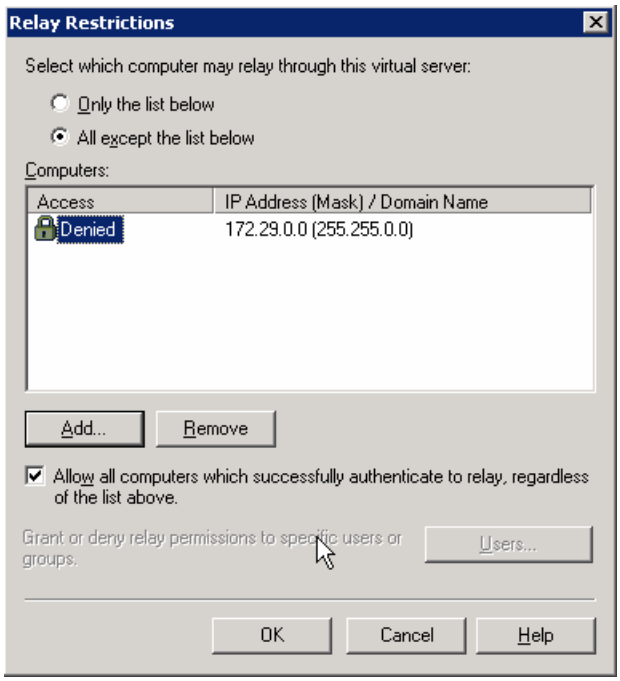
Bước 2: chọn Tab Access, sau đó chọn nút Relay



Bước 3: chọn mục All except the list below, sau đó chọn Add. Chọn mục Group of computers và điền địa chỉ IP của đường mạng 172.29.0.0/16 vào. Sau đó chọn Ok



Bước 4: sau khi đã thêm vào, bạn thấy kết quả như sau:

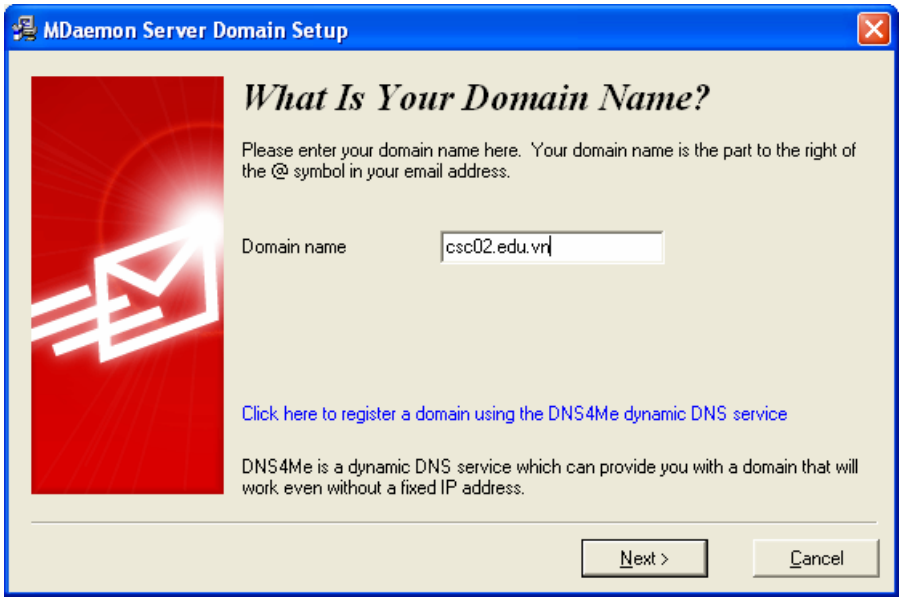


Bước 5: chọn Ok để tắt hộp thoại Relay Restrictions và chọn Ok lần nữa để hoàn tất thiết lập.

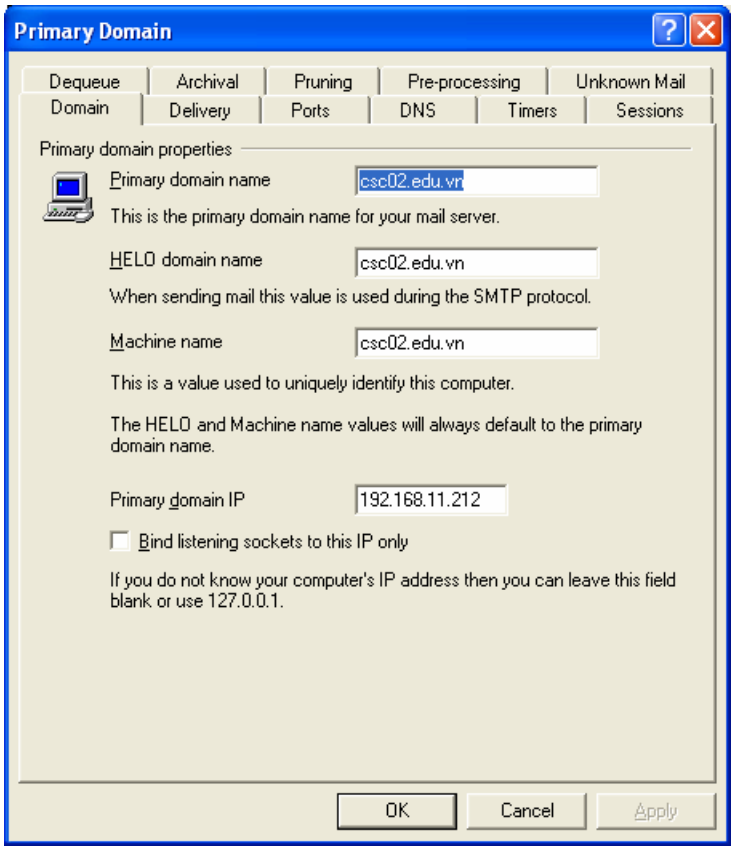
3. Bài 3:

a. Cài đặt mail cho tên miền csc02.edu.vn

Trong quá trình cài đặt Mdeamon thì bạn sẽ đặt tên miền csc02.edu.vn).

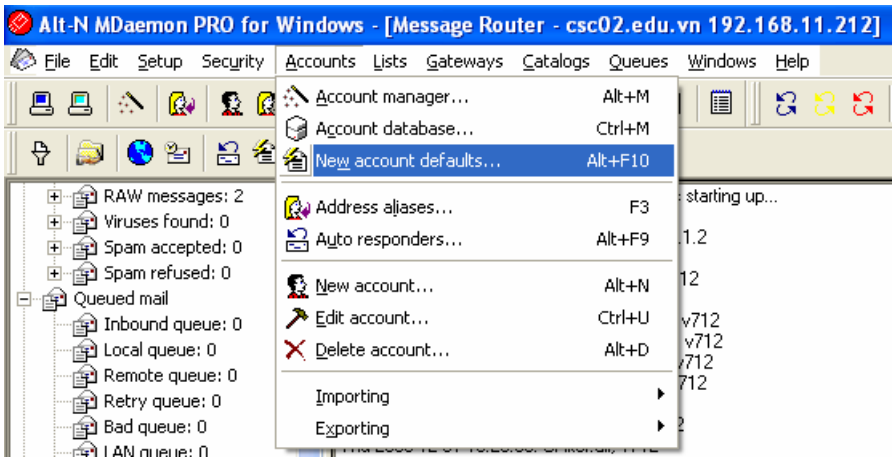


Hoặc, sau khi cài đặt xong, bạn có thể hiệu chỉnh lại bằng cách vào Menu Setup, Primary Domain (hoặc phím tắt là F2)

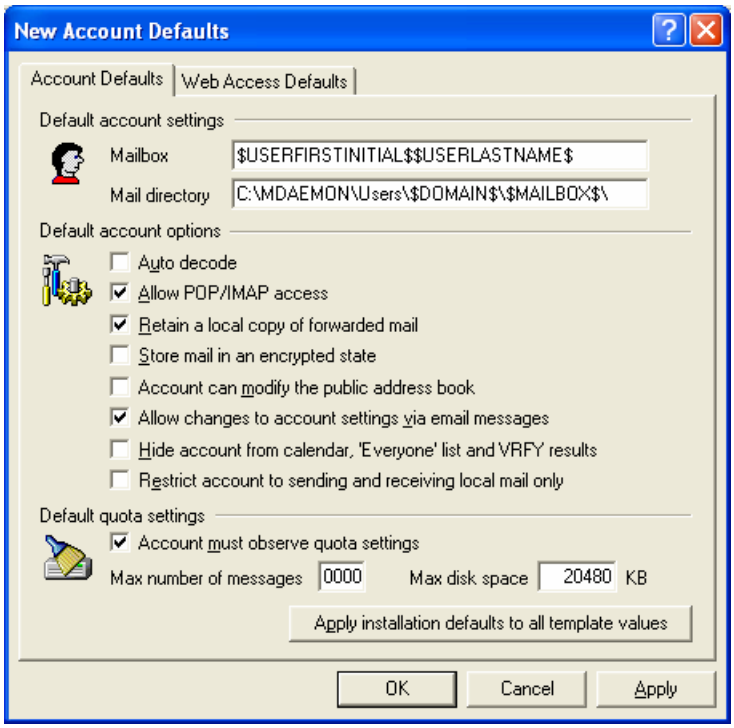


b. Mỗi hộp thư của tài khoản có dung lượng tối đa cho phép là 20M.

Bạn chọn Menu Accounts, chọn new account defaults (hoặc phím tắt là Alt+F10),



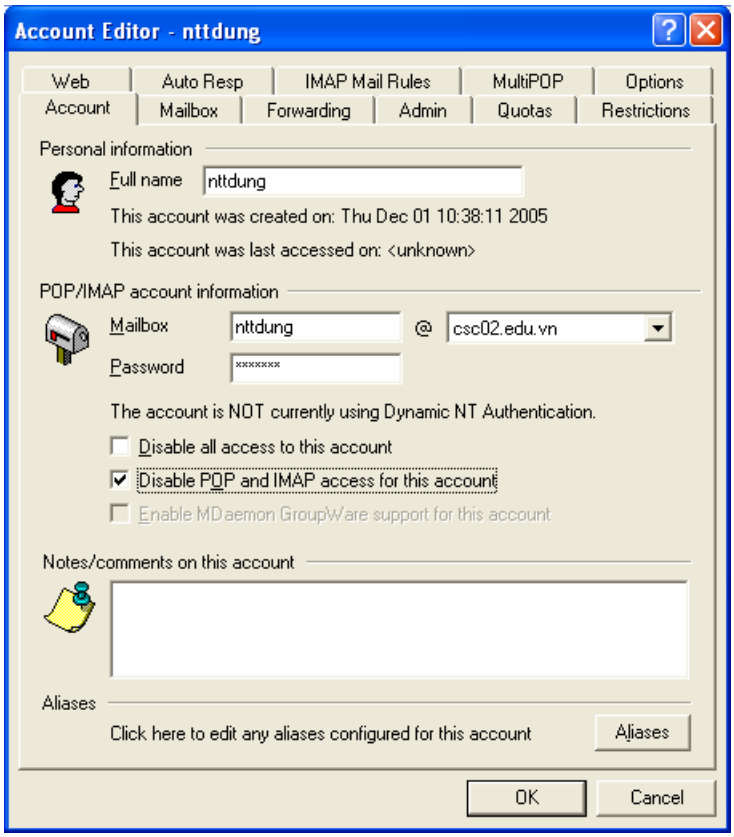
Bạn sẽ thấy hộp thoại New Account Defaults, trong Tab Account Defaults, trong phần Default quota settings, chọn vào mục “Account must observe quota settings” (thiết lập quota cho user), trong mục “Max disk space”, bạn chọn giá trị là 20480. Giá trị trong mục “Max number of messages” thì bạn để là 0000 (không thiết lập).



c. Chỉ cho phép các tài khoản trong nhóm Admins và Giamdoc trên được sử dụng Web mail, OMA, POP3, IMAP. Các user còn lại chỉ sử dụng Webmail, POP3.

Chú ý: trong Mdeamon, tài khoản POP3 và IMAP đi chung với nhau. Nghĩa là nếu không cho user sử dụng POP3 thì user đó cũng không thể sử dụng IMAP. Do đó, không thể thực hiện được yêu cầu này. Trong trường hợp bạn muốn không cho user sử dụng POP3 thì bạn làm như sau:

Bạn vào Menu Account, chọn Account Manager (phím tắt là Alt+M), chọn vào Account muốn cấm sử dụng POP3 (ví dụ là account **nttdung**), chọn Edit. Chương trình sẽ hiện lên hộp thoại Account Editor, và bạn chọn Tab Account, trong phần POP/IMAP account information, bạn chọn vào mục “Disable POP and IMAP access for this account”. Sau đó chọn Ok để kết thúc.

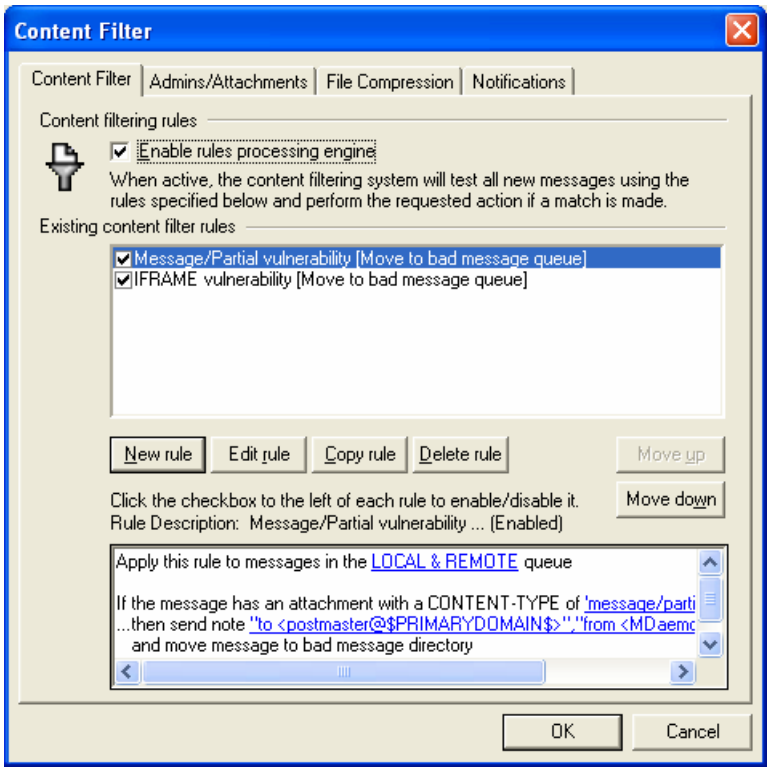


d. Dung lượng tối đa của Public Folder được lưu trên server 100M, cho phép mọi người dùng có thể sử dụng Public Folder.

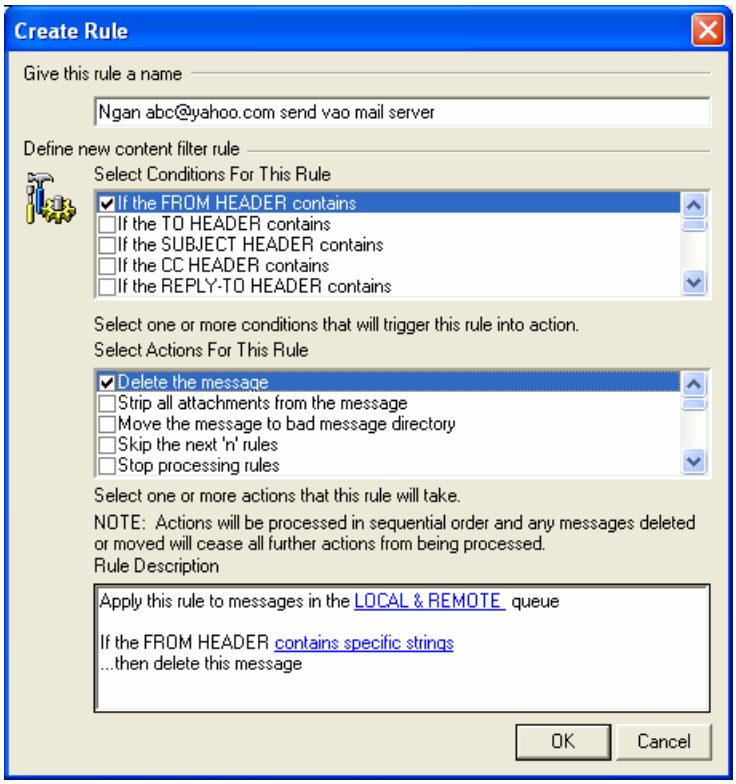
Trong Mdeamon không có Public Folder, mà chỉ có IMAP Folder.

e. Ngăn địa chỉ mail abc@yahoo.com gởi mail vào miền nội bộ, chặn tất cả email từ miền nội bộ gởi tới người dùng có địa chỉ mlbadmail@yahoo.com

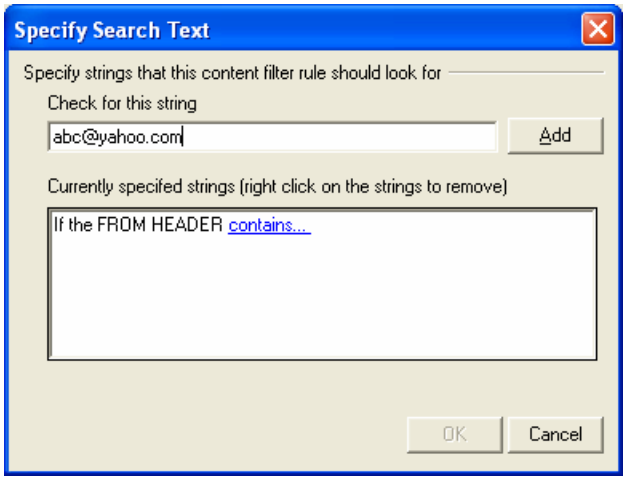
Bước 1: bạn chọn Menu Security, chọn Content Filter (phím tắt là Ctrl+F5).



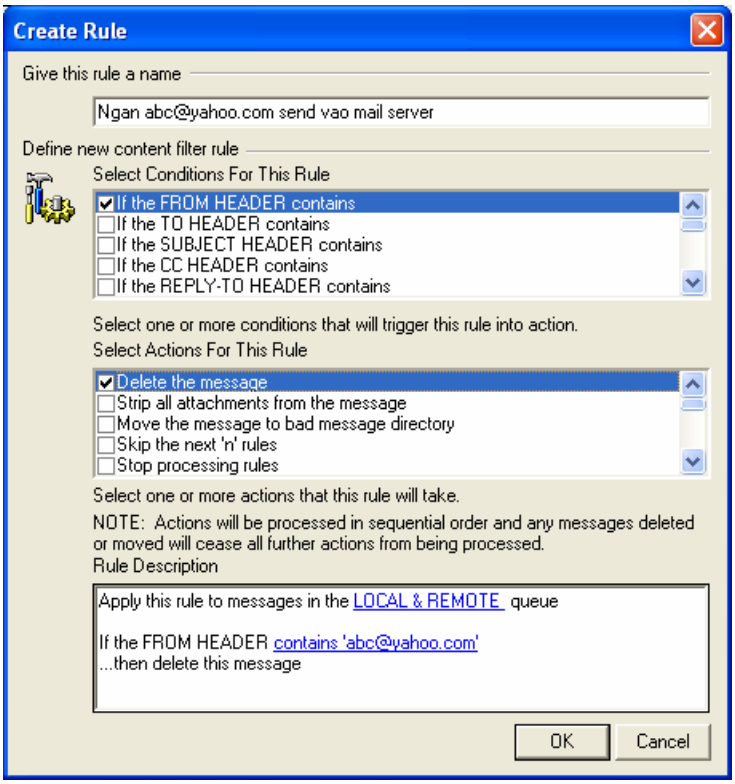
Bước 2: trong Tab Content Filter, bạn chọn nút New Rule để thiết lập Rule mới. Trong mục "Give this rule a name", bạn đặt tên cho Rule, ví dụ là "ngan abc@yahoo.com send vao mail server". Trong mục "Select Conditions for this Rule", bạn chọn vào dòng "If the FROM HEADER contains" (vì ngăn địa chỉ abc@yahoo.com gởi mail vào). Trong mục "Select Actions For this Rule", bạn chọn vào dòng "Delete the message" (sẽ xóa luôn mail abc@yahoo.com). Kết quả của việc lựa chọn sẽ được tổng kết lại trong mục "Rule Description", và bạn thấy rằng mình vẫn chưa xác định giá trị chứa trong phần "FROM HEADER". Vì vậy, bạn kích vào dòng "contain specific strings" ở trong mục Rule Description



Bước 3: hộp thoại Specify Search Text hiện lên, bạn nhập địa chỉ cần chặn (abc@yahoo.com) vào và chọn Add, sau đó chọn Ok để tắt hộp thoại này đi.



Bước 4: lúc này, kết quả trong phần Rule Description sẽ khác đi.



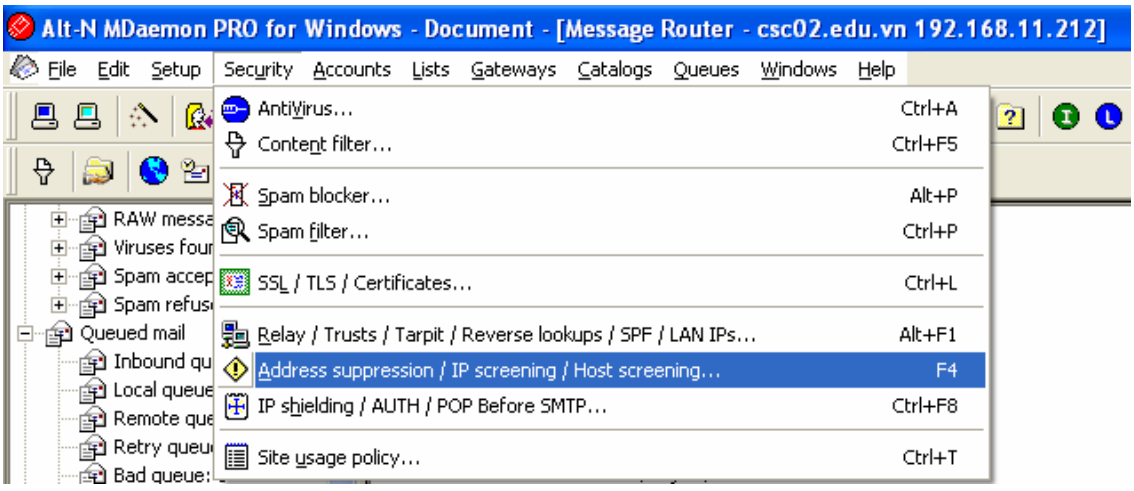
Bước 5: chọn Ok để hoàn tất việc thiết lập

Chú ý:

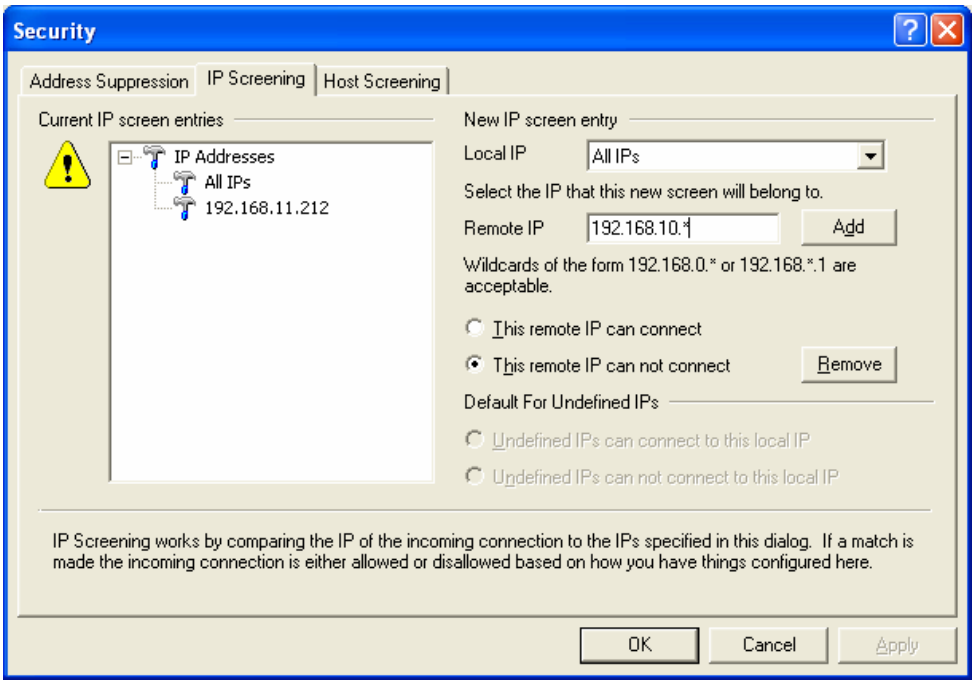
Để ngăn không cho mạng nội bộ gởi đến địa chỉ mlbadmail@yahoo.com thì bạn cũng thực hiện tương tự như trên, chỉ khác là trong mục “Select Conditions for this Rule”, bạn chọn vào dòng “If the TO HEADER contains” và sau đó nhập địa chỉ mlbadmail@yahoo.com vào.

f. Ngăn chặn địa chỉ mạng 192.168.10.0 không được connect và mail server.

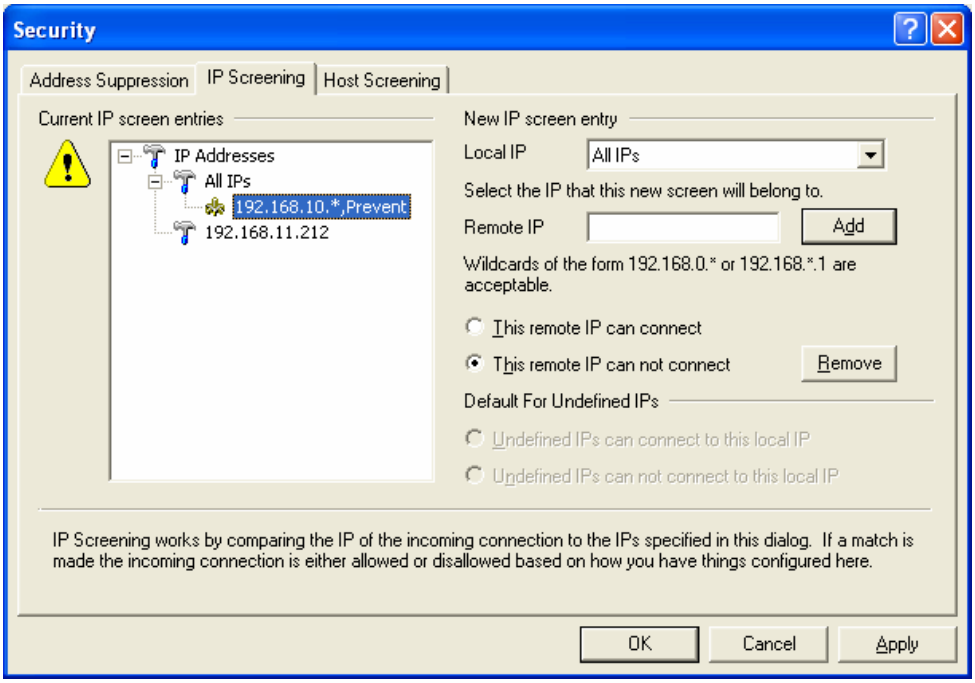
Bước 1: bạn chọn vào Menu Security, chọn “Address suppression / IP screening / Host screening…” (phím tắt là F4)



Bước 2: trong Tab IP Screening, trong mục Remote IP, bạn nhập vào 192.168.10.* (đường mạng 192.168.10.0/24) và chọn vào mục “This remote IP can not connect”, sau đó chọn Add.

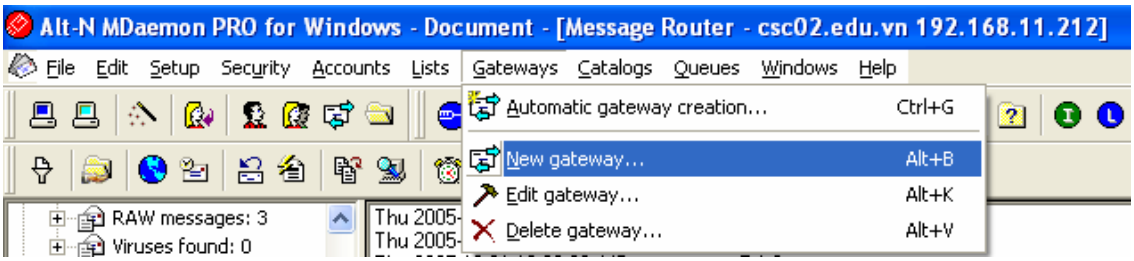


Bước 3: kết quả sẽ như hình sau, chọn Apply để thực thi và chọn tiếp Ok để tắt hộp thoại Security.

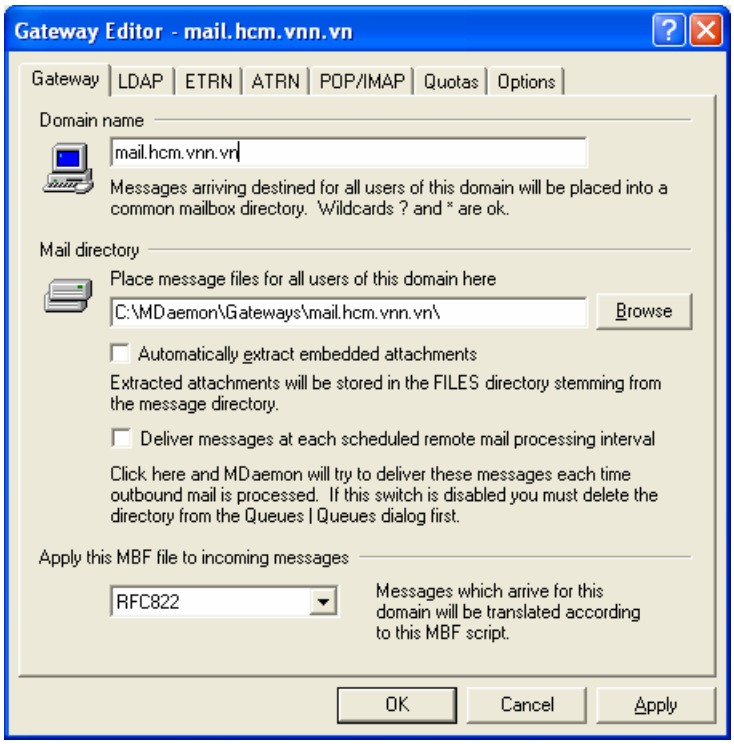


g. Khai báo Smart host có địa chỉ mail.hcm.vnn.vn để chỉ định mail gateway cho mail server nội bộ.

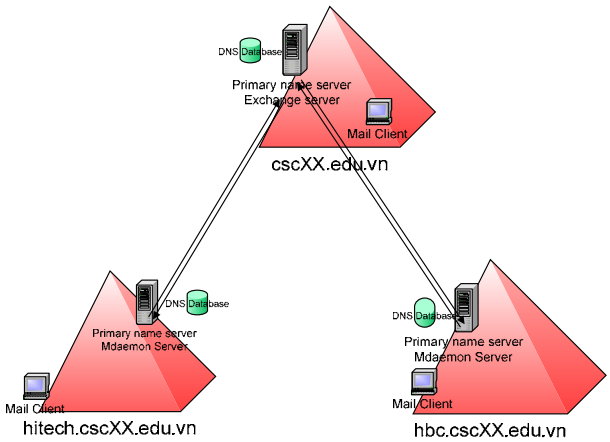
Bước 1: bạn chọn Menu Gateway, chọn “New gateway…” (phím tắt là Alt+B)



Bước 2: hộp thoại Gateway hiện ra, trong mục Domain name, bạn nhập địa chỉ Mail Gateway (mail.hcm.vnn.vn). Sau đó chọn Apply để thực thi và chọn Ok để hoàn tất việc thiết lập.



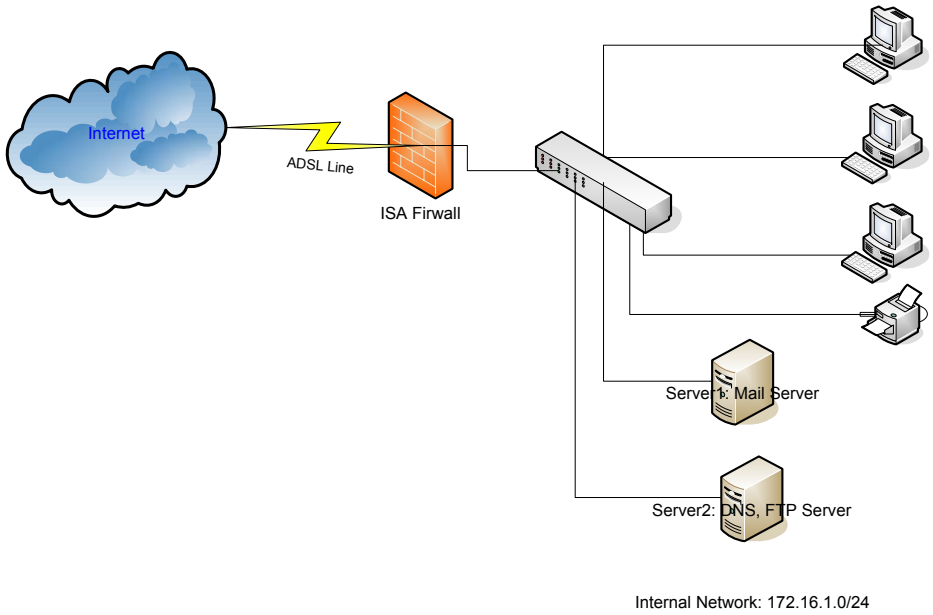
4. Bài 4: tổ chức mail cho ba miền sau có thể trao đổi mail với nhau.


DNS Database
Primary name server
Exchange server
Mail Client
cscXX.edu.vn
DNS Database
Primary name server
Mdaemon Server
Mail Client
hitech.cscXX.edu.vn
DNS Database
Primary name server
Mdaemon Server
Mail Client
hbc.cscXX.edu.vn

Bài 05
Dịch Vụ Proxy

Bài tập 05.1

Bạn là người quản trị cho một mạng máy tính cho trung tâm đào tạo tin học (có sơ đồ kết nối như hình vẽ). Máy chủ Server1 cài Win2k3 Server và cung cấp dịch vụ Mail Server. Server2 là DNS, FTP Server cho công ty, công ty thuê một tên miền "**cscXX.edu.vn"** sau đó dùng phần mềm ISA để triển khai Firewall và cung cấp dịch vụ Proxy để protect hệ thống mạng nội bộ.



1. **Bài 1: cài đặt ISA Firewall trên máy tính chủ có ít nhất hai card mạng để tổ chức hệ thống kết nối như trên sơ đồ.**

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 5 – phần IV – trang 164)

2. **Bài 2: cấu hình ISA Firewall theo các yêu cầu sau:**
   a. Cấu hình trên ISA Firewall như một Proxy Server sao cho có thể chia sẻ kết nối Internet cho các máy tính trong Internal network (sử dụng cổng 8080)

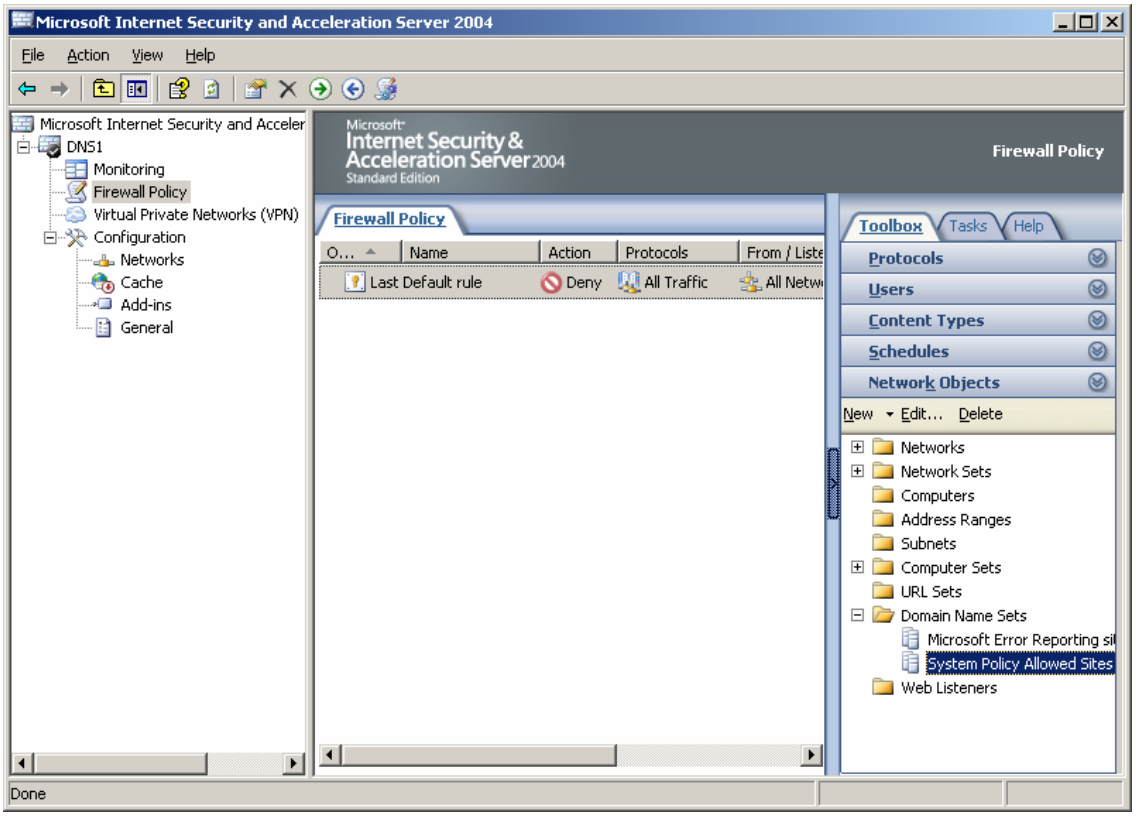
Bạn cần thực hiện 4 yêu cầu:

- Yêu cầu 1: hiệu chỉnh danh sách các trang Web được phép truy cập.
- Yêu cầu 2: enable Policy các trang Web được phép truy cập
- Yêu cầu 3: cho phép tất cả các máy tính trong mạng đều được truy cập.

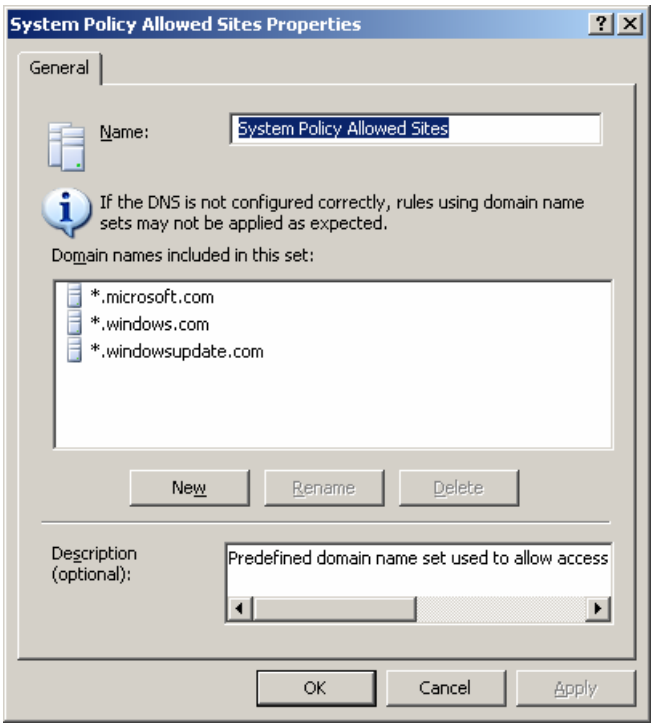
- Yêu cầu 4: cài đặt Proxy cho các máy tính trong mạng.

Yêu cầu 1: Hiệu chỉnh danh sách các trang Web được phép truy cập

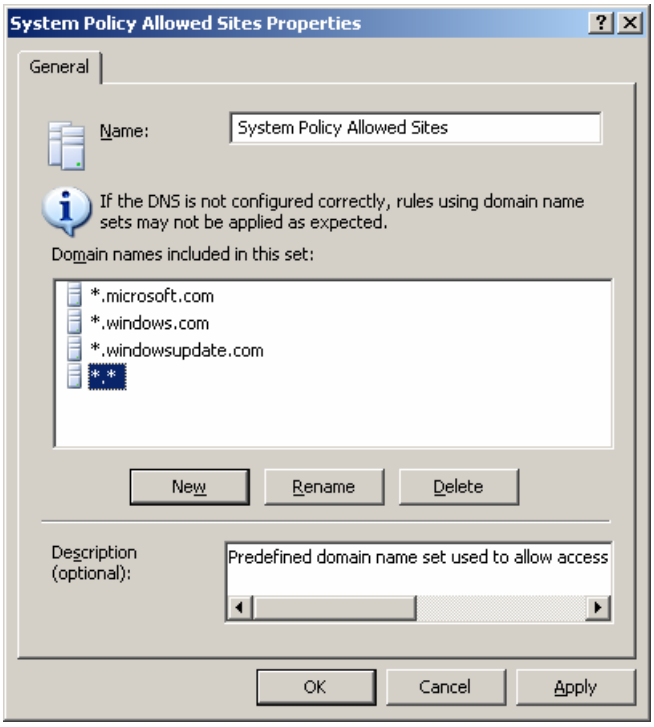
Bước 1: mở ISA Management, chọn mục Firewall Policy, ở cột bên phải, chọn ToolBox. Kích đúp chuột vào mục System Policy Allowed Sites (như hình sau)



Bước 2: mặc định, các trang Web được phép truy cập chỉ có "*.microsoft.com", "*.windows.com", "*.windowsupdate.com". Do đó, bạn chọn New và thêm vào "*.*" (tất cả các trang).

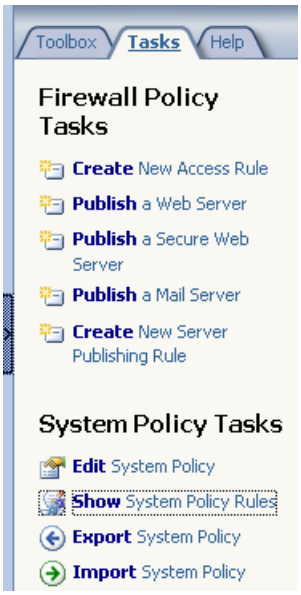


Bước 3: sau khi thực hiện xong, bạn sẽ thấy như sau:

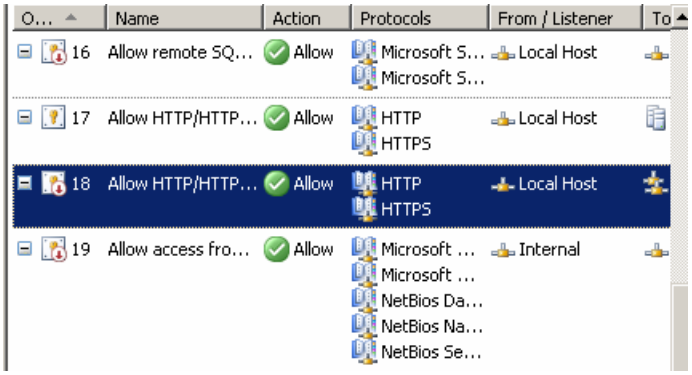


Yêu cầu 2: Enable Policy các trang Web được phép truy cập

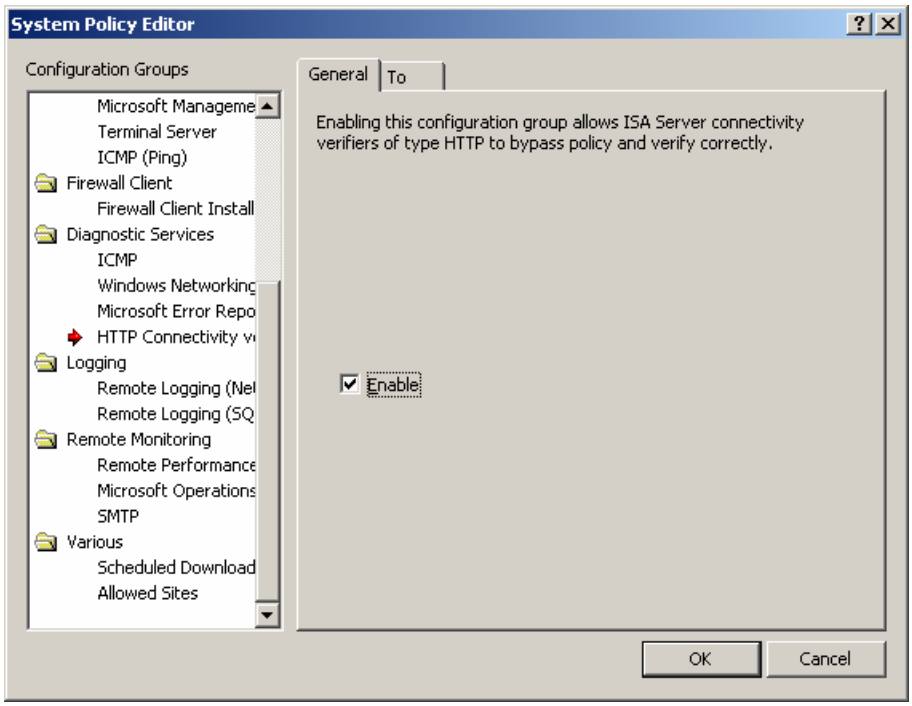
Bước 1: chọn mục Firewall Policy, ở cột bên phải, chọn Tasks, sau đó chọn mục Show System Policy Rules.



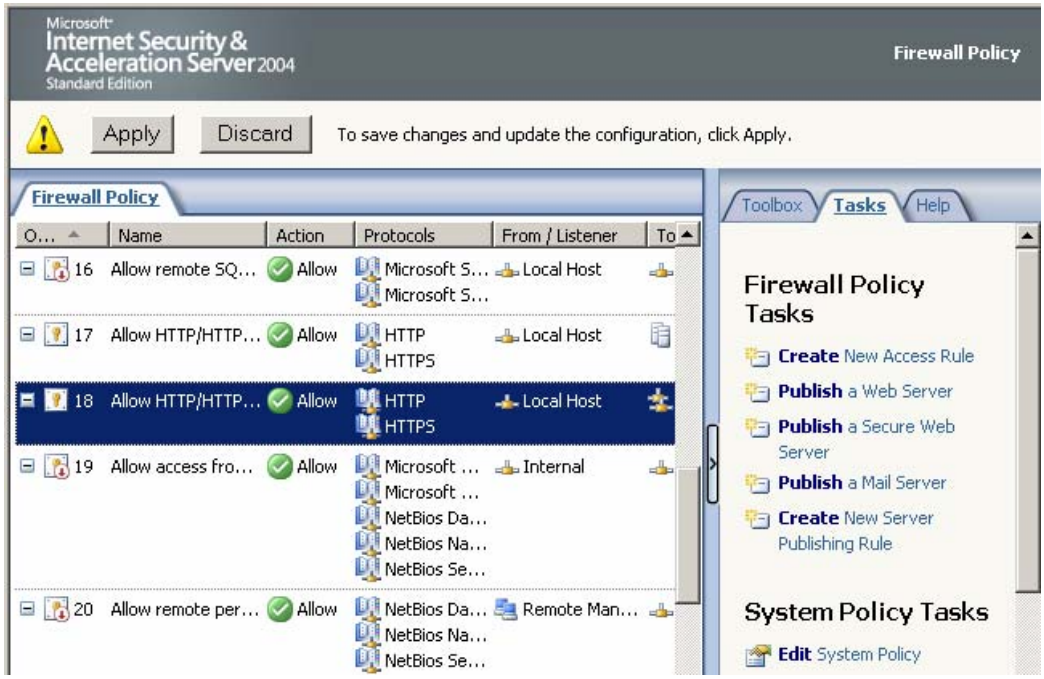
Bước 2: kích đúp chuột trái vào mục 18 (Allow HTTP/HTTPS)



Bước 3: Chọn vào mục Enable, sau đó chọn Ok

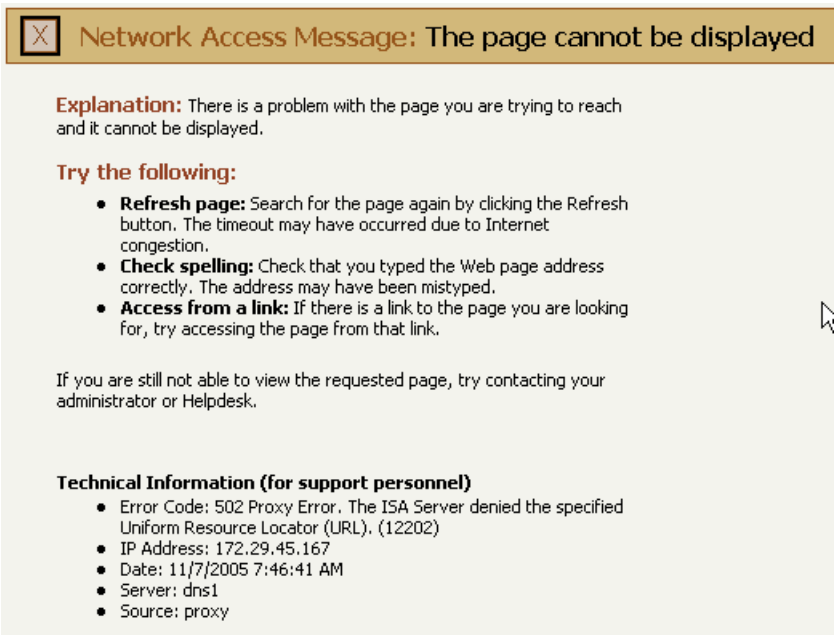


Bước 4: sau mỗi lần thay đổi, bạn sẽ thấy nút Apply và Discard như hình sau. Nếu muốn cập nhật ISA ngay lập tức thì bạn có thể chọn nút Apply, nếu không thì bạn có thể thực hiện xong toàn bộ cấu hình cần thay đổi và chọn nút Apply.

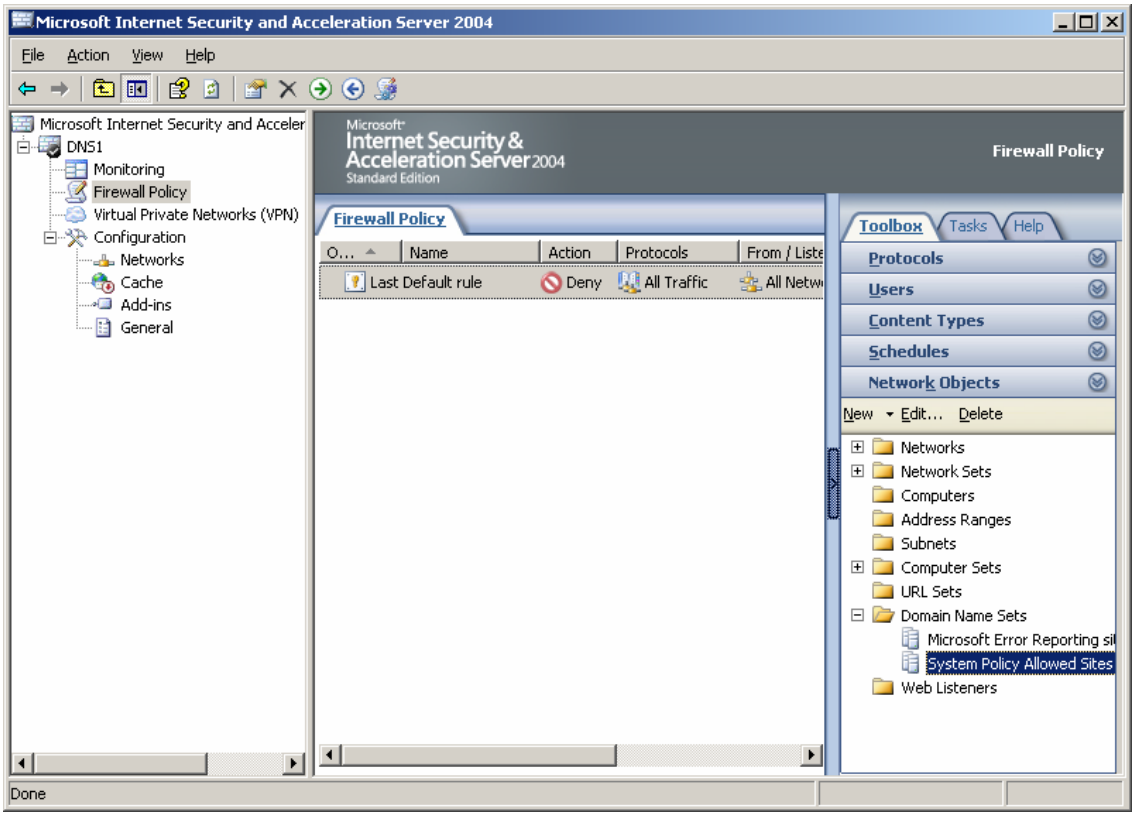


Yêu cầu 3: Cài đặt cho phép các máy trong mạng nội bộ được phép truy cập.

Sau khi bạn thực hiện xong yêu cầu 1 và yêu cầu 2, nếu bạn bỏ qua yêu cầu 3 và thực hiện yêu cầu 4, thì các máy client khi truy cập thông qua ISA sẽ thấy thông báo sau:

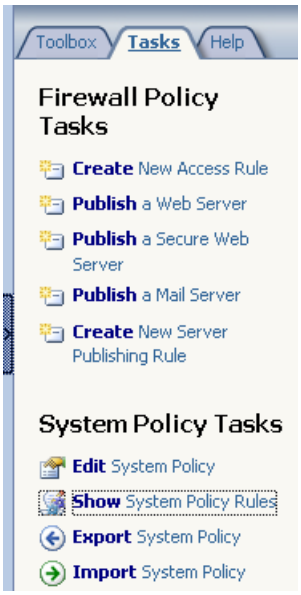


Nguyên nhân của thông báo này là vì trong mục Firewall Policy, bạn thấy chỉ có duy nhất một Rule, vào Rule đó có tác dụng **DENY** tất cả thông tin đi qua Proxy.



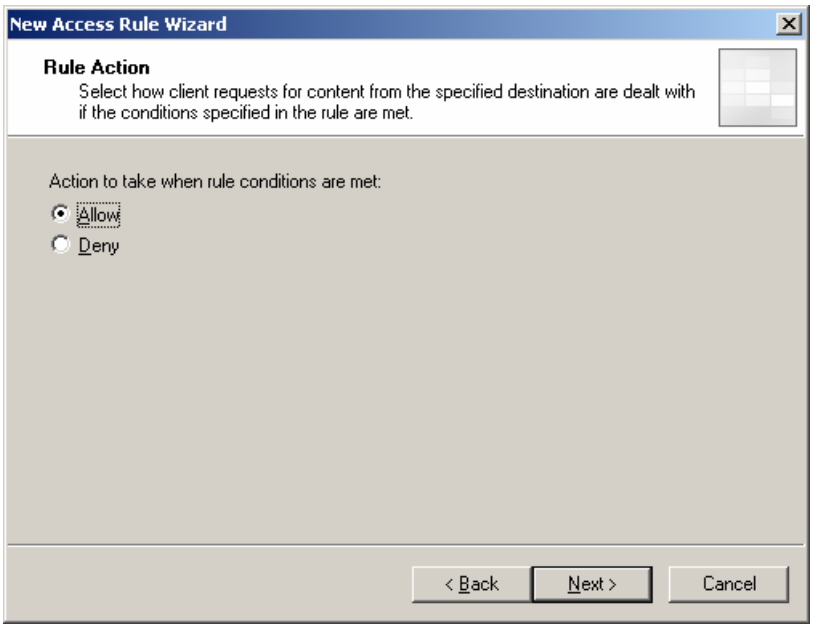
Bạn thực hiện yêu cầu 3 như sau:

Bước 1: trong chọn lựa Tasks ở cột bên phải, bạn chọn Create New Access Rule

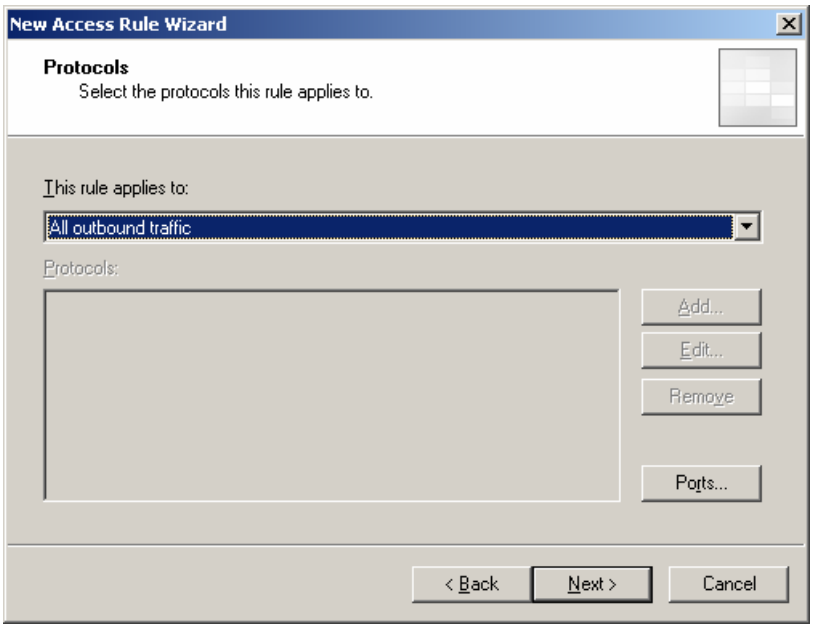


Bước 2: nhập tên cho Rule, trong ví dụ này là "Chia se ket noi Internet". Sau đó chọn Next

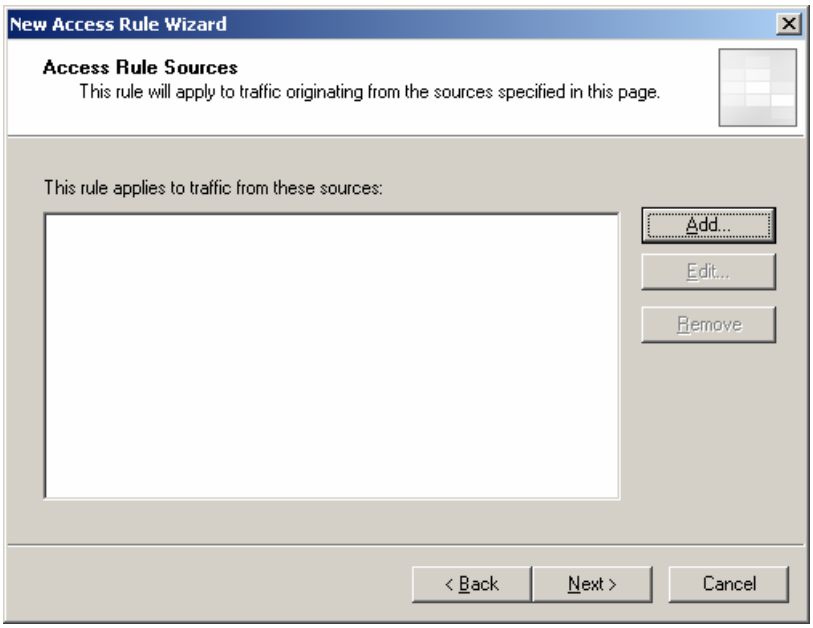
Bước 3: chọn hoạt động tiếp theo nếu như gói tin phù hợp với điều kiện bạn đưa ra. Trong ví dụ này là bạn muốn các máy đều được phép truy cập internet. Nên bạn sẽ chọn mục Allow. Sau đó chọn Next



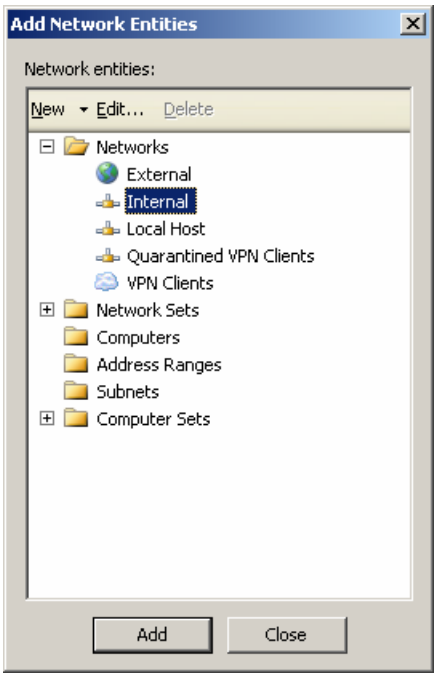
Bước 4: bạn muốn áp dụng luật này đối với các gói tin thuộc giao thức (Protocol) nào ? Vì đang thực hiện việc chia sẻ Internet cho các máy trong mạng nội bộ nên ta sẽ áp dụng luật này cho tất cả các gói tin đi ra (không phân biệt giao thức nào). Do đó, chọn mục All outbound traffic và chọn Next



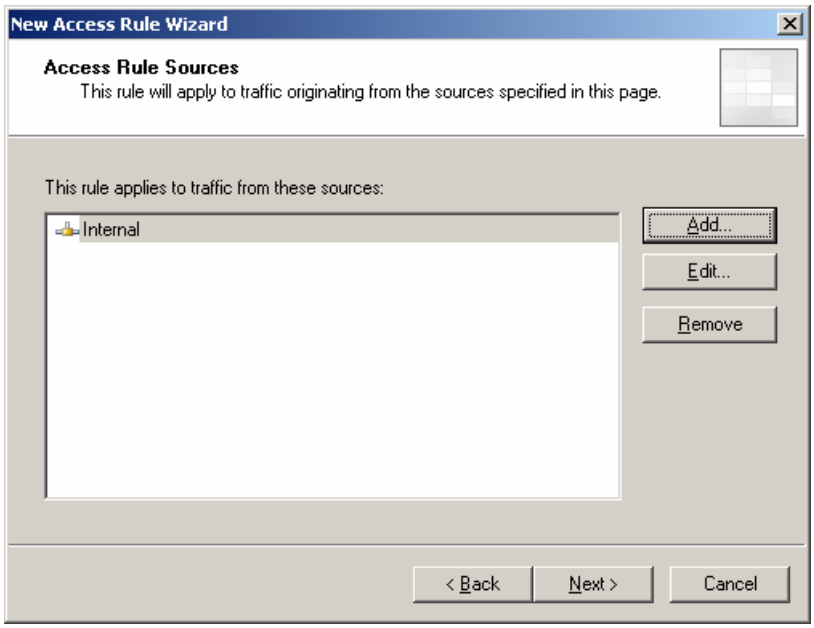
Bước 5: tuy áp dụng các gói tin không phân biệt kiểu giao thức, nhưng ta cũng cần xác định địa chỉ nguồn và địa chỉ đích. Vì các máy Client truy cập internet thông qua ISA proxy, nên trong mục Source, bạn sẽ chọn là Internal Network. Để làm được điều này thì bạn chọn Add



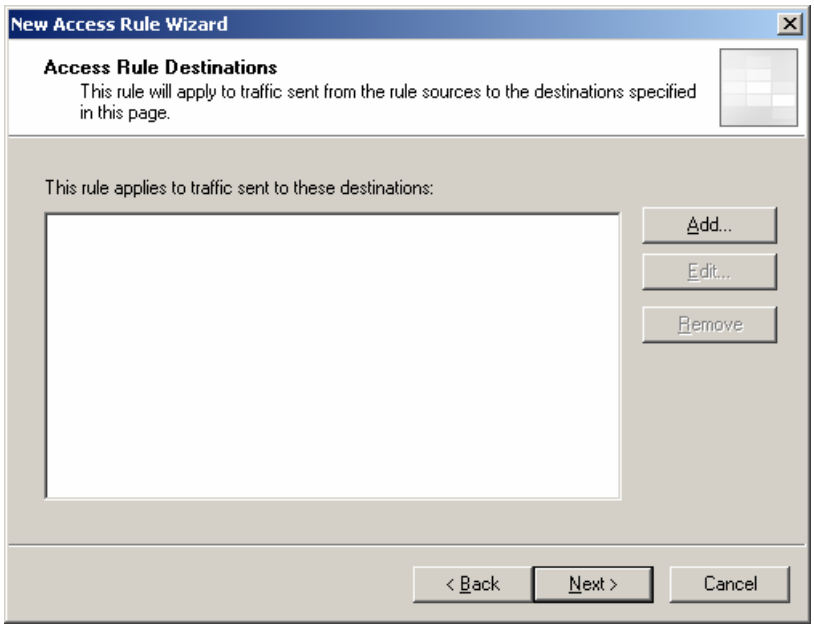
Bước 6: chọn mục Networks, chọn Internal, sau đó chọn Add



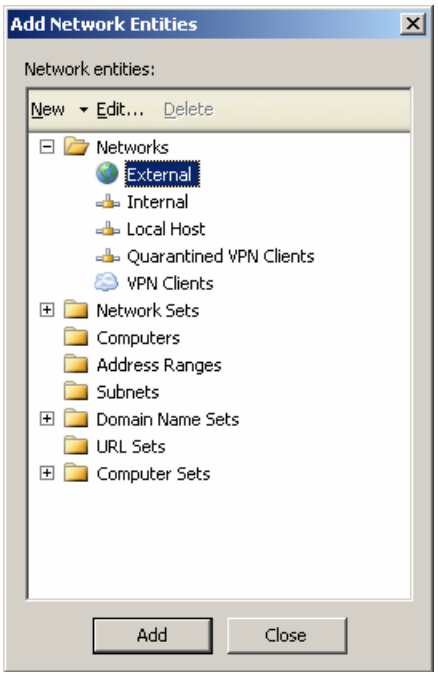
Bước 7: chọn Next để tiếp tục



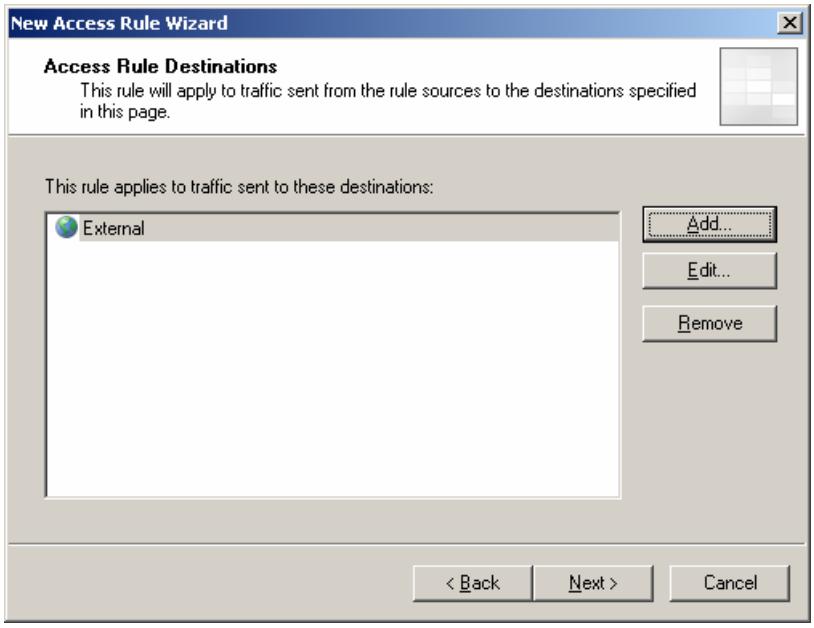
Bước 8: nhập địa chỉ đích của gói tin (trong ví dụ này là External)



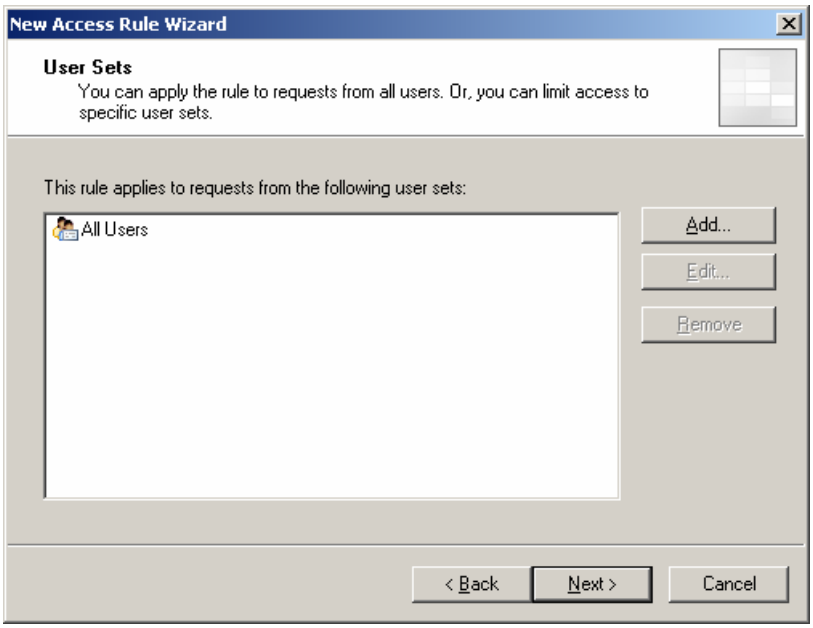
Bước 9: chọn mục Networks, Externals sau đó chọn Add



Bước 10: chọn Next để tiếp tục

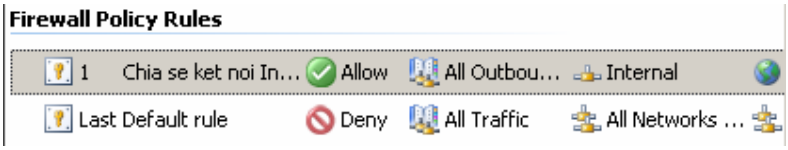


Bước 11: chọn lựa các user bị áp dụng luật này. Sau đó chọn Next

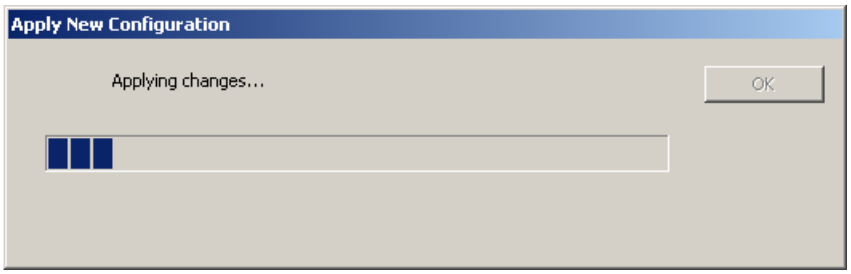


Bước 12: bạn kiểm tra lại thông tin lần nữa. Nếu thấy đúng thì Finish để hoàn tất việc thiết lập RULE.

Bước 13: sau khi đã cấu hình xong, bạn sẽ thấy trong Firewall Policy Rules có thêm một Rule nữa và Rule được tạo ra sẽ được áp dụng trước Rule mặc định.



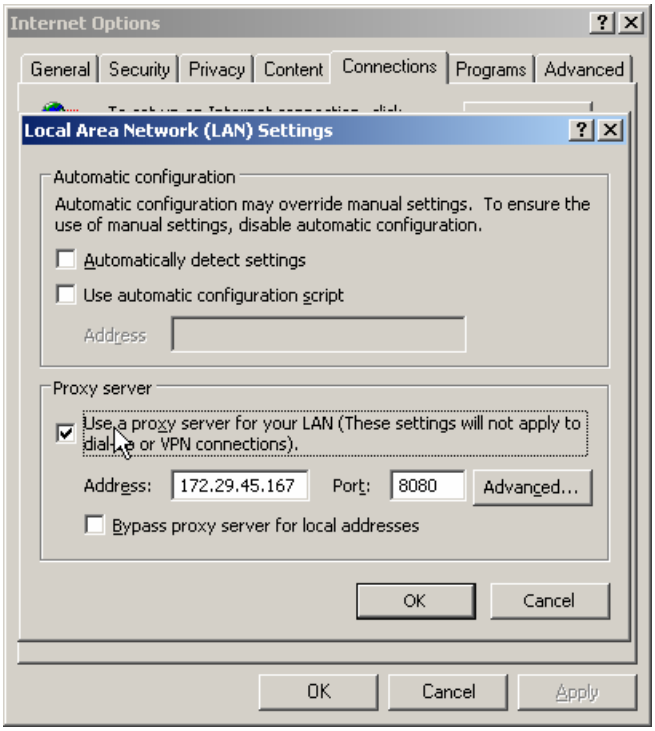
Bước 14: bạn chọn Apply để thực thi các thay đổi.



Sau khi cập nhật sự thay đổi, bạn đã có thể thực hiện cấu hình Proxy cho các máy Client.

Yêu cầu 4: Cấu hình Proxy cho các máy Client.

Nếu các máy truy cập bằng Internet Explore (IE) thì bạn chọn mục Tools → Internet Options. Sau đó chọn Tab Connections, chọn mục Lan Settings. Trong mục Proxy Server, chọn mục "Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)" và điền địa chỉ của máy cài đặt ISA, Port đi qua (trong ví dụ này là 172.29.45.167:8080)



b. Cấm các máy tính trong mạng 192.168.XX.0/24 truy xuất Internet.

Bạn có thể thực hiện điều này thông qua 2 yêu cầu

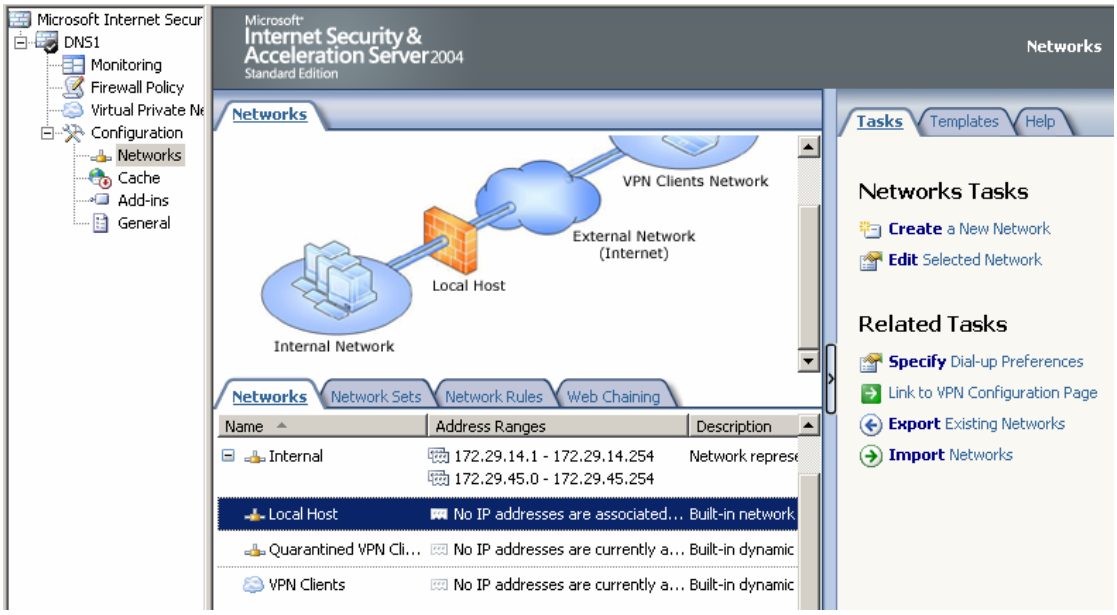
- Yêu cầu 1: Tạo một đường mạng hoặc một Subnet mới
  - Cách 1: Tạo đường mạng mới
  - Cách 2: Tạo một Subnet mới
- Yêu cầu 2: Thiết lập Rule.

- Cách 1: Hiệu chỉnh Rule ở câu trước
- Cách 2: Tạo Rule mới.

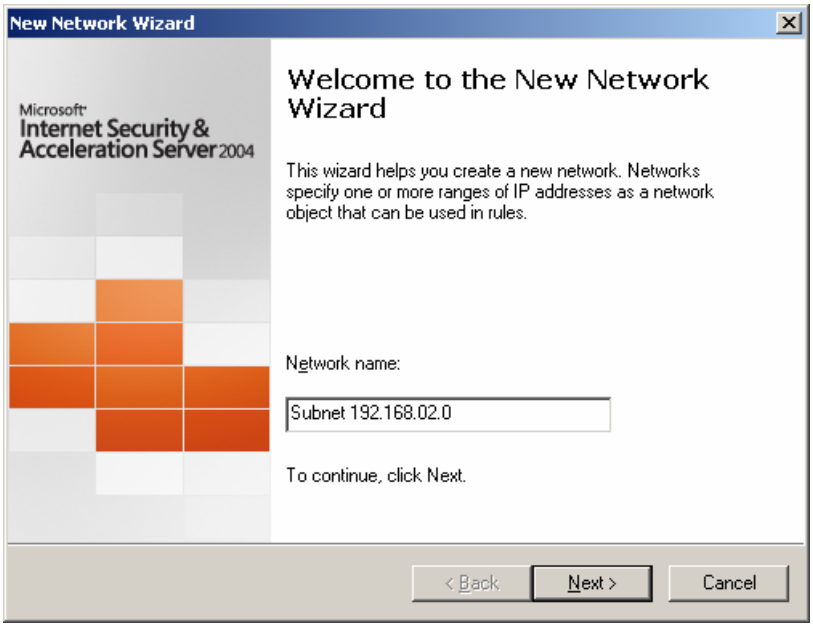
Hướng dẫn thực hiện theo cách 1 ở cả 2 yêu cầu:

Yêu cầu 1: Tạo một network mới

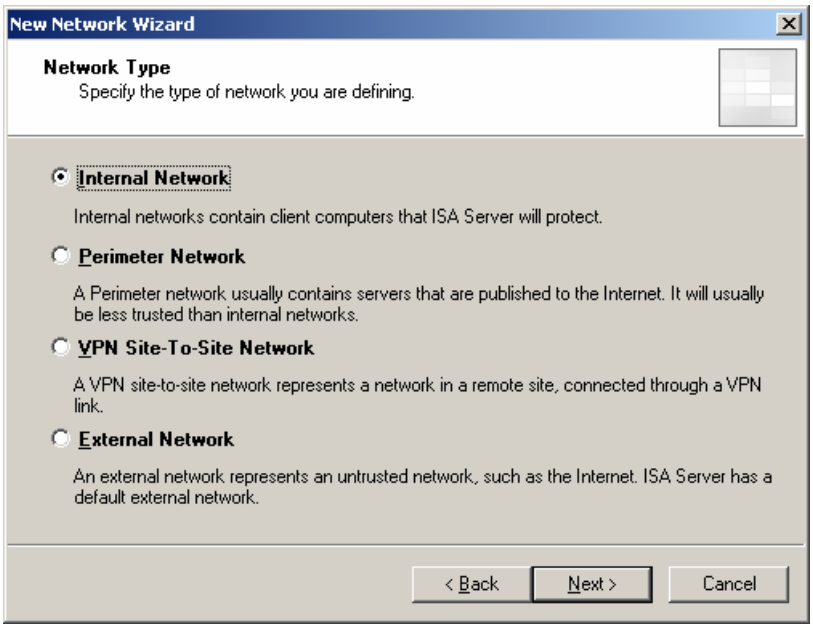
Bước 1: chọn mục Networks, chọn mục Tasks ở cột bên phải. Sau đó chọn "Create a New network"



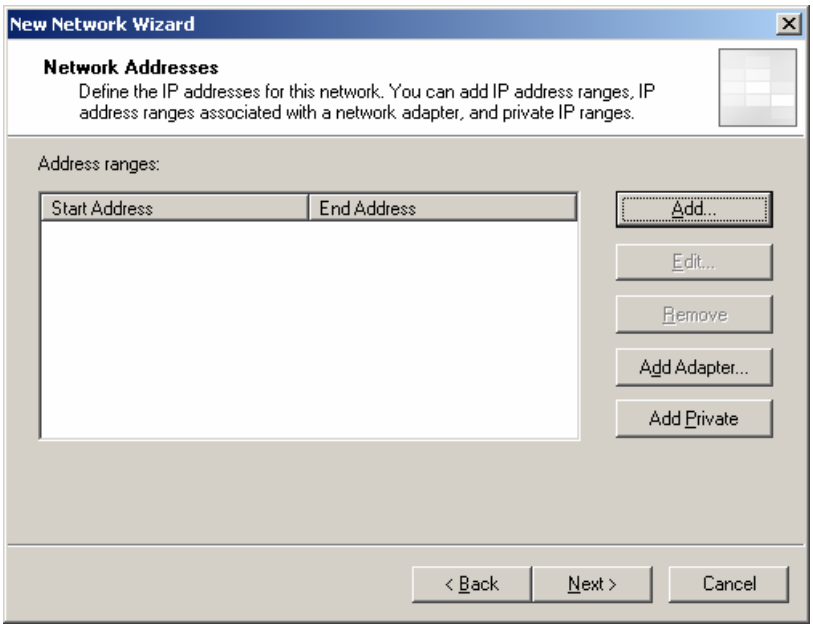
Bước 2: nhập tên cho Network này (ví dụ là "Subnet 192.168.02.0") sau đó chọn Next



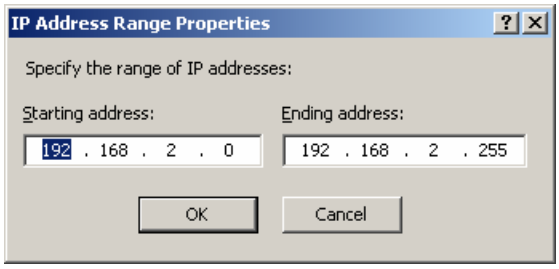
Bước 3: đường mạng đó thuộc phạm vi nào. Trong ví dụ này là Internal (đường mạng bên trong). Sau đó chọn Next



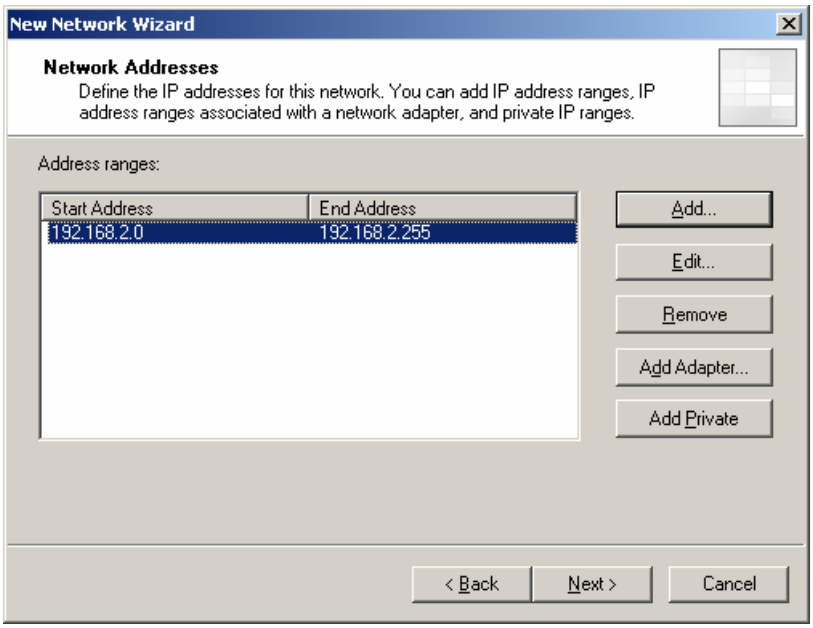
Bước 4: nhập giá trị đường mạng. Chọn nút Add để thêm vào giá trị đường mạng



Bước 5: nhập địa chỉ đầu và địa chỉ cuối của đường mang, sau đó chọn Ok.



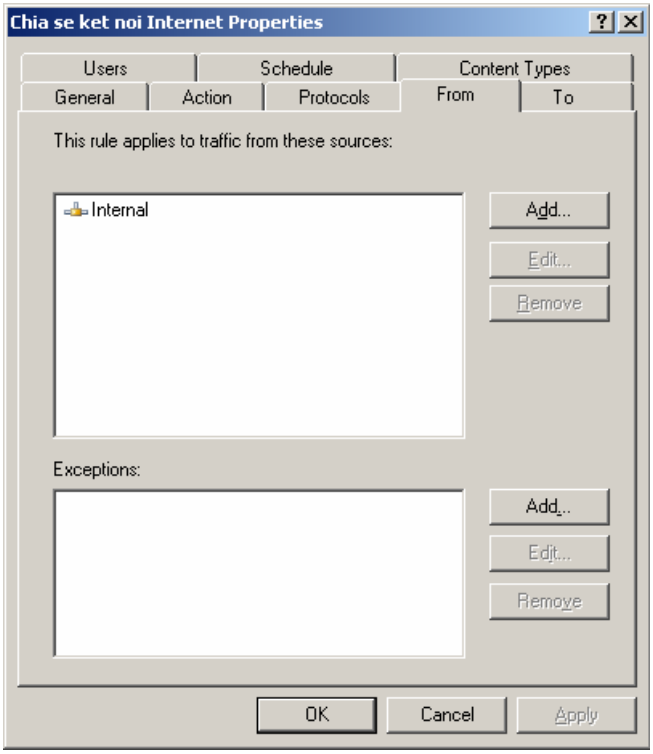
Bước 6: sau khi nhập xong thì bạn sẽ thấy kết quả như sau. Nếu bạn muốn thêm đường mạng nữa thì chọn nút Add, nếu không thì chọn Next để tiếp tục



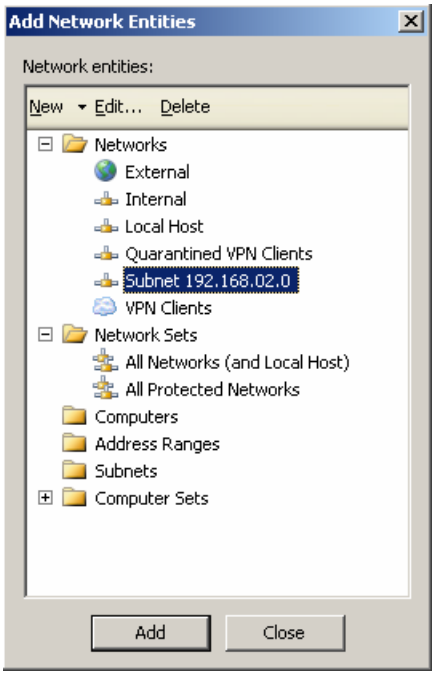
Bước 7: kiểm tra thông tin lại một lần nữa và chọn Finish để hoàn tất việc thiết lập

Yêu cầu 2: Hiệu chỉnh Rule trước để ngăn cấm

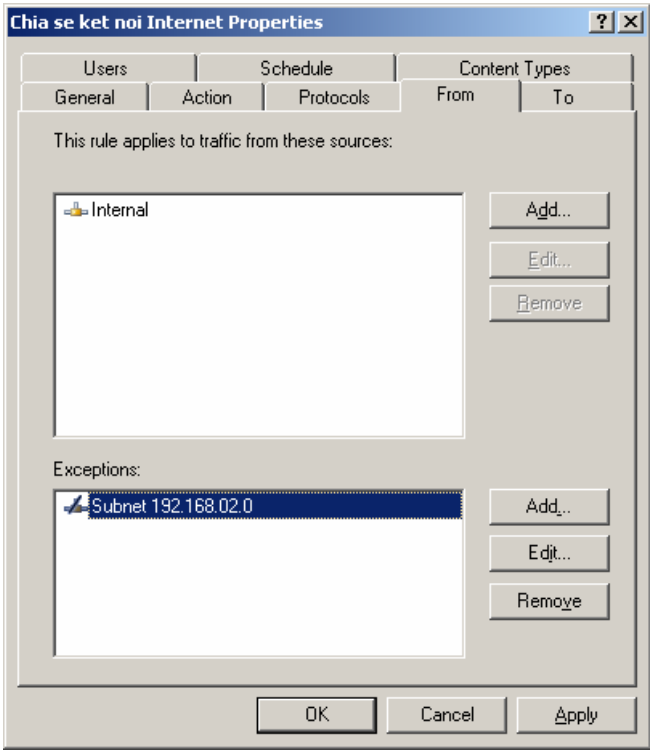
Bước 1: kích đúp chuột trái vào Rule trước ("Chia se ket noi Internet"), sau đó chọn Tab From



Bước 2: vì muốn ngăn cấm đường mạng 192.168.2.0 nên trong mục Exceptions bạn sẽ thêm đường mạng này vào. Điều này có ý nghĩa là áp dụng đối với tất cả các đường mạng Internet, ngoại trừ đường mạng 192.168.2.0. Chọn vào nút Add ở mục Exceptions

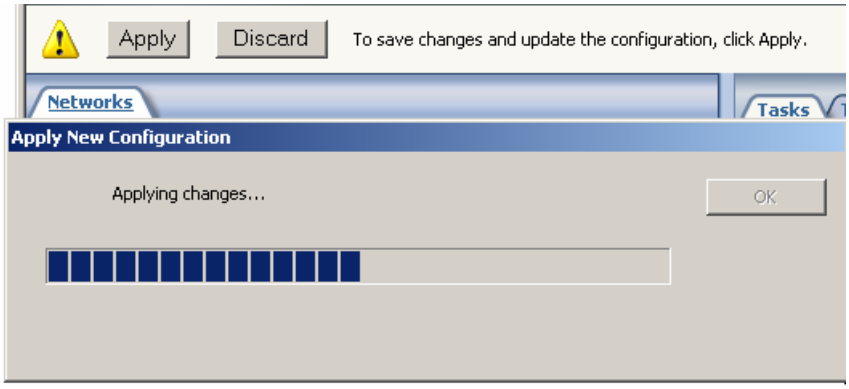


Bước 3: chọn mục Networks, chọn vào đường mạng mới tạo ra ("Subnet 192.168.02.0") sau đó chọn Add. Bạn sẽ thấy kết quả như sau:



Bước 4: chọn Ok để tắt. Bạn sẽ thấy kết quả như sau:

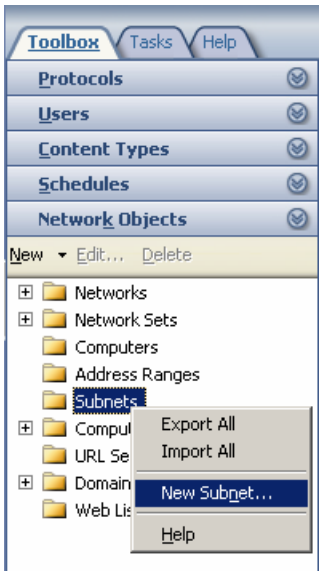
Bước 5: chọn vào Apply để hoàn tất việc thiết lập



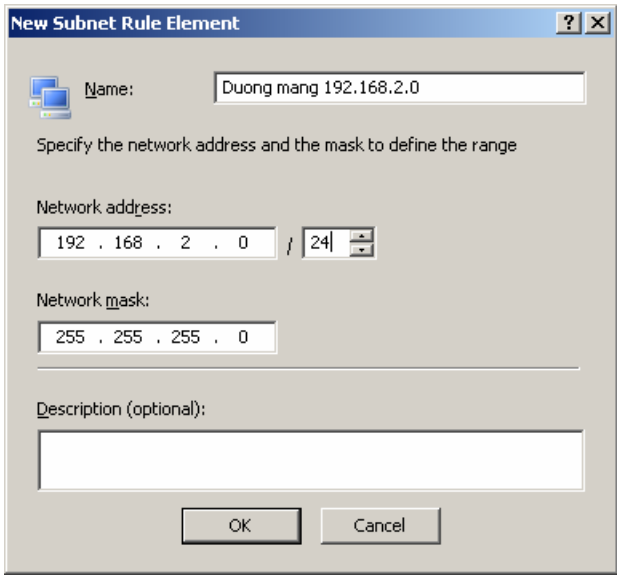
<u>Hướng dẫn thực hiện theo cách 2 ở cả 2 yêu cầu:</u>

<u>Yêu cầu 1</u>: Tạo một Subnet mới

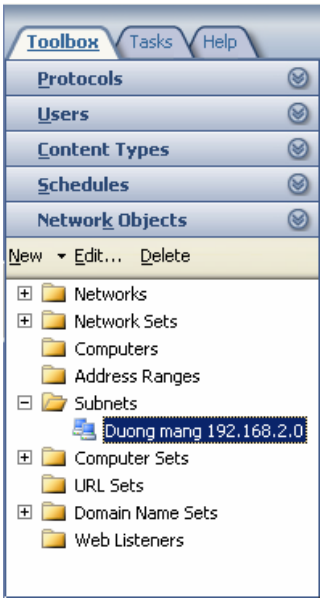
Bước 1: chọn mục Firewall Policy, ở cột bên tay phải, chọn mục Toolbox. Sau đó kích chuột phải vào mục Subnets, chọn New Subnet…



Bước 2: đặt tên của Subnet, giá trị đường mạng và Subnetmask của đường mạng đó, Sau đó chọn Ok. (như hình sau)

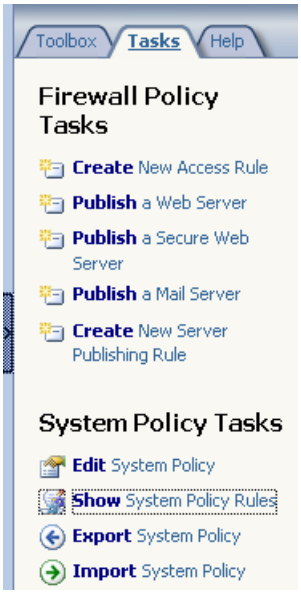


Bước 3: kết quả sau khi tạo Subnet mới.



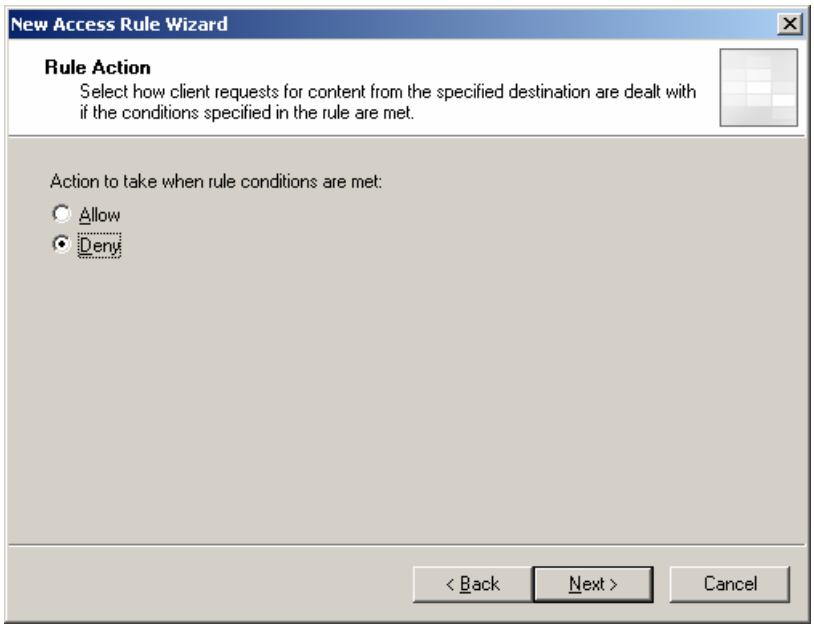
Yêu cầu 2: Tạo một Rule mới

Bước 1: trong Firewall Policy, chọn lựa Tasks ở cột bên phải, bạn chọn Create New Access Rule

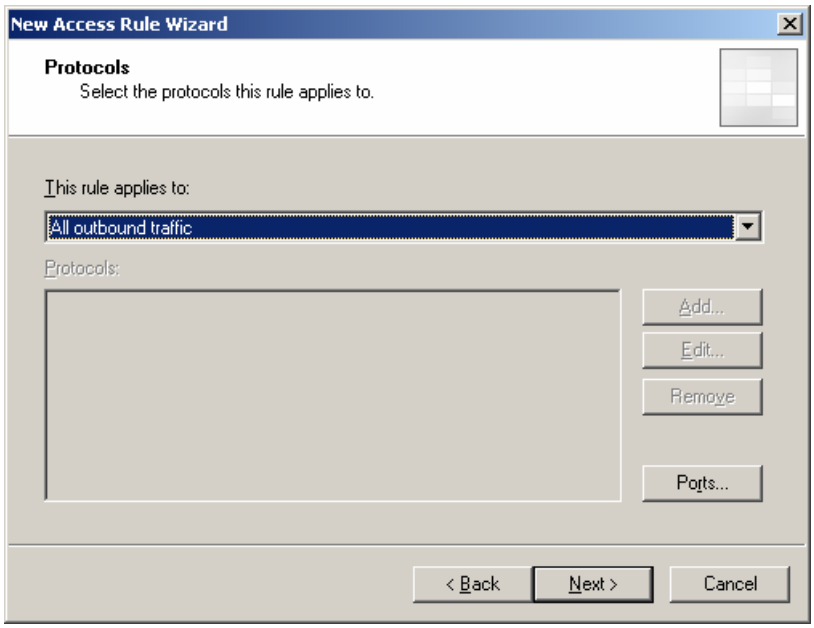


Bước 2: đặt tên cho Rule (ví dụ: “Chan duong mang 192.128.2.0”), sau đó chọn Next

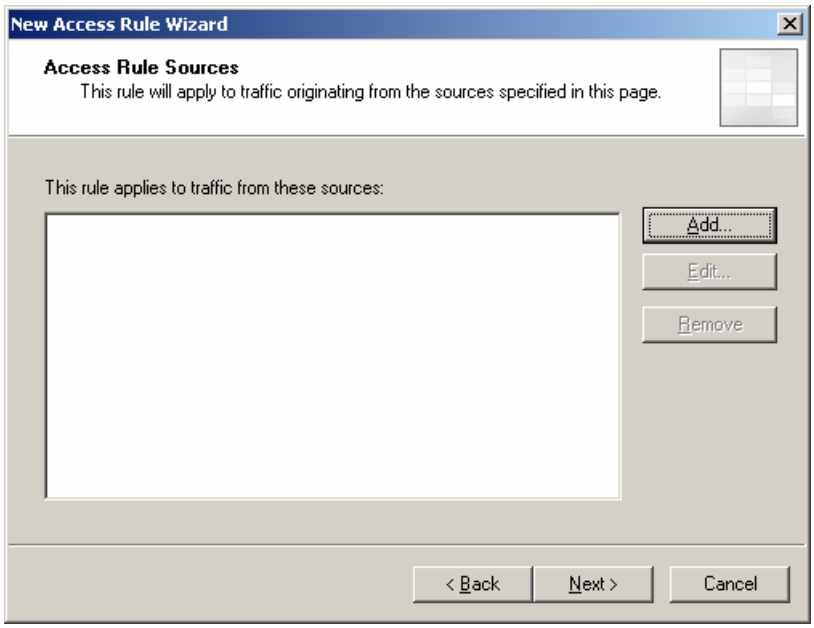
Bước 3: chọn Deny (vì đang muốn không cho đường mạng truy cập), sau đó chọn Next



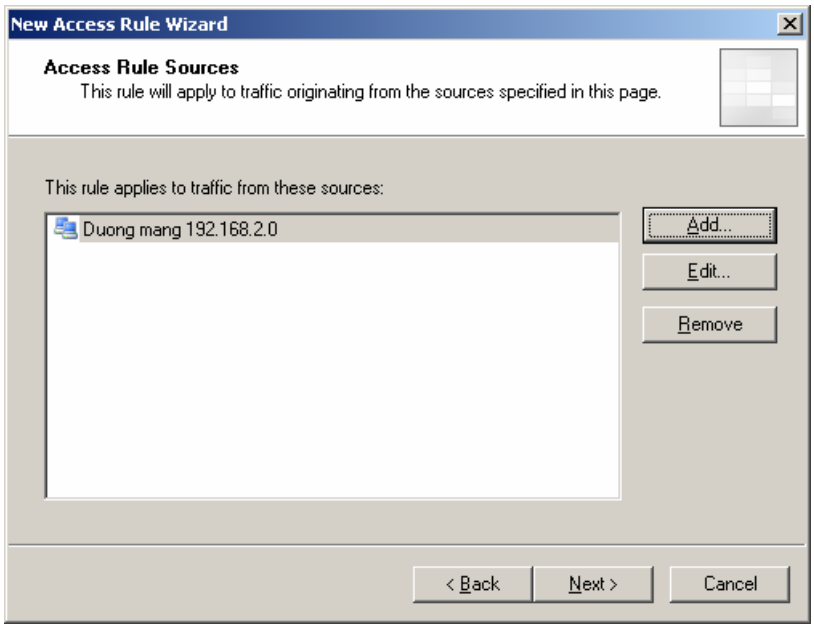
Bước 4: chọn All outbound traffic (với bất kỳ giao thức nào), sau đó chọn Next



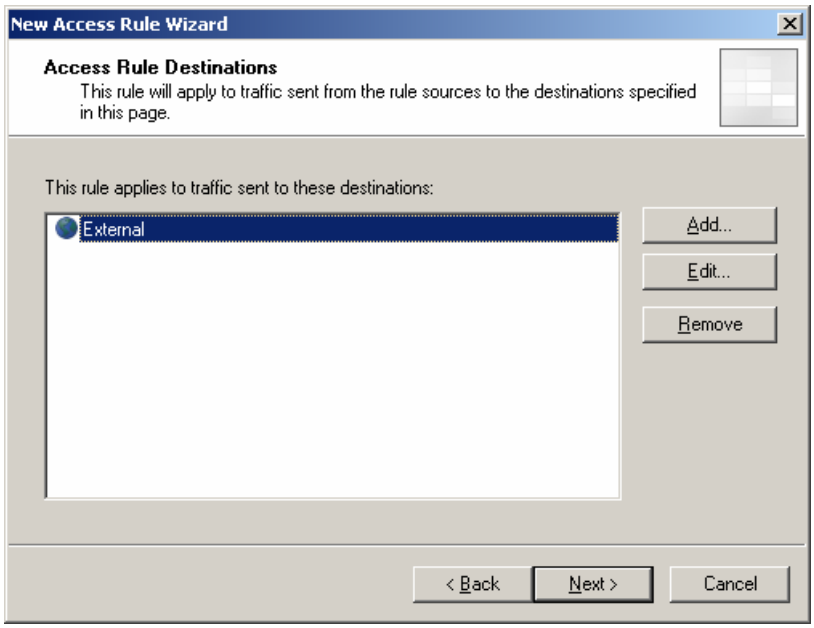
Bước 5: chọn Add để thêm đường mạng vào



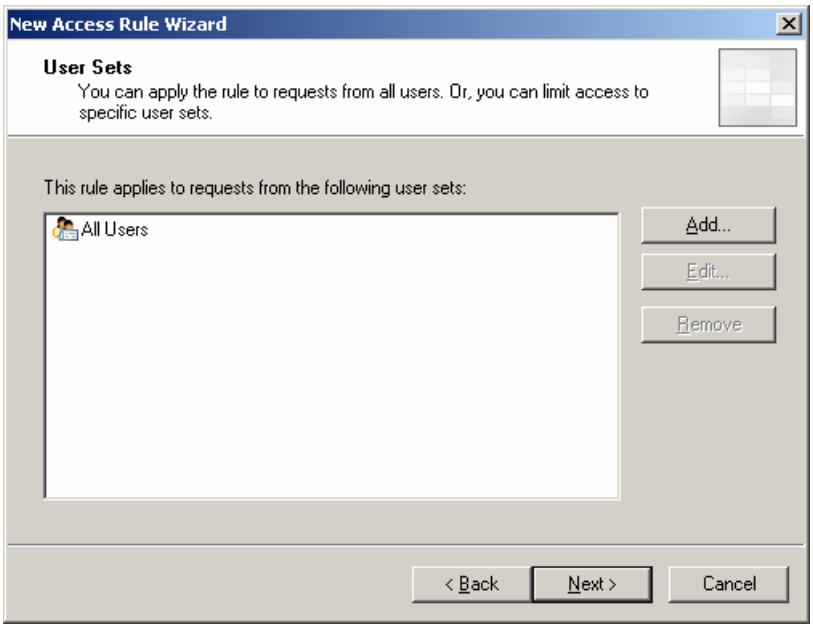
Bước 6: sau khi thêm vào



Bước 7: chọn đường mạng đích là External, chọn Next để tiếp tục



Bước 8: áp dụng đối với tất cả các user, chọn Next để tiếp tục



Bước 9: kiểm tra lại thông tin của Rule trước khi hoàn tất. Chọn Finish để kết thúc

Bước 10: chọn Apply để hoàn tất việc thiết lập.

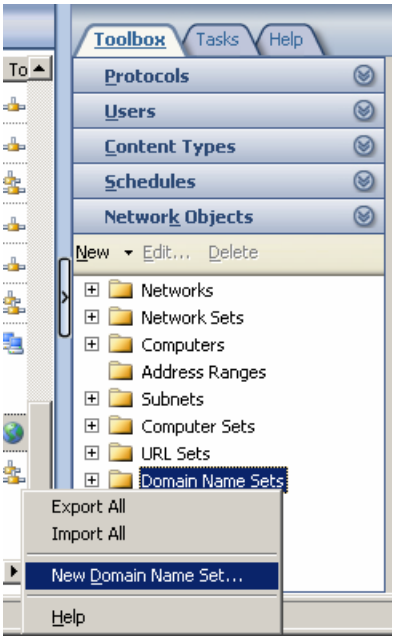
c. Cho phép tất cả các máy tính trong mạng được truy xuất Internet nhưng trong giờ hành chánh không được truy xuất vào các trang như: *.yahoo.com, *.vnn.vn, *.vnexpress.net.

Để thực hiện điều này, bạn thực hiện các yêu cầu sau:

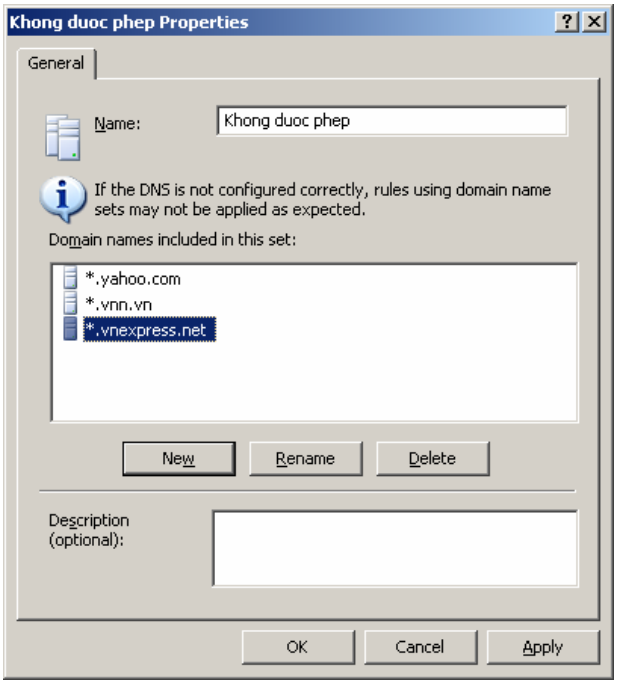
- Yêu cầu 1: tạo một Domain Set (chứa các trang Web cần cấm)
- Yêu cầu 2: tạo Rule để cấm
- Yêu cầu 3: chọn thời gian áp dụng cho Rule này.

Yêu cầu 1: Tạo một Domain Set.

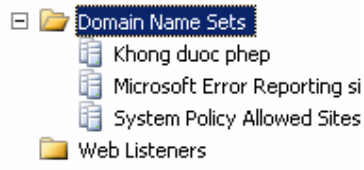
Bước 1: trong Firewall Policy, chọn Toolbox, kích chuột phải vào mục Domain Name Sets, chọn mục New Domain Name Set… (như hình sau).



Bước 2: nhập tên cho Domain Name Set, sau đó chọn nút New để thêm các địa chỉ Domain cần thực hiện.

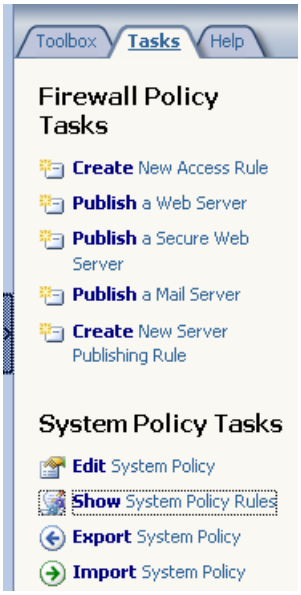


Bước 3: sau khi nhập xong, chọn Ok để hoàn tất việc thiết lập Domain Name Set mới.



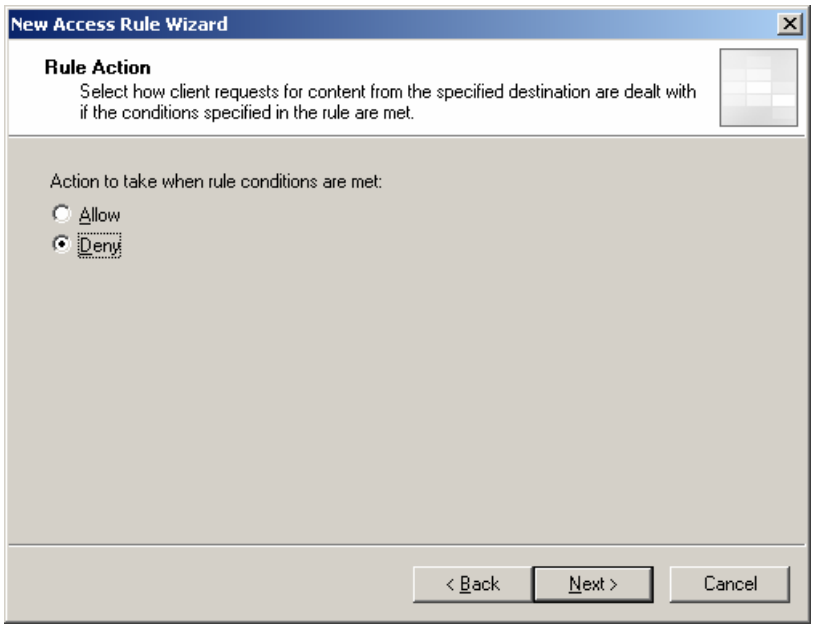
Yêu cầu 2: Tạo Rule để cấm

Bước 1: trong Firewall Policy, chọn lựa Tasks ở cột bên phải, bạn chọn Create New Access Rule

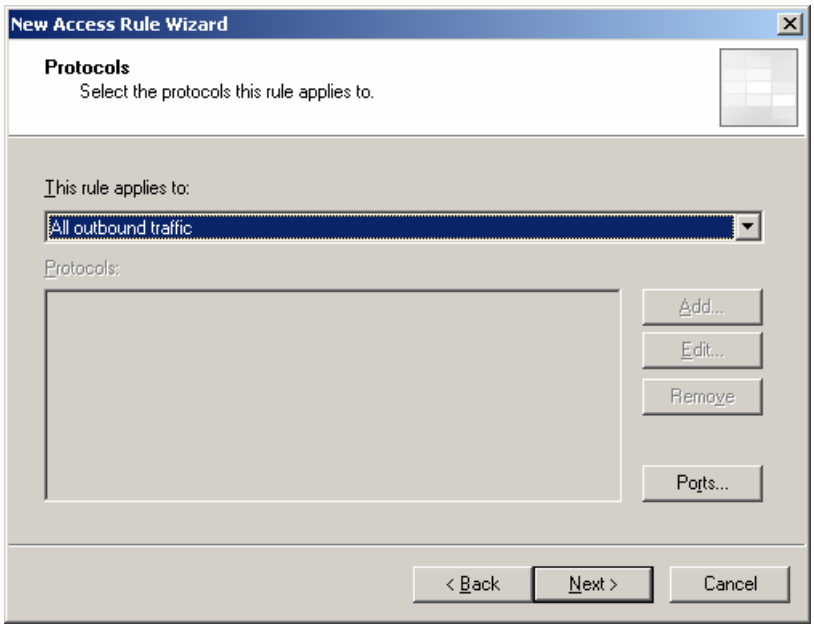


Bước 2: nhập tên cho Rule mới

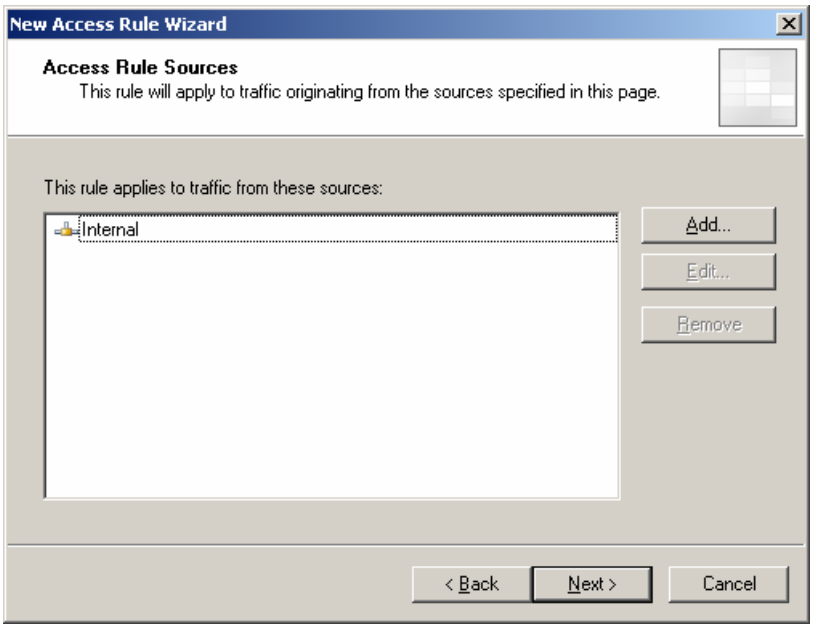
Bước 3: chọn hành động của Rule nếu gói tin phù hợp với yêu cầu



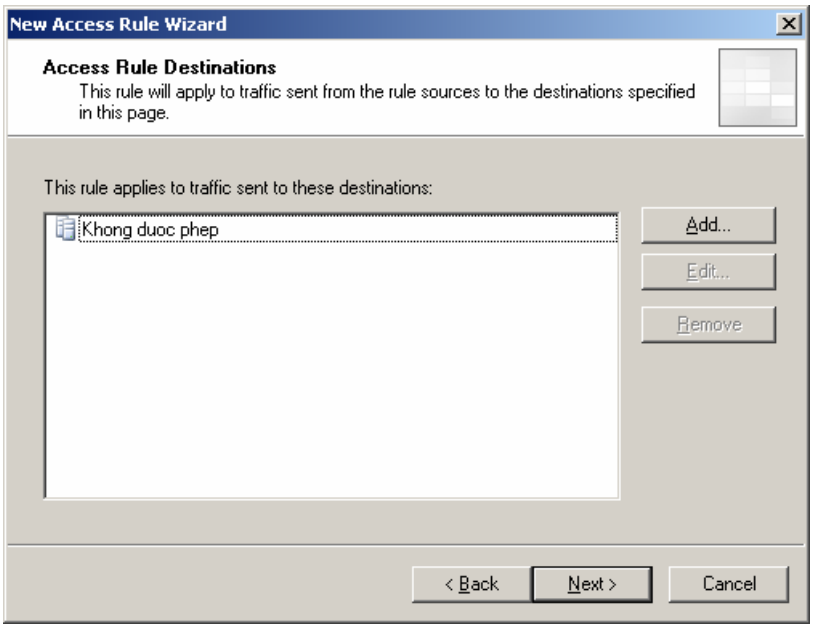
Bước 4: chọn các giao thức sẽ áp dụng luật này.



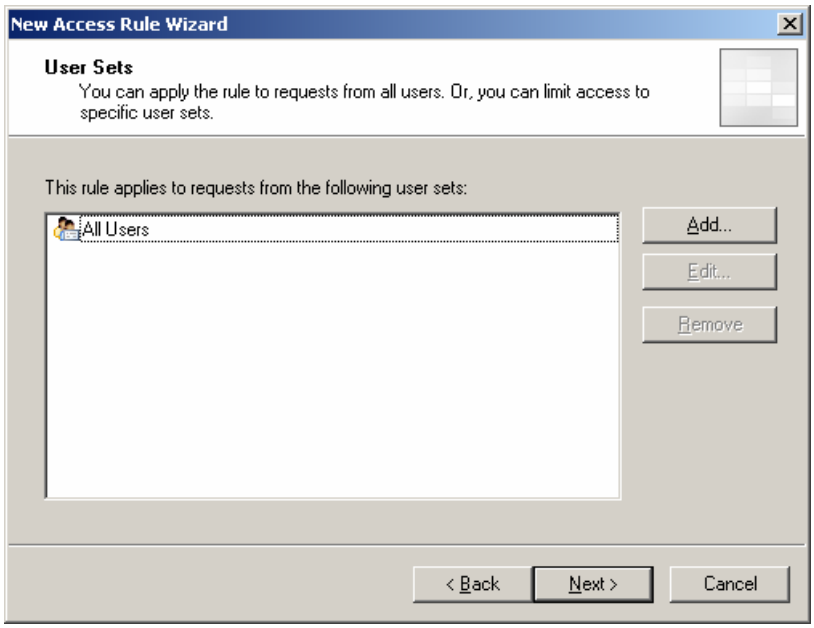
Bước 5: chọn địa chỉ nguồn của gói tin



Bước 6: chọn địa chỉ đích của gói tin. Bạn cần chọn Domain Name Set vừa mới tạo ra (Domain Name Set: khong duoc phep)



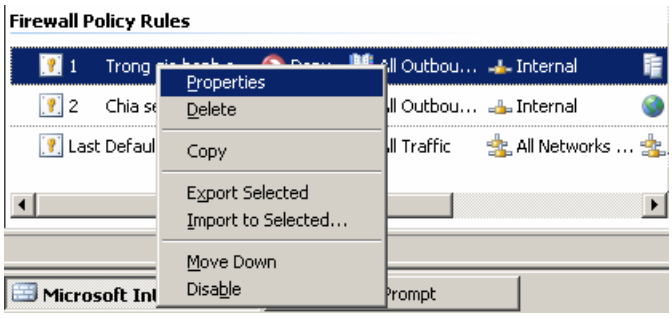
Bước 7: chọn các User sẽ được áp dụng



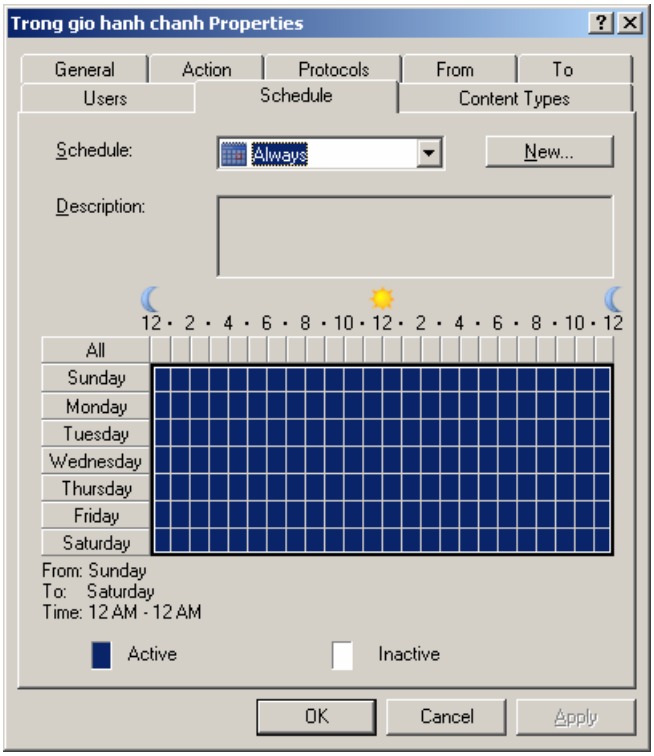
Bước 8: kiểm tra lại thông tin lần nữa

Yêu cầu 3: Chọn thời gian áp dụng cho luật

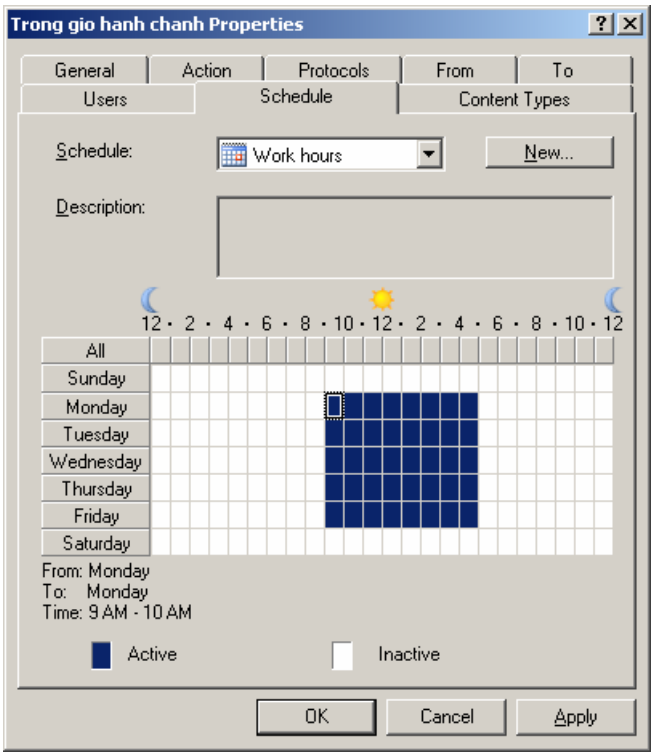
Bước 1: kích chuột phải vào Rule vừa mới tạo, chọn Properties



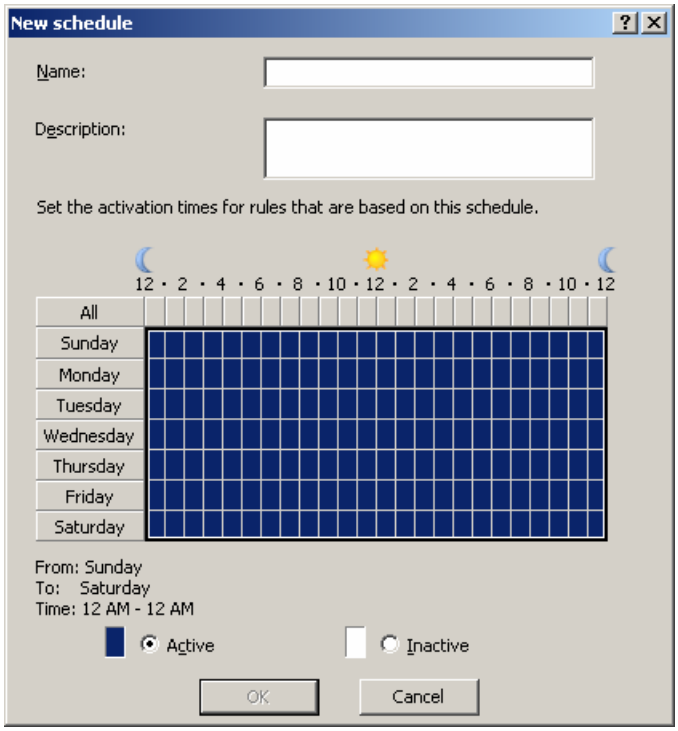
Bước 2: chọn Tab Schedule



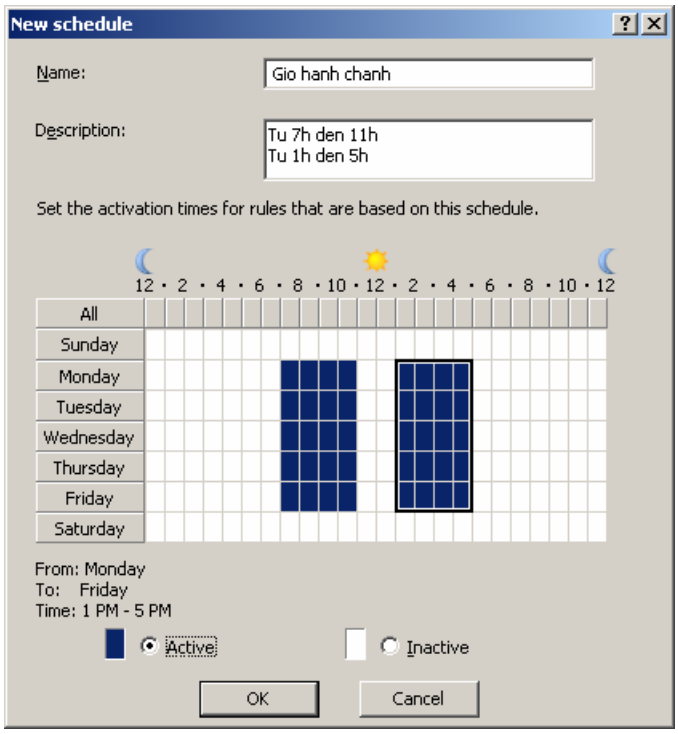
Bước 3: nếu chọn Work hours hiện đang có thì bạn sẽ thấy thời gian áp dụng từ 9h-17h. Điều này không phù hợp với thời gian công việc hiện tại.



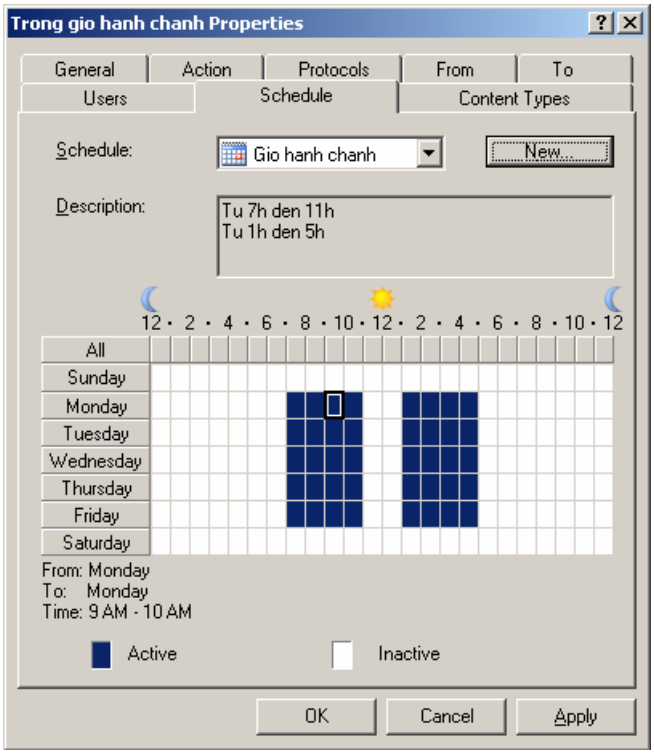
Bước 4: chọn New…để tạo khoảng thời gian mới



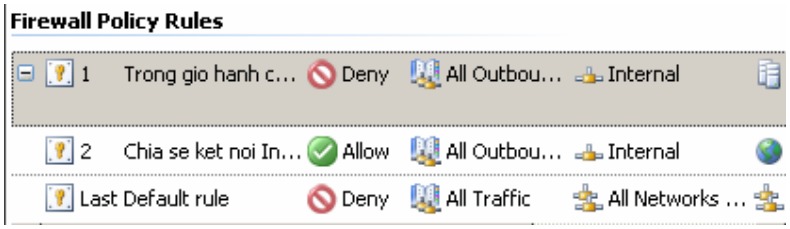
Bước 5: nhập tên cho khoảng thời gian này, và chọn lựa khoảng thời gian cần thiết lập (từ 7h đến 11h và từ 13h đến 17h). Bạn chỉ cần kéo cả khoảng thời gian cần thiết lập, sau đó chọn vào mục Active để kích hoạt khoảng thời gian đó.



Bước 6: sau khi chọn Ok thì bạn sẽ thấy trong mục Schedule có thêm mục mới là "Gio hanh chanh"



Bước 7: kết quả sau khi tạo xong.



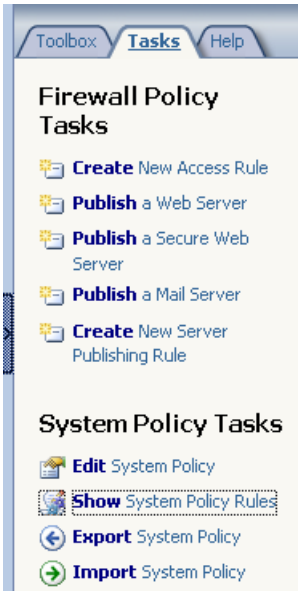
d. Chỉ cho phép các máy trong mạng nội ping tới ISA Firewall.

Để thực hiện điều này, bạn thực hiện 2 yêu cầu sau:

- Yêu cầu 1: Cho phép mạng nội bộ được Ping đến Server
- Yêu cầu 2: Cấm tất cả các mạng khác được ping đến Server

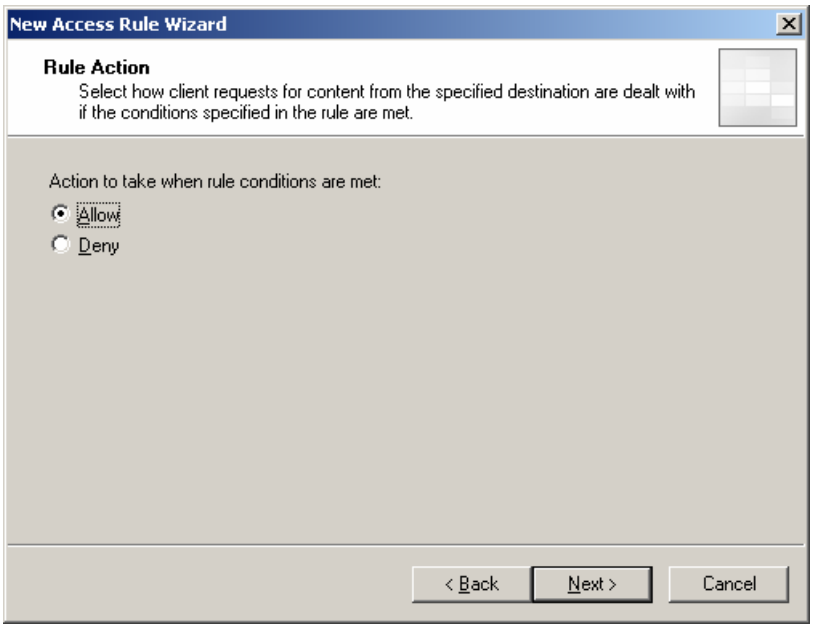
Yêu cầu 1: Cho phép mạng nội bộ được Ping đến Server

Bước 1: trong Firewall Policy, chọn lựa Tasks ở cột bên phải, bạn chọn Create New Access Rule

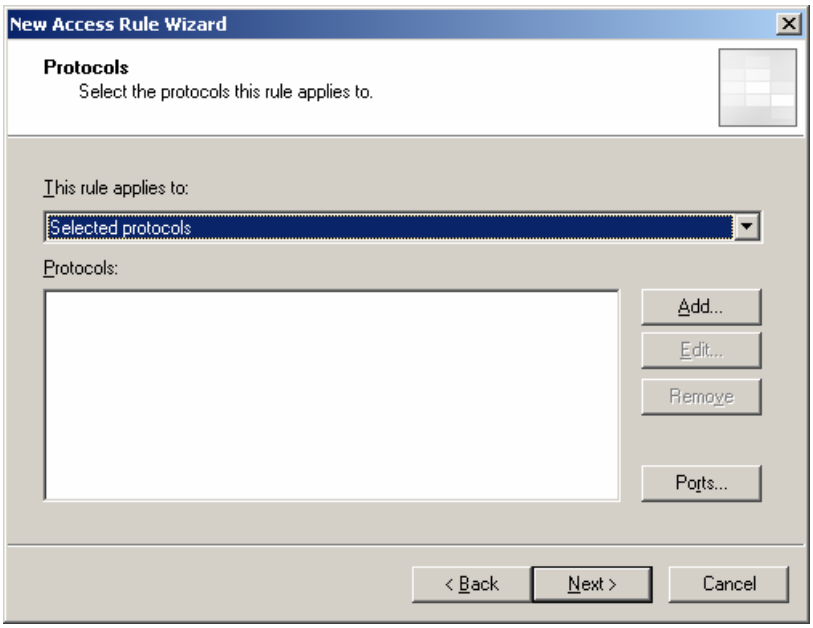


Bước 2: nhập tên cho Rule (“Cho phep PING noi bo”)

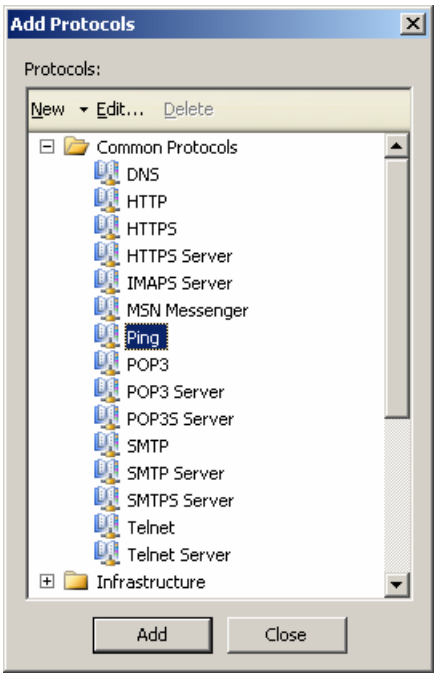
Bước 3: chọn hành động tương ứng với Rule (cho phép PING)



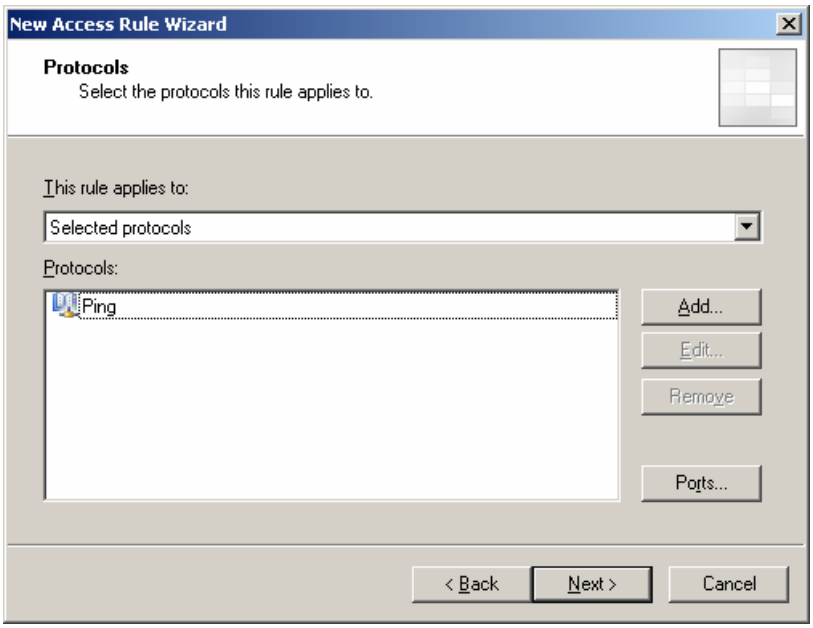
Bước 4: chọn giao thức tương ứng (giao thức ICMP). Trong mục This rule applies to, chọn Selected protocols. Chọn Add để thêm giao thức.



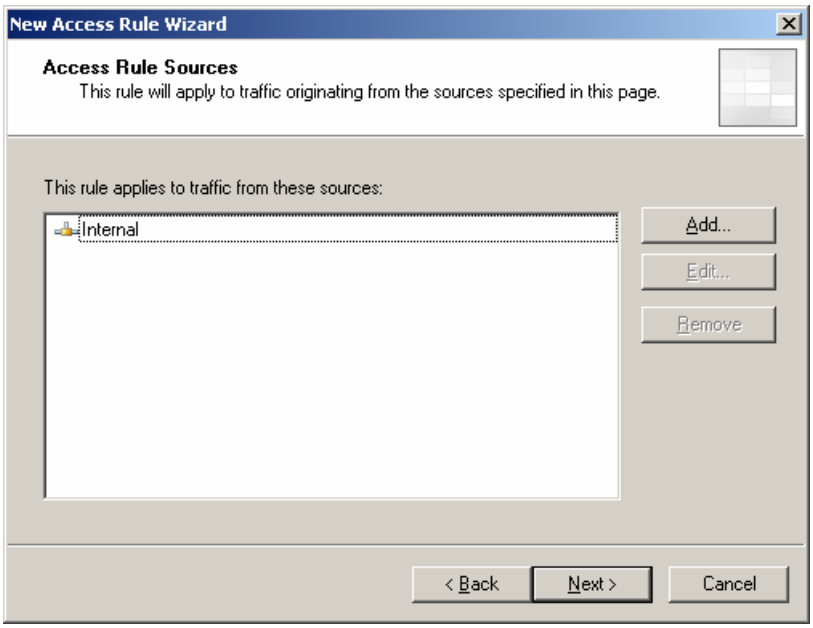
Bước 5: chọn giao thức PING từ mục Common Protocols, sau đó chọn Add



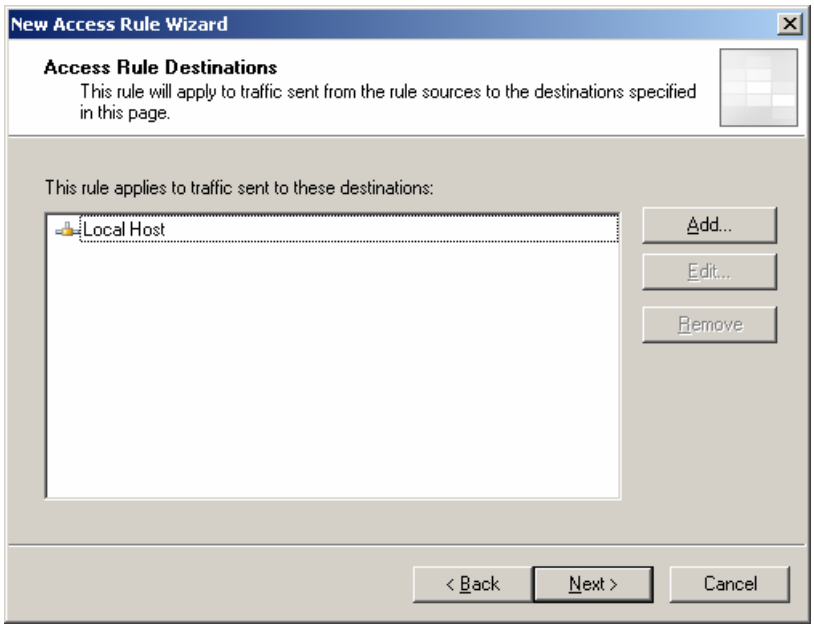
Bước 6: chọn Next để tiếp tục cấu hình



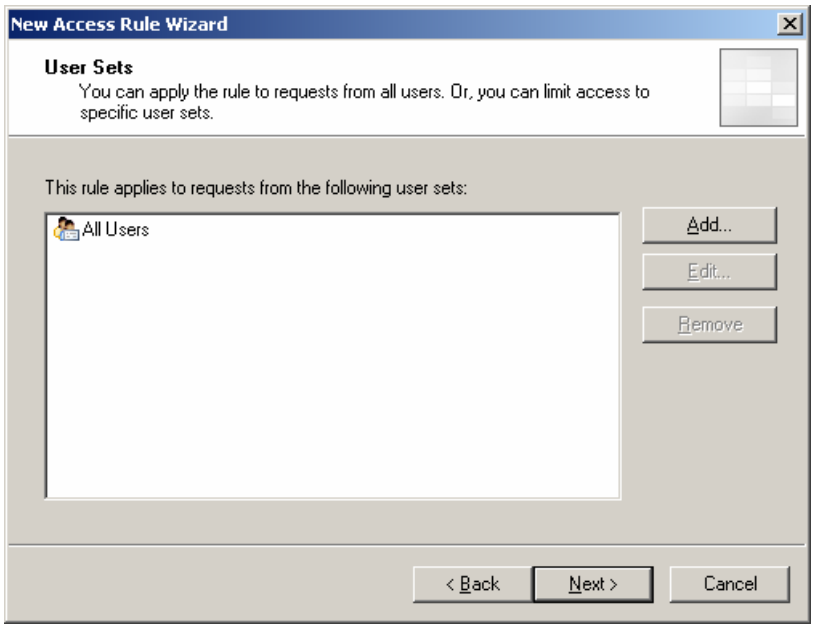
Bước 7: chọn địa chỉ nguồn của gói tin (Internal)



Bước 8: chọn địa chỉ đích của gói tin (Local Host – máy cấu hình ISA).



Bước 9: chọn các User cần áp đặt Rule

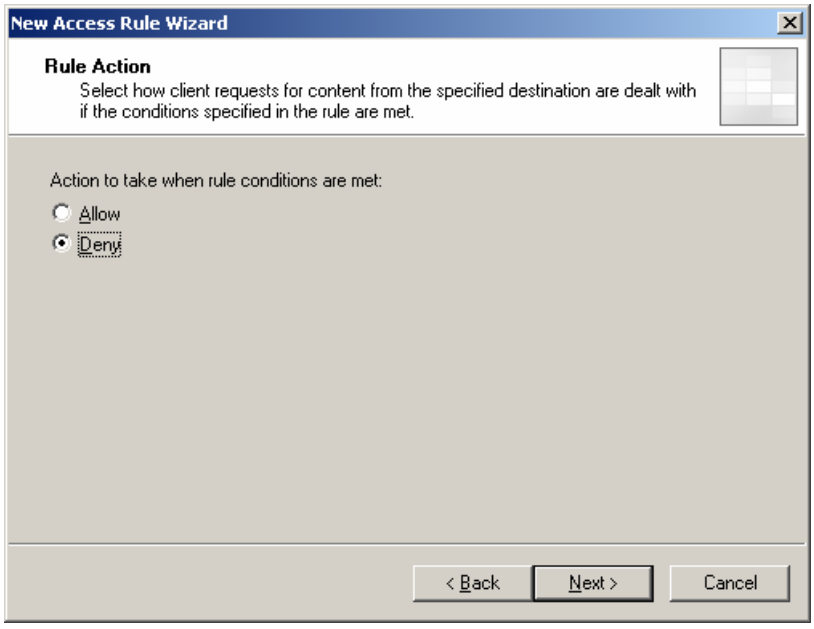


Bước 10: kiểm tra lại thông tin trước khi hoàn tất cấu hình RULE

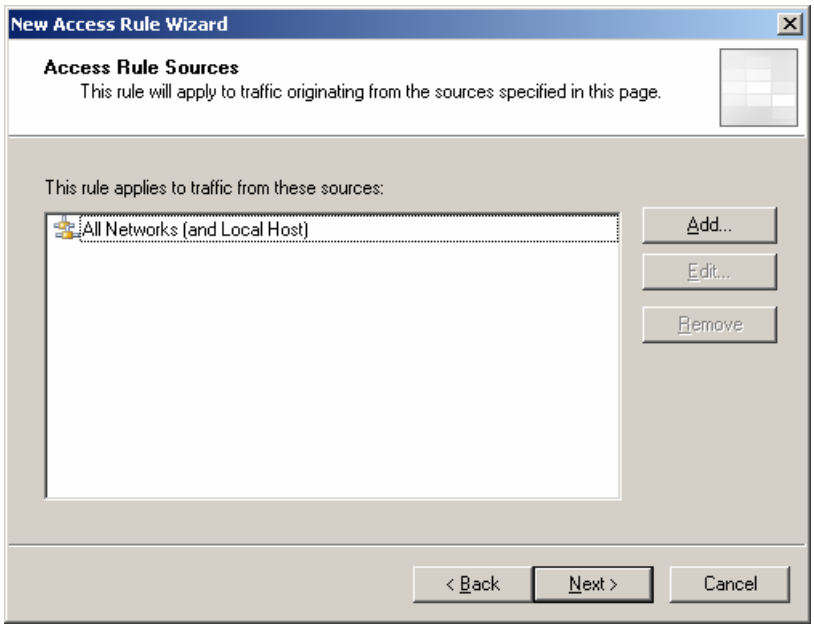
Yêu cầu 2: Cấu hình RULE không cho các mạng khác PING đến ISA proxy.

Bạn thực hiện giống yêu cầu 1, chỉ có sự thay đổi ở bước 3 (cách thức hoạt động) và bước 7 (địa chỉ nguồn của gói tin)

Bước 3: chọn mục DENY thay vì ALLOW



Bước 7: chọn tất cả các đường mạng

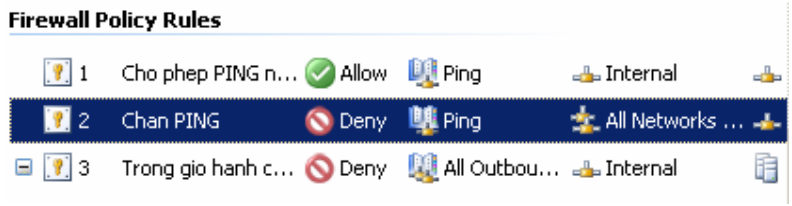


Kết quả sau khi bạn thực hiện xong 2 yêu cầu:

Bạn để ý thấy rằng luật tạo ra bởi yêu cầu 2 được thực hiện trước luật tạo ra bởi yêu cầu 1. Do đó, nếu bạn không thay đổi vị trí thì tất cả các máy đều không PING được đến LOCAL HOST. Để thay đổi vị trí của các RULE, bạn làm như sau:

Nhìn vào cột bên phải, bạn sẽ thấy xuất hiện dòng Move Selected Rules **Down**, do đó, bạn chọn RULE được tạo ra bởi yêu cầu 2 (Chan PING) và chọn vào Move Selected Rules **Down**.

Kết quả sau khi thực hiện sẽ như sau:



e. Cho phép một số máy trong mạng nội bộ có thể truy xuất Internet thông qua cơ chế NAT được cung cấp trên ISA Firewall.

Để thực hiện điều này, bạn thực hiện như sau:

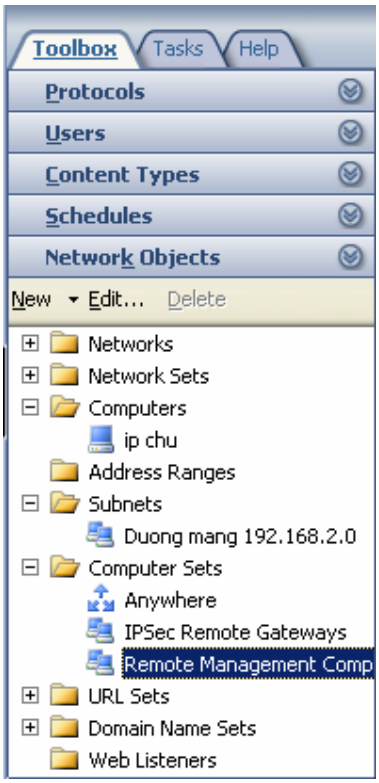
- Yêu cầu 1: Tạo Computer hoặc Set Computer
- Yêu cầu 2: Disable các NAT mặc định
- Yêu cầu 3: Thiết lập NAT mới.

Yêu cầu 1: Tạo Computer hoặc tập hợp Computer

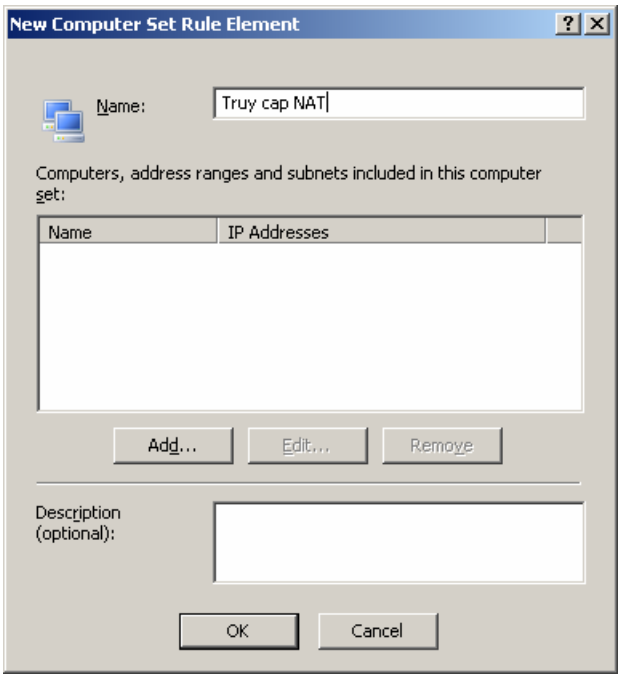
Bước 1: trong Firewall Policy, ở cột bên phải bạn chọn Toolbox, bạn sẽ thấy biểu tượng Computer và Computer Sets.

- Nếu muốn thêm từng Computer thì bạn kích chuột phải vào Computer, chọn New Computer
- Nếu muốn thêm một nhóm Computer thì bạn kích chuột phải vào Computer Sets, chọn New Computer Sets. Trong trường hợp số lượng Computer cần áp dụng cho Policy ít thì bạn có thể tạo New Computers, sau đó khi tạo Policy, ở phần Source Address thì bạn chọn các New Computer này. Nhưng với số lượng lớn thì bạn nên tạo một Computers Sets, vì sẽ dễ dàng quản lý hơn, và khi tạo một Policy thì việc thêm một Computer Sets vào Source Address sẽ dễ hơn nhiều so với việc chọn nhiều Computers.

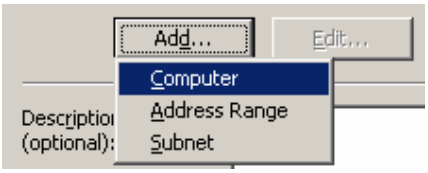
Do đó, trong ví dụ này sẽ hướng dẫn bạn tạo một Computer Sets. Kích chuột phải vào Computers Sets, chọn New Computers Set.



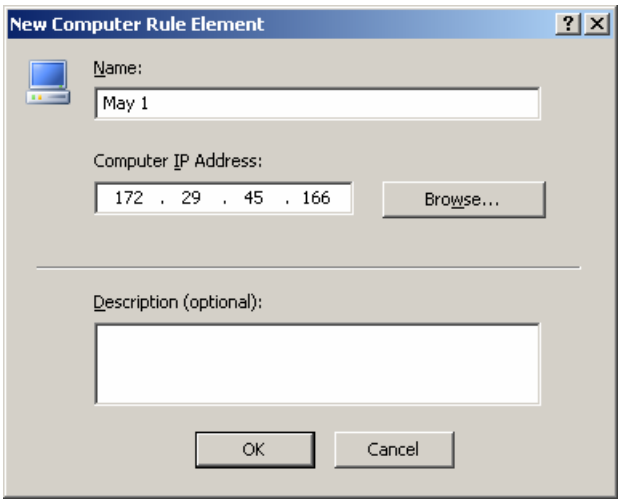
Bước 2: nhập tên cho Computer Set. (ví dụ là Truy cap NAT).



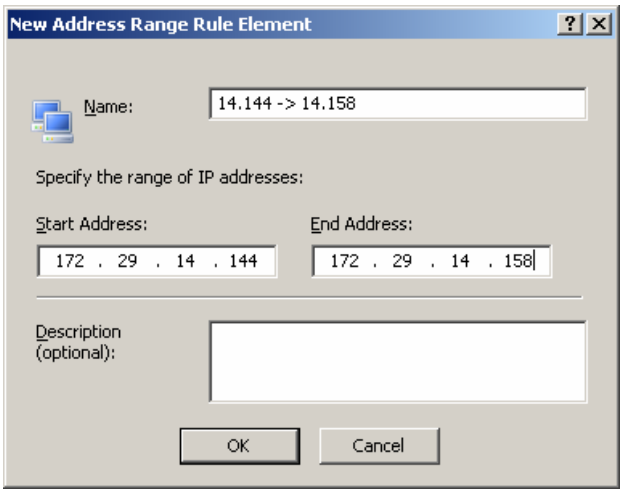
Bước 3: chọn Add để thêm các Computer vào. Bạn có thể thêm từng Computer (theo địa chỉ IP), hoặc thêm một đường mạng, một khoảng địa chỉ IP.



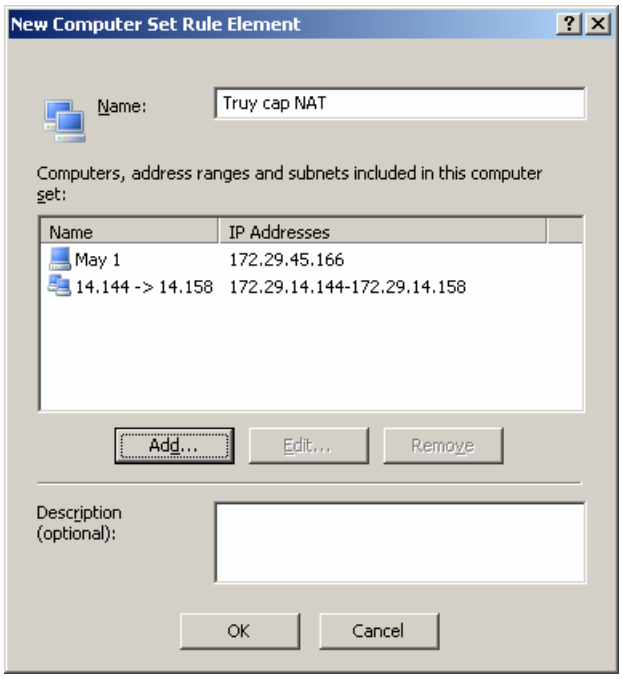
Bước 4: nếu chọn Computer, bạn sẽ thấy hộp thoại sau hiện ra. Nhập thông tin của máy cần thêm vào. (Bạn có thể chọn Browse.. để tìm địa chỉ IP hoặc tên máy). Sau đó chọn Ok



Bước 5: nếu chọn Address Range, bạn sẽ thấy hộp thoại sau hiện ra. Nhập địa chỉ đầu và địa chỉ cuối của đoạn mạng đó. Sau đó chọn Ok

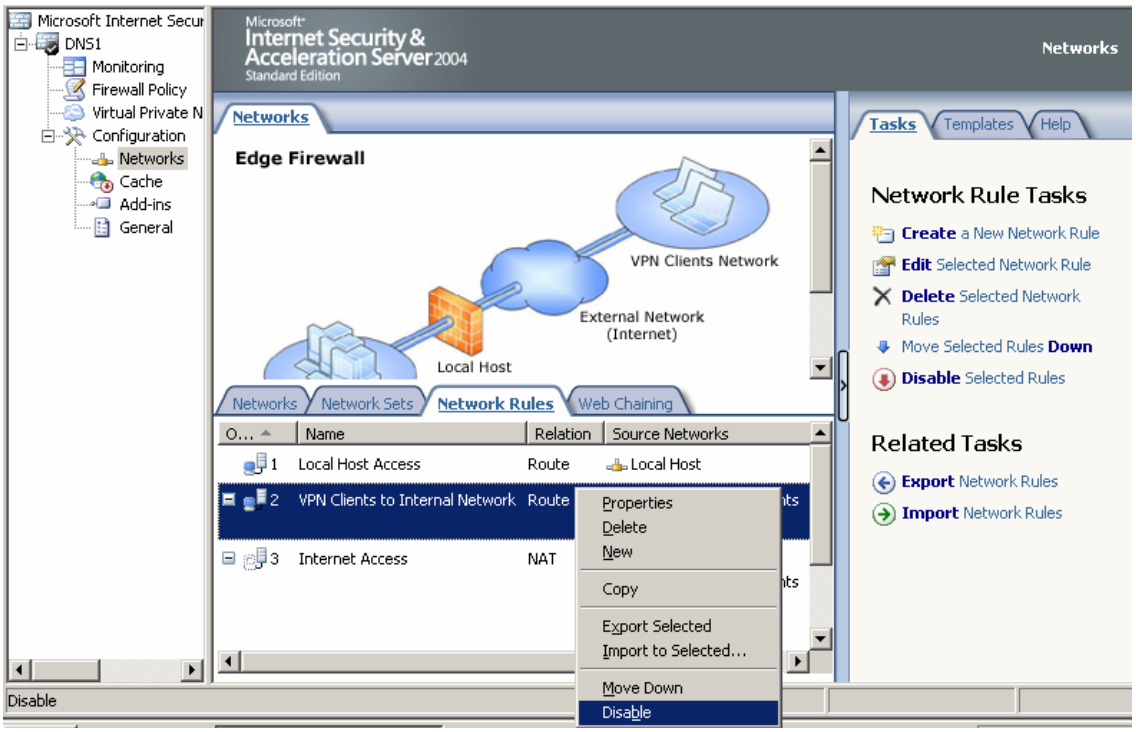


Bước 6: sau khi thực hiện xong bước 4 và bước 5. Kết quả sẽ xuất hiện trong hộp thoại như sau. Chọn Ok để hoàn tất việc thiết lập Computer Set.

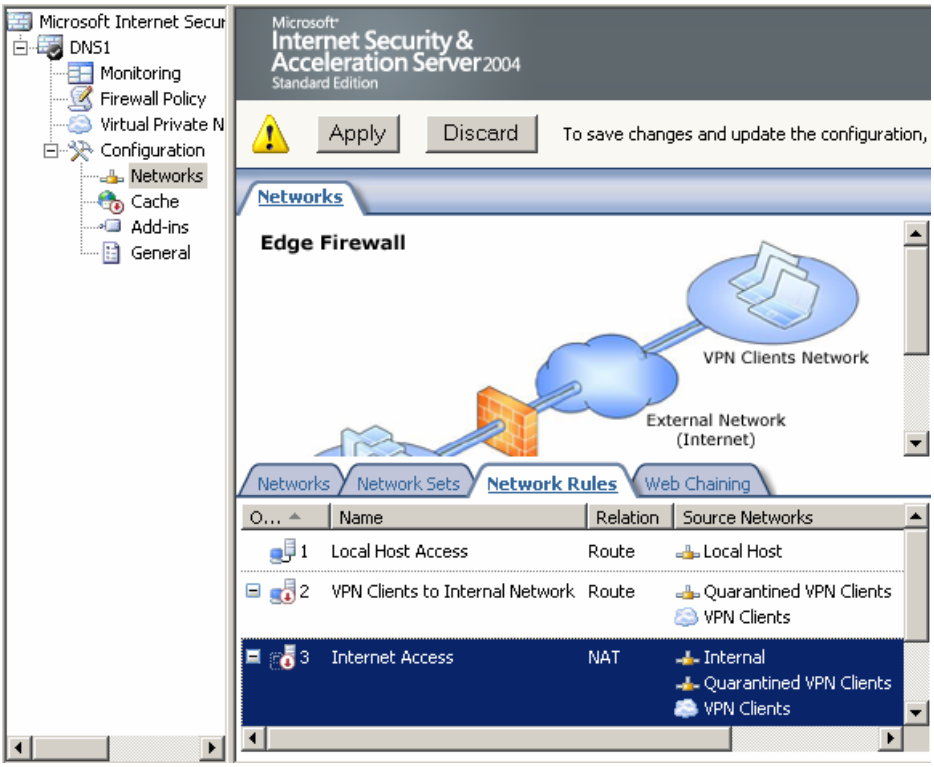


Yêu cầu 2: Disable các NAT mặc định

Bước 1: chọn Configuration, chọn Networks, chọn Tab Network Rules. Bạn sẽ thấy 3 Rule. Bạn chỉ cần Disable Rule 2 và Rule 3. Lần lượt kích chuột phải vào Rule 2, Rule 3 chọn Disable

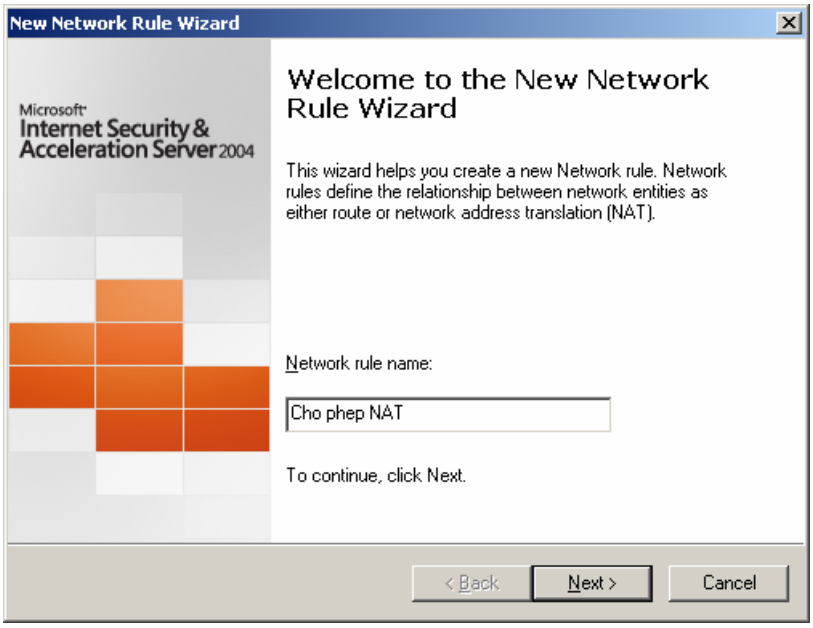


Bước 2: kết quả sau khi bạn Disable Rule 2,3. (Chưa cập nhật sự thay đổi).

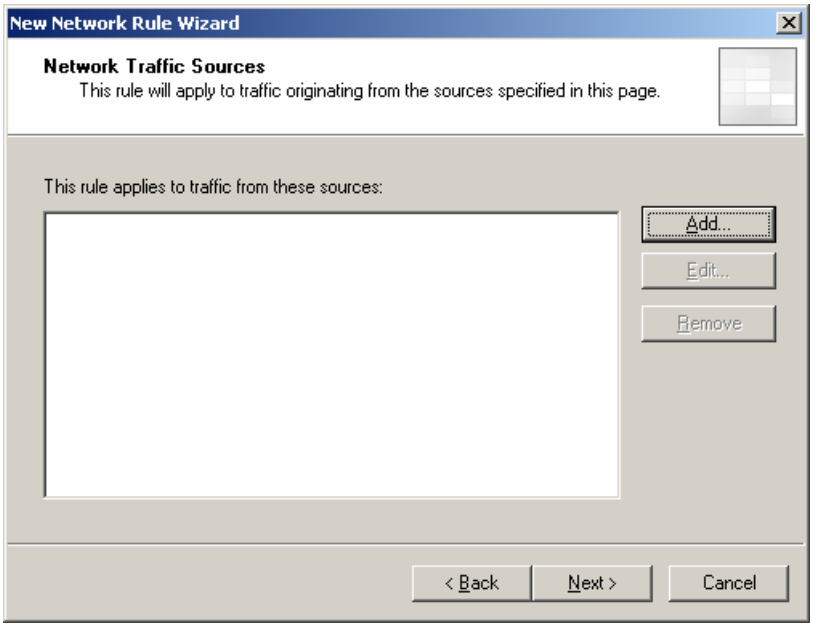


<u>Yêu cầu 3</u>: Tạo NAT mới

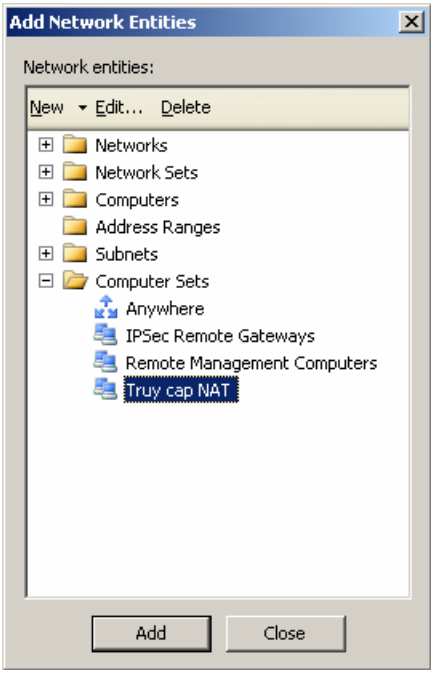
Bước 1: ở cột bên phải, bạn chọn Tab Tasks, chọn Create a New network Rule. Sau đó nhập tên cho Network Rule.



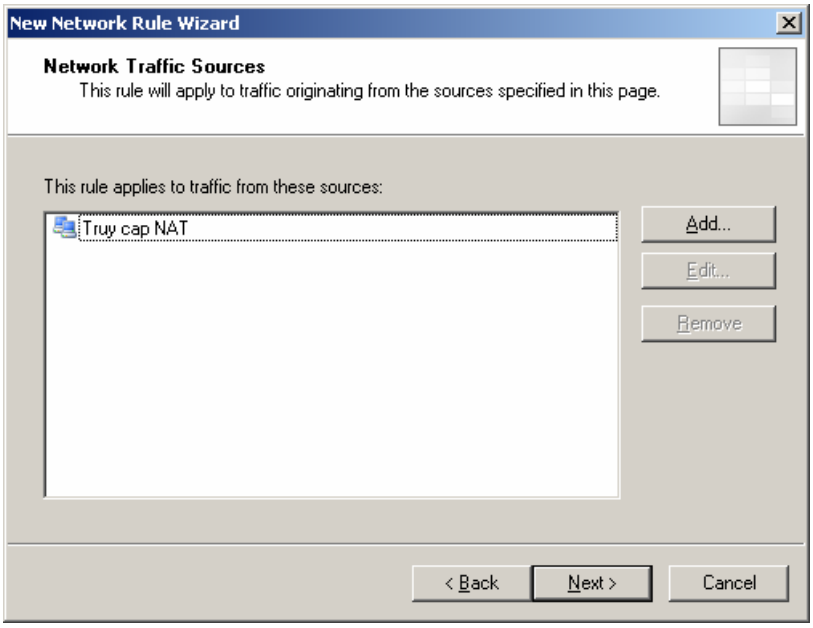
Bước 2: chọn Add để nhập địa chỉ nguồn



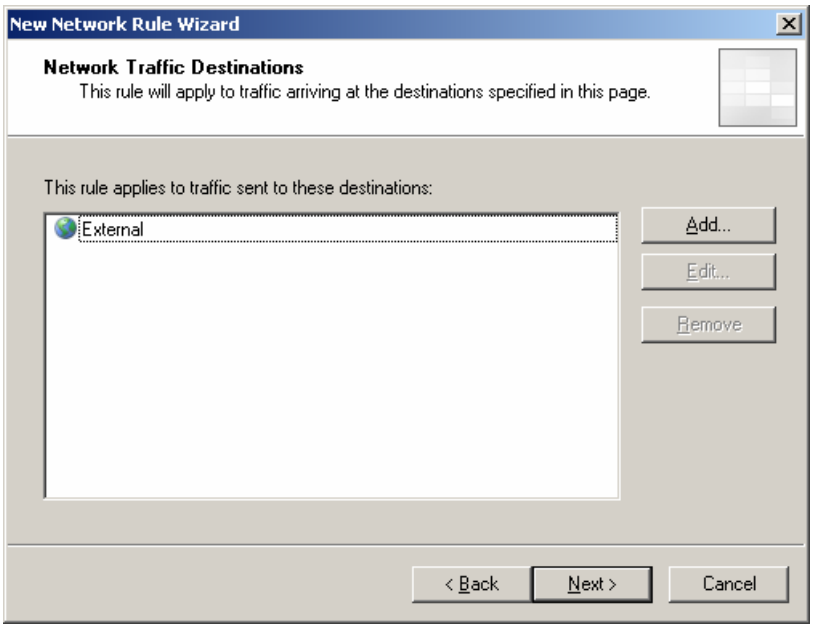
Bước 3: chọn Computer Sets, chọn Computer Set vừa mới tạo (truy cap NAT). Sau đó chọn Add.



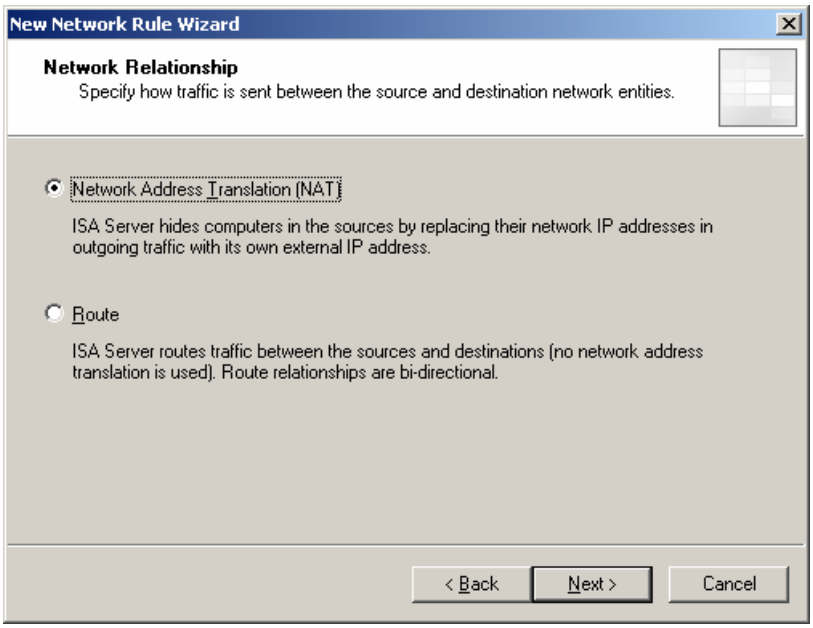
Bước 4: kết quả sau khi thêm địa chỉ nguồn. Chọn Next để tiếp tục



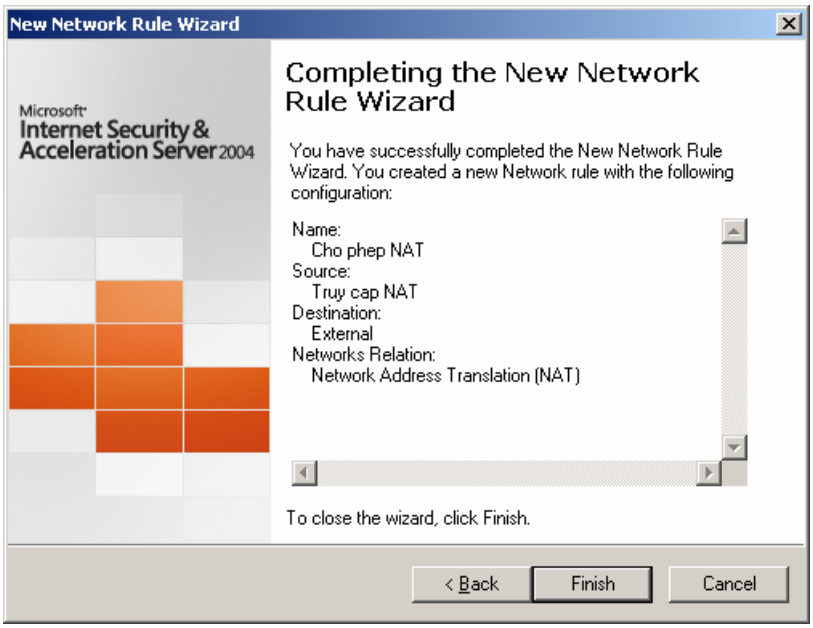
Bước 5: ở phần địa chỉ nguồn, chọn Add để thêm đường mạng External. Sau đó chọn Next để tiếp tục



Bước 6: trong phần Network Relationship, bạn chọn Network Address Translation (NAT). Sau đó chọn Next để tiếp tục



Bước 7: kiểm tra lại thông tin trước khi chọn Finish để hoàn tất việc thiết lập

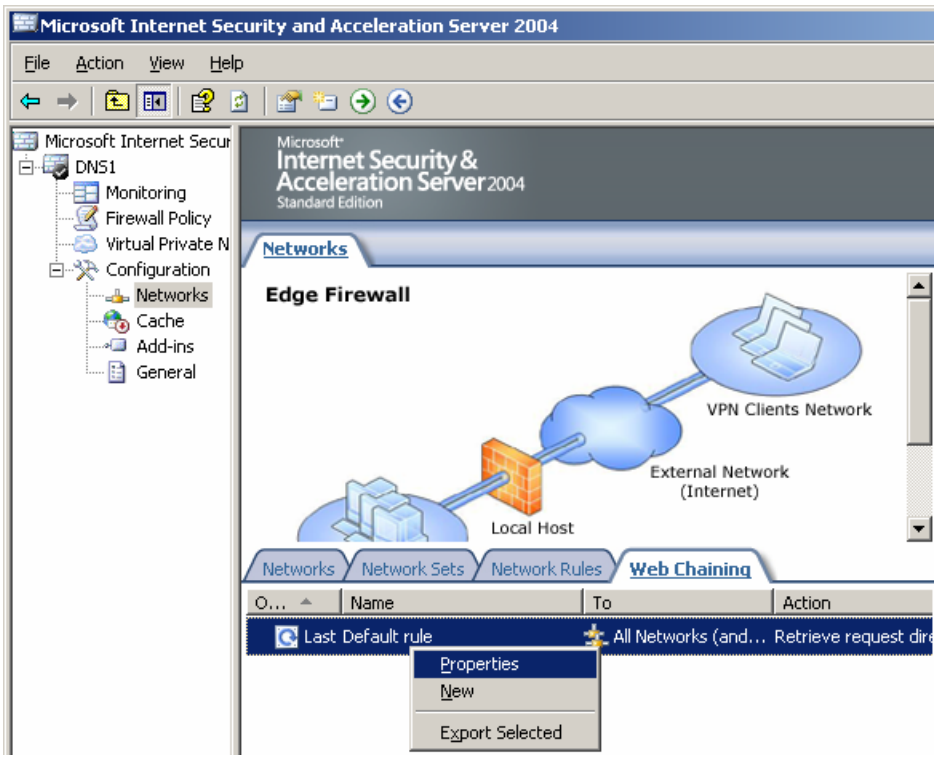


Bước 8: chọn vào nút Apply để cập nhật sự thay đổi trên ISA Server.

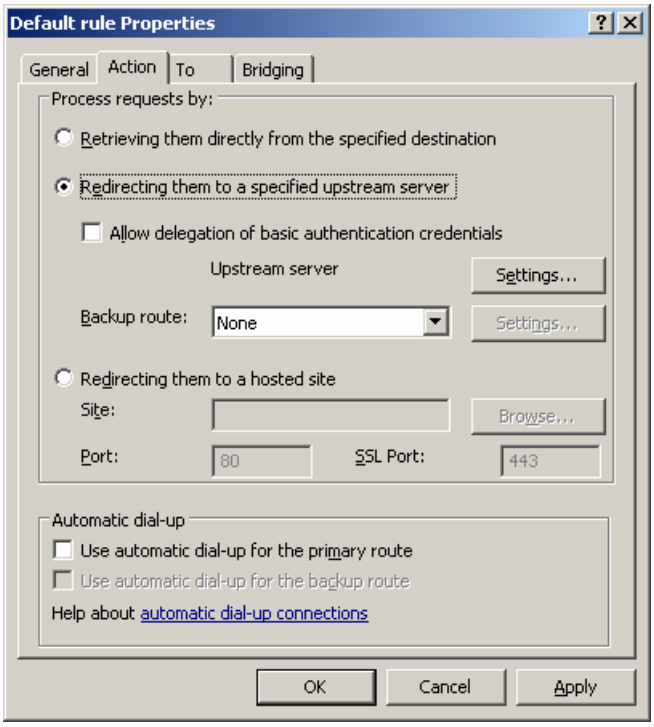
f. Cấu hình route uptream lên proxy cha có địa chỉ 192.168.11.1

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 5 – phần V.3 – trang 181)

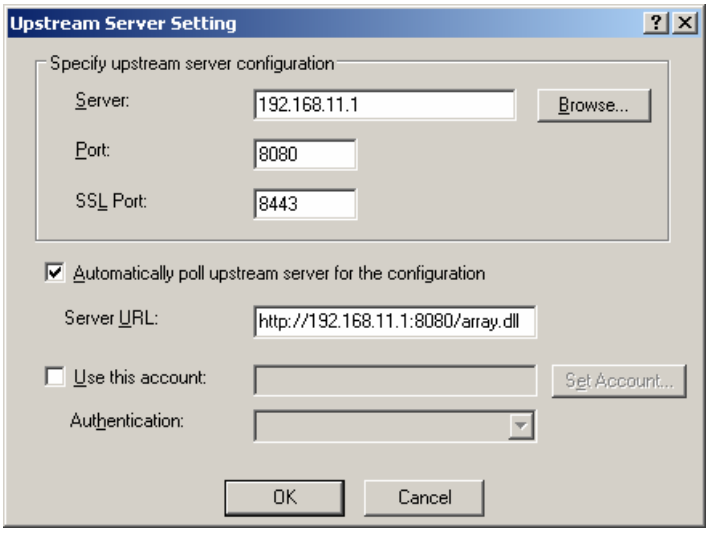
Bước 1: vào ISA Server Management, chọn Configuration, chọn mục Network, chọn tab Web chaning. Kích chuột phải vào Last Default rule, chọn Properties. (hoặc kích đúp chuột vào Last Default rule).



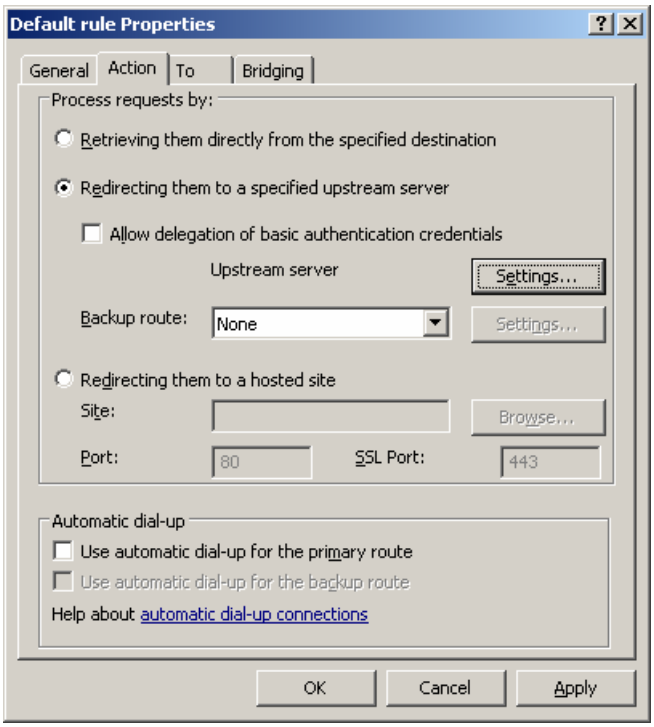
Bước 2: chọn Tab Action, chọn Redirecting them to a specified upstream server. Sau đó chọn vào nút Setting



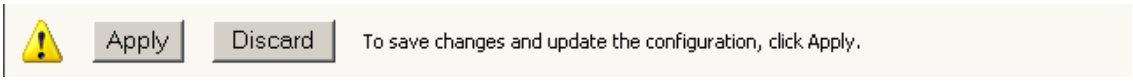
Bước 3: trong mục Specify upstream server configuration, mục Server, bạn điền địa chỉ của Proxy cha (ở đây là 192.168.11.1), và điền Port 8080 vào mục Port (Port 8080 là Port mặc định). Sau đó chọn Ok



Bước 4: chọn Ok để hoàn tất việc thiết lập Upstream



Bước 5: cập nhật lại sự thay đổi bằng cách Apply các sự thay đổi.



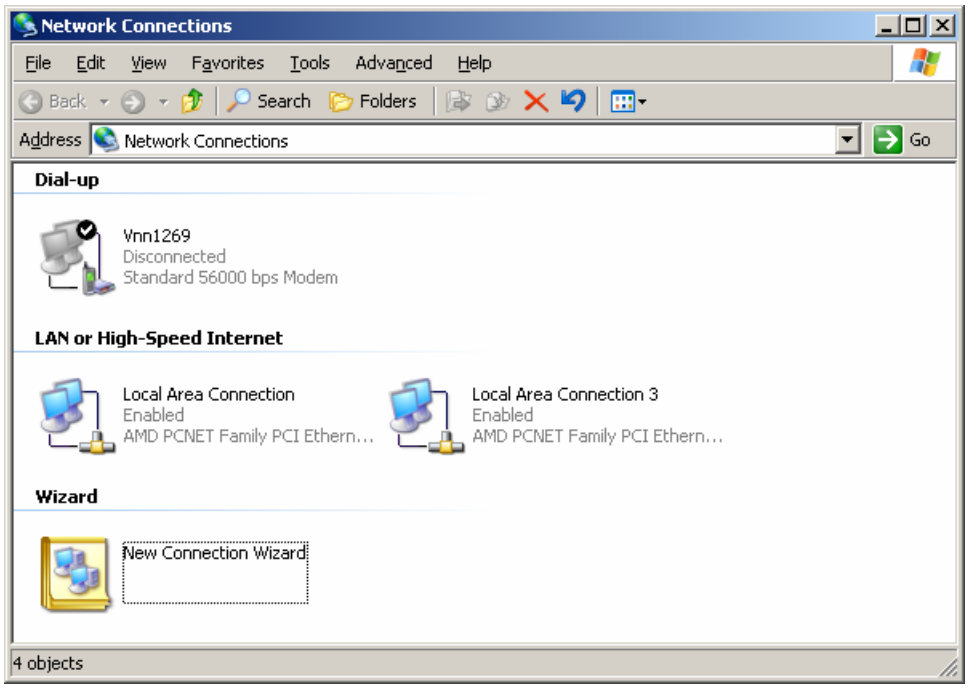
g. Proxy dùng kết nối dial-up lên VNN theo thông tin account dial-up.

Để thực hiện được thì bạn phải thực hiện 2 yêu cầu sau:

- Yêu cầu 1: cài đặt kết nối quay số vnn1269
- Yêu cầu 2: thêm kết nối đó vào ISA

Yêu cầu 1: Cài đặt kết nối quay số vnn1269

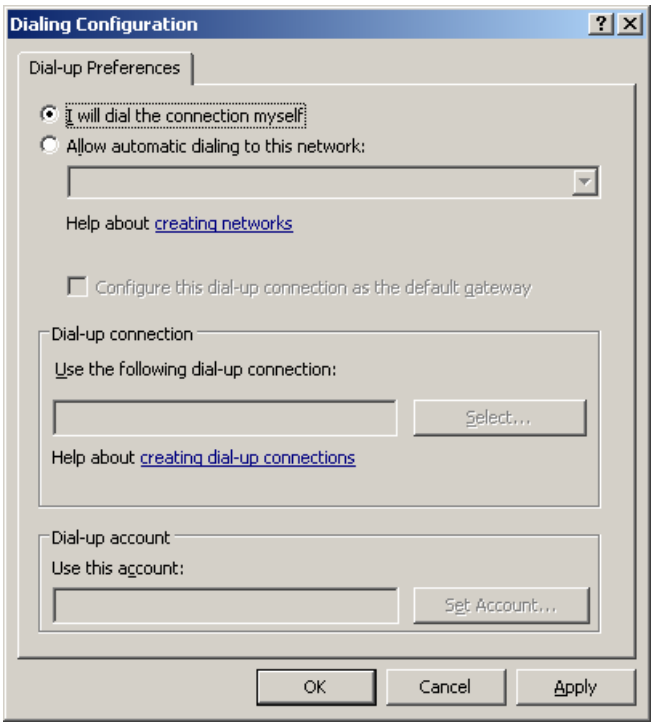
Kích chuột phải vào My Network Places, chọn Properties. Sau đó chọn New Connection Wizard để tạo kết nối vnn1269. Kết quả sau khi tạo ra sẽ tương tự hình sau:



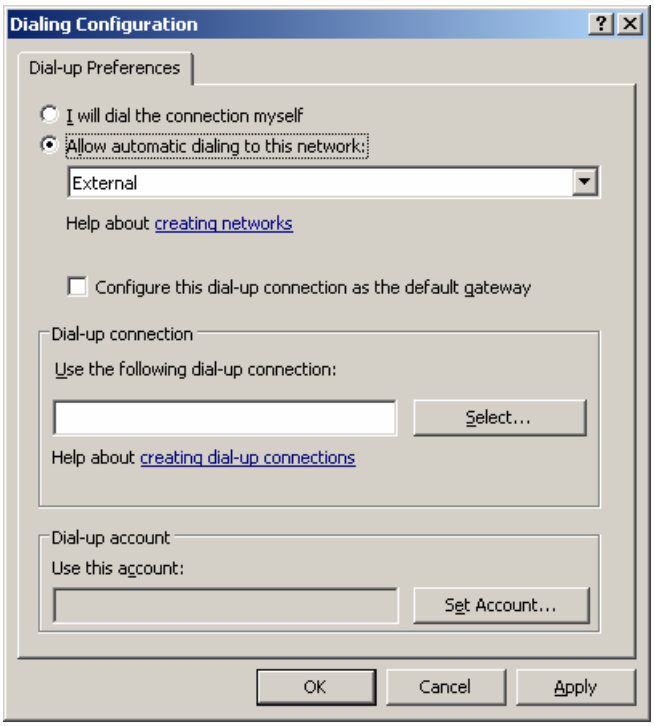
Yêu cầu 2: Thêm kết nối đó vào ISA

Bước 1: vào ISA Server Managerment, trong Configuration, chọn General

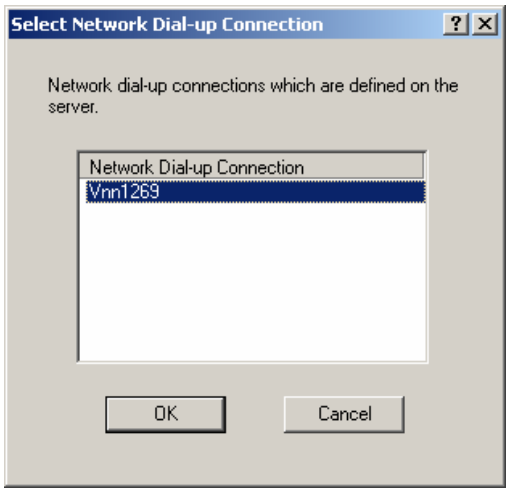
Bước 2: chọn vào mục Specify Dial-up Preferences.



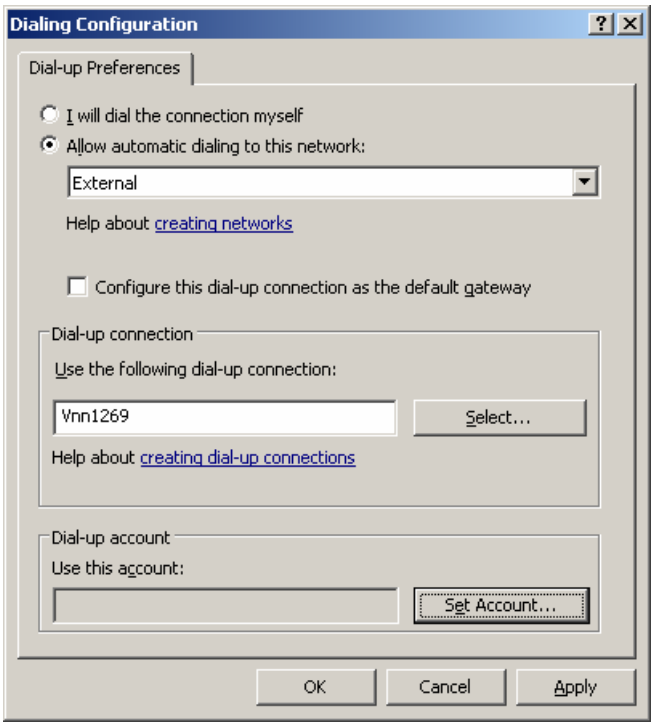
Bước 3: chọn vào mục Allow automatic dialing to this network, sau đó chọn External (thiết lập kết nối này khi có yêu cầu đi ra mạng External)



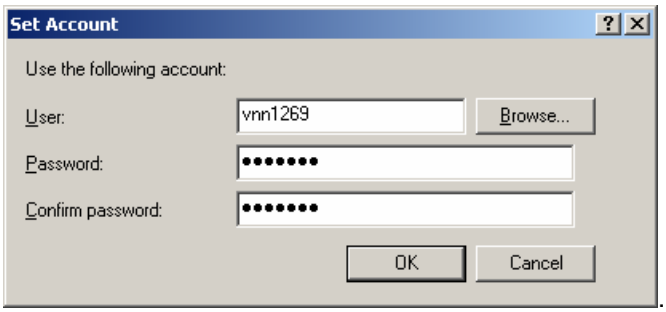
Bước 4: trong mục Dial-up Connection, chọn vào nút Select… để chọn kết nối



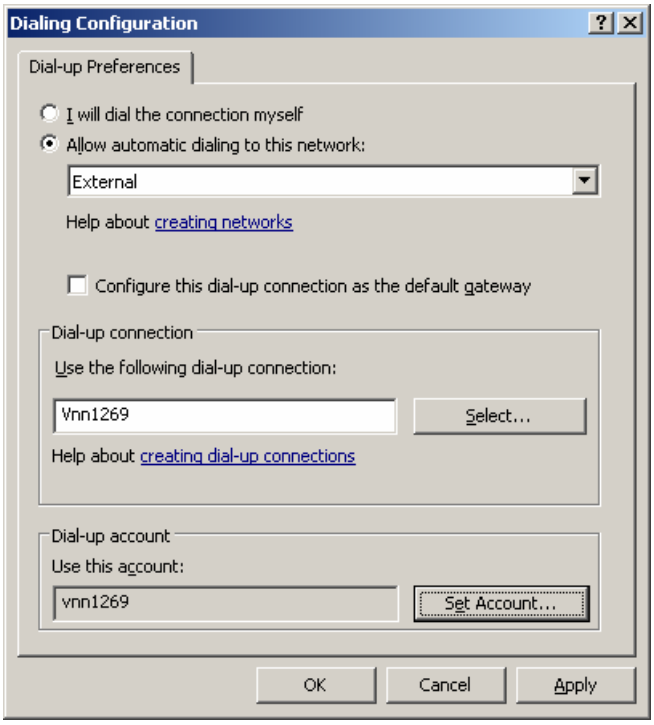
Bước 5: sau khi chọn kết nối vnn1269, bạn chọn Ok thì thấy kết quả như sau:



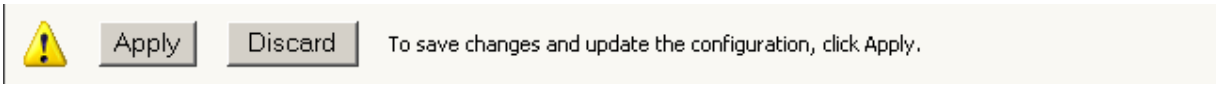
Bước 6: trong mục Dial-up account, bạn chọn nút Set Account…. Đây là account được dùng để quay số.



Bước 7: kết quả sau khi thực hiện xong. Chọn Ok để kết thúc việc thiết lập



Bước 8: sau khi thực hiện xong, bạn cần chọn Apply để thực thi sự thay đổi trên ISA.

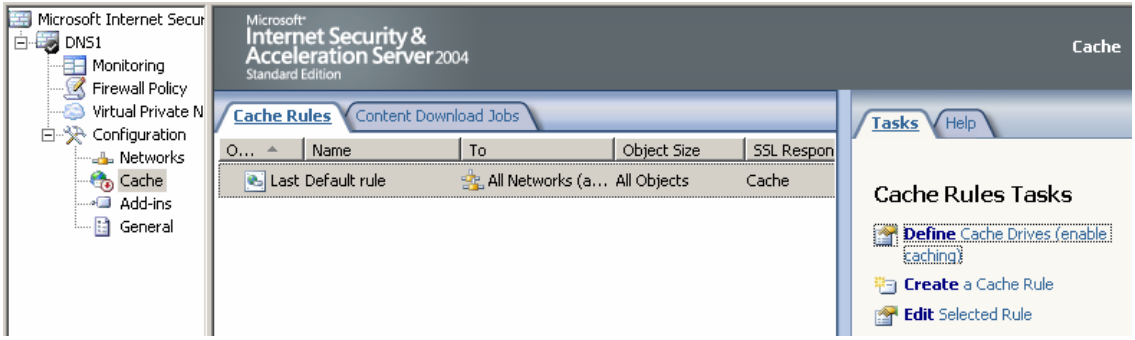


3. Bài 3: cấu hình Caching:

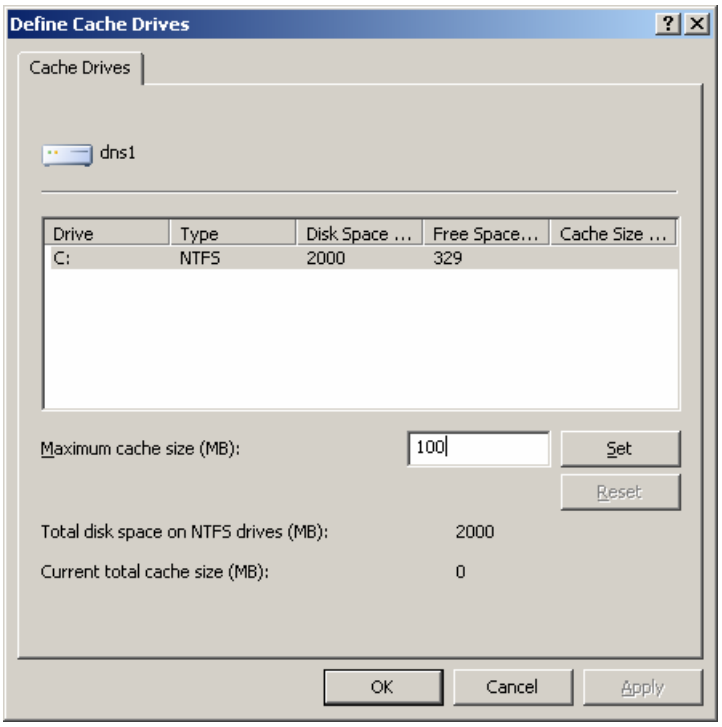
a. Cấu hình Cache memory size : 100MB

Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 5 – phần V.9 – trang 207)

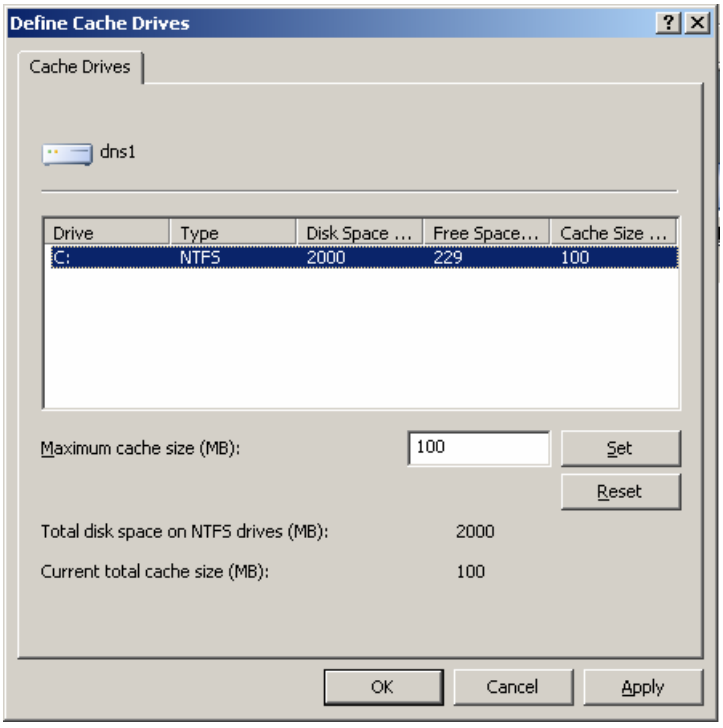
Bước 1: chọn Configuration, chọn Cache. Ở cột bên phải, chọn Tab Tasks, chọn Define Cache Drives (enable Caching).



Bước 2: ở dòng Maximum cache size (MB), bạn nhập 100. (memory size là 100MB). Sau đó chọn Set

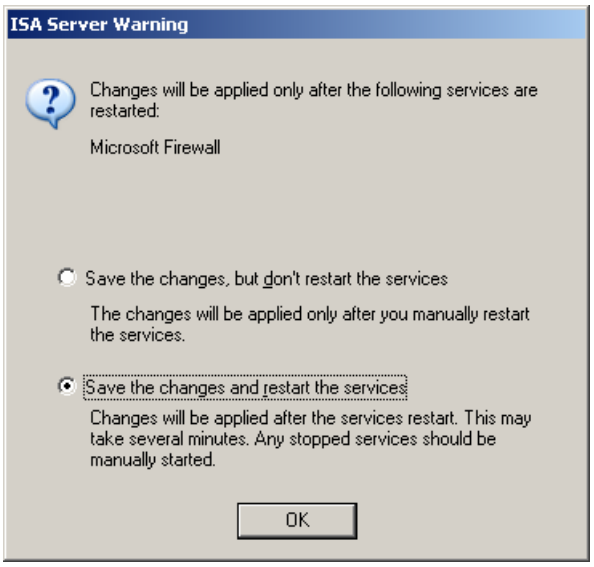


Bước 3: sau khi nhấn Set, hộp thoại sẽ như sau:



Bước 4: chọn Ok để hoàn tất việc thiết lập.

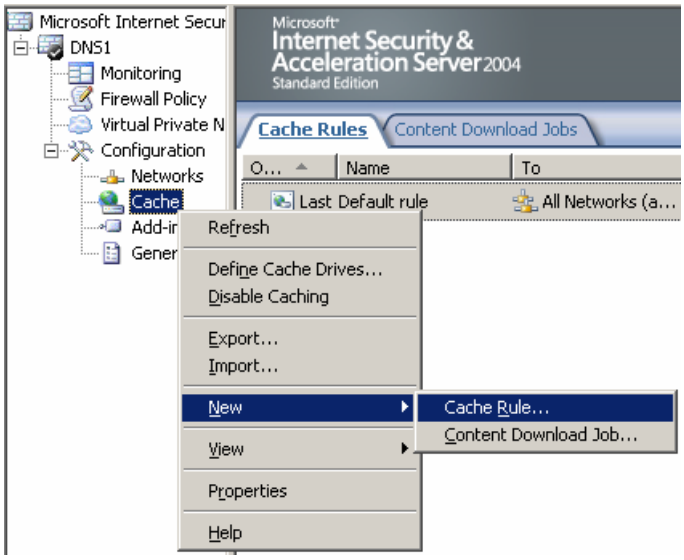
Bước 5: chọn Apply để cập nhật sự thay đổi. Chương trình sẽ hỏi bạn có muốn Restart Service hay không ? Tốt nhất bạn nên chọn Save the changes and restart the services để chương trình khởi động lại và cập nhật sự thay đổi.



b. Tạo rule cache cho ISA proxy để theo dõi và quản lý các cache objects

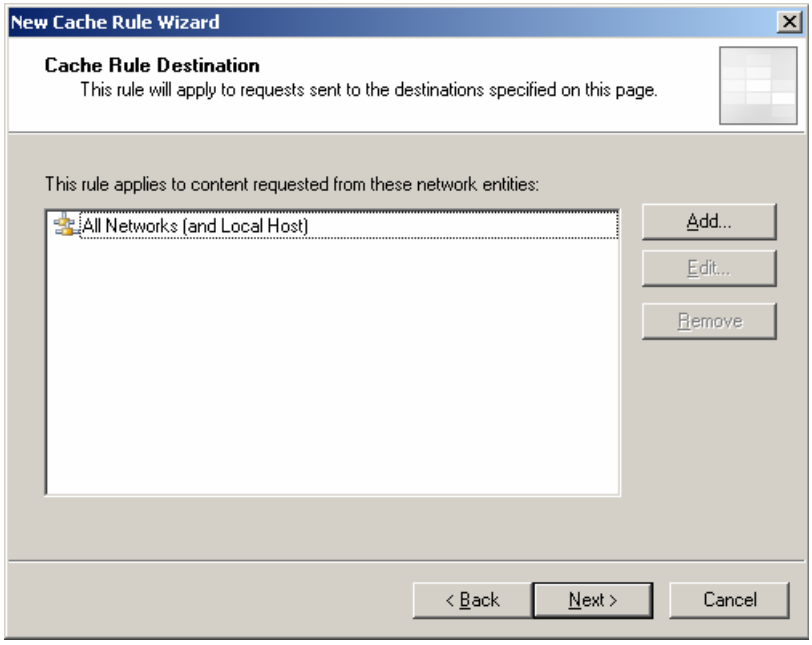
Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 5 – phần V.9.3 – trang 209)

Bước 1: chọn configuration, chọn Cache, chọn New, Cache Rule..

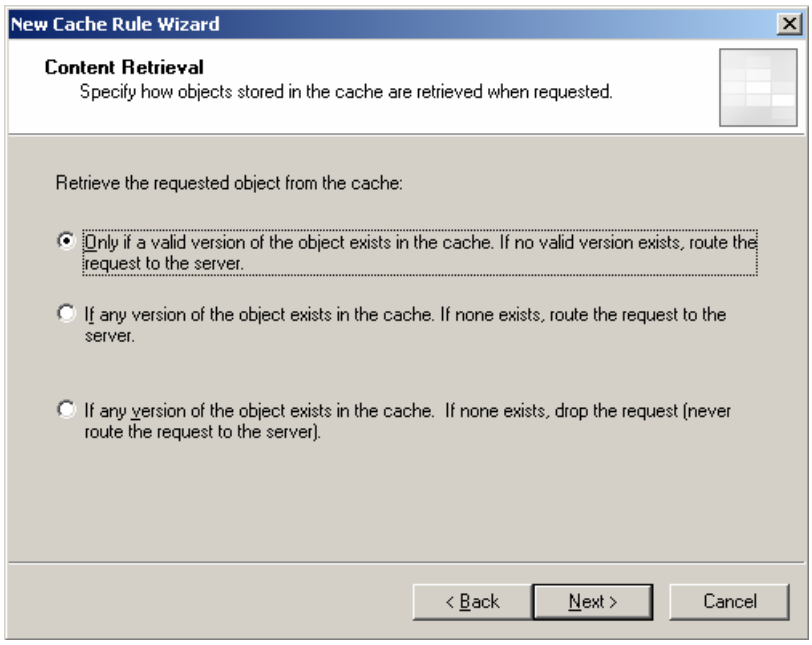


Bước 2: nhập tên cho Cache Rule (ví dụ là Cau 3b)

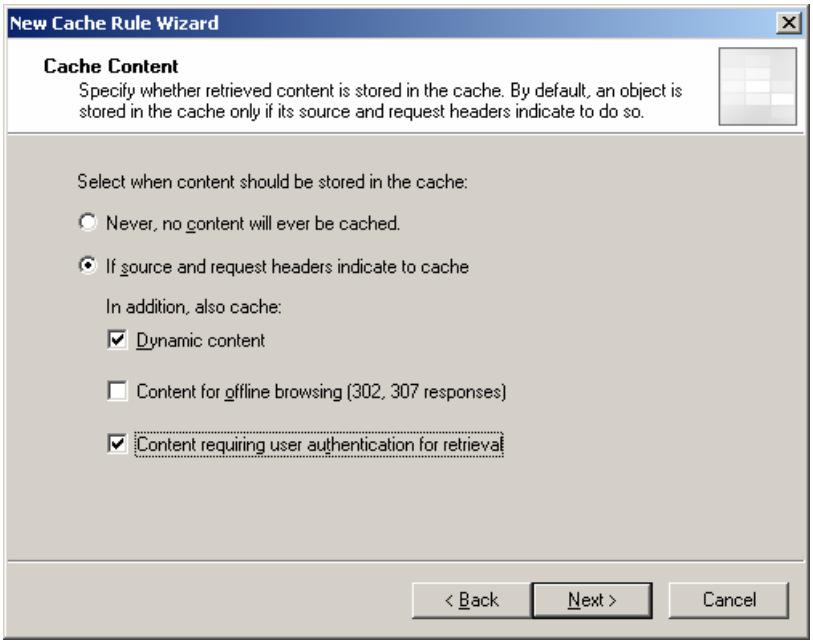
Bước 3: chọn network đích là All Networks (and Local Host), sau đó chọn Next để tiếp tục



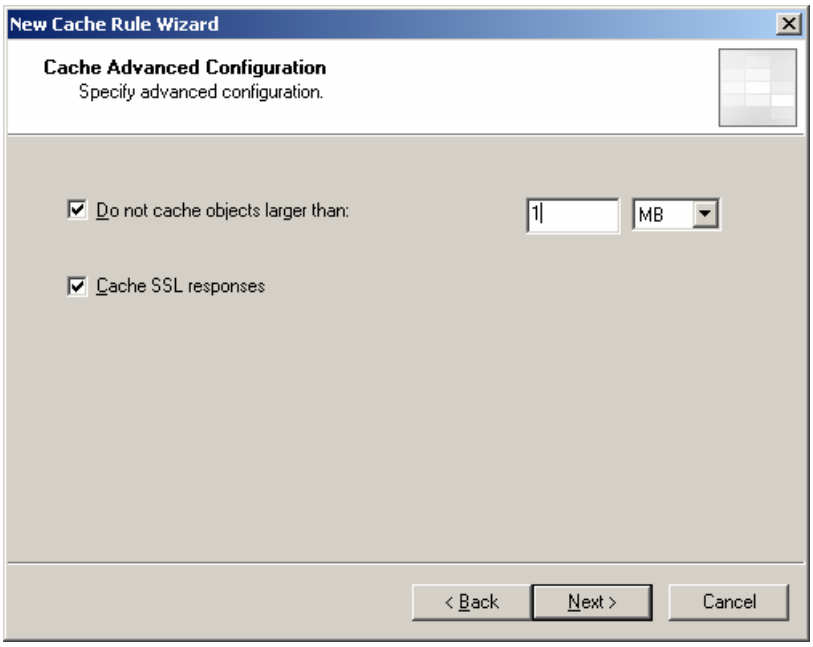
Bước 4: chọn Object phù hợp, sau đó chọn Next



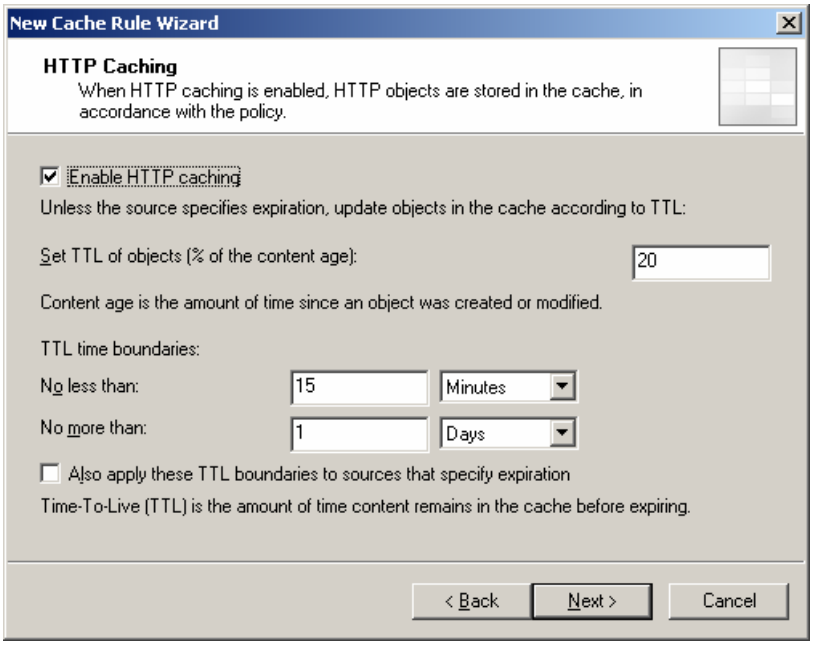
Bước 5: chọn các nội dung cần lưu Cache



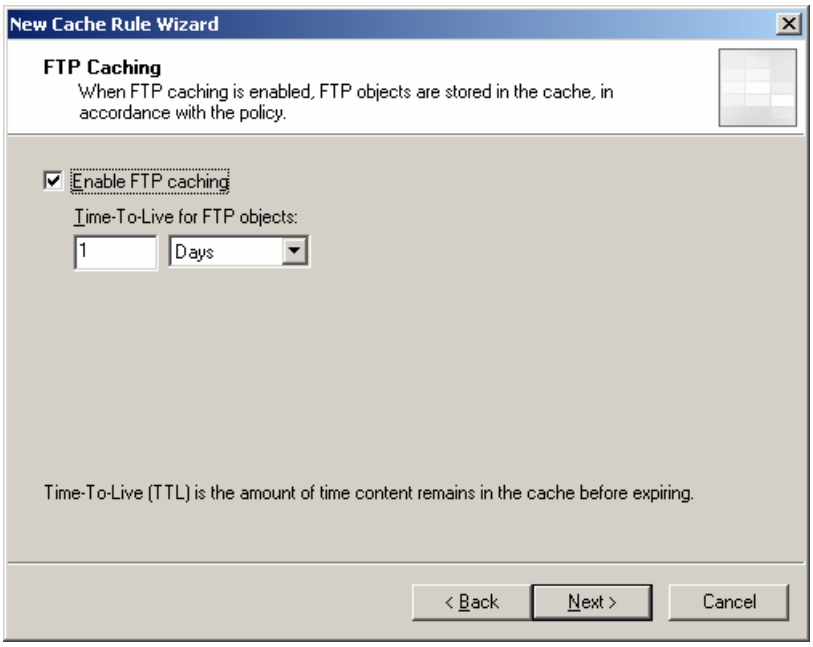
Bước 6: chọn giới hạn kích thước Cache



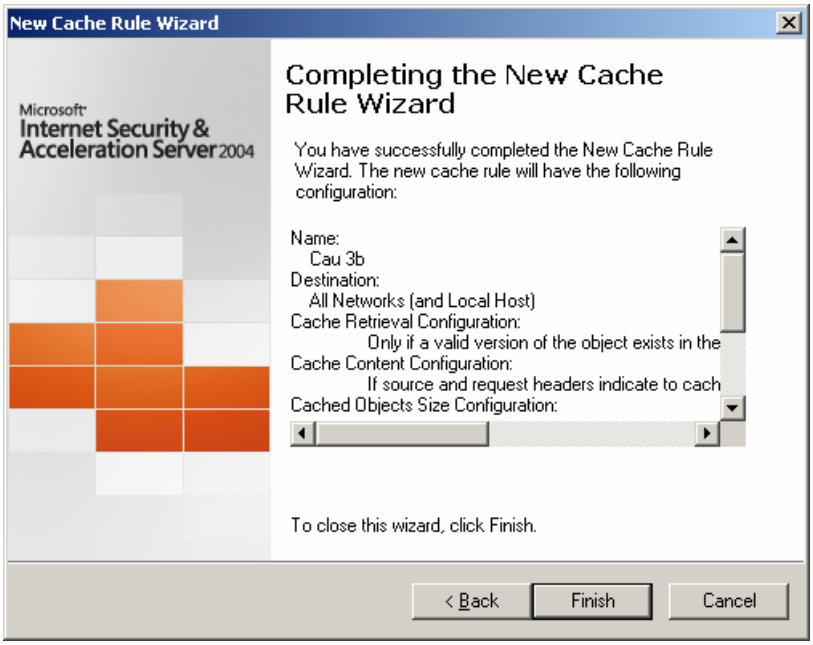
Bước 7: chỉ định thời gian lưu trữ Cache



Bước 8: chọn thời gian lưu trữ Cache Object của Cache



Bước 9: kiểm tra lại thông tin trước khi hoàn tất việc thiết lập Cache Rule



Bước 10: chọn Apply để cập nhật sự thay đổi trên ISA Server.

4. <u>Bài 4: khai báo Proxy server là máy Server1 cho máy trạm để tiến hành kiểm tra.</u>

Bài tập 05.2

Bạn là người quản trị cho một mạng máy tính cho trung tâm đào tạo tin học (có sơ đồ kết nối như hình vẽ trong **Bài tập 05.1**). Máy chủ Server1 cài Win2k3 Server và cung cấp dịch vụ Mail Server. Server2 là DNS, FTP Server cho công ty, công ty thuê một tên miền "**cscXX.edu.vn"** sau đó dùng phần mềm ISA để triển khai Firewall và cung cấp dịch vụ Proxy để protect hệ thống mạng nội bộ.

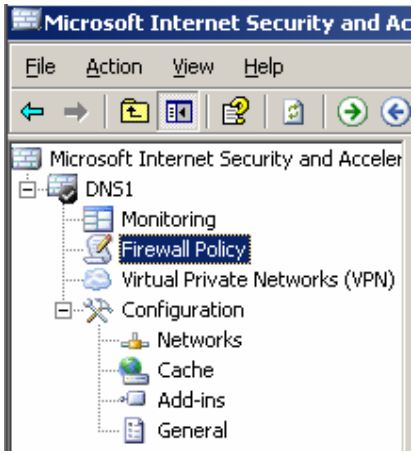
1. Bài 1: Publishing Server:

Publish Server (tham khảo giáo trình "Dịch vụ mạng Windows 2003" – chương 5 – phần V.5.2 – trang 187)

Trong giáo trình sẽ hướng dẫn cài đặt Publish Web Server và Publish Mail Server

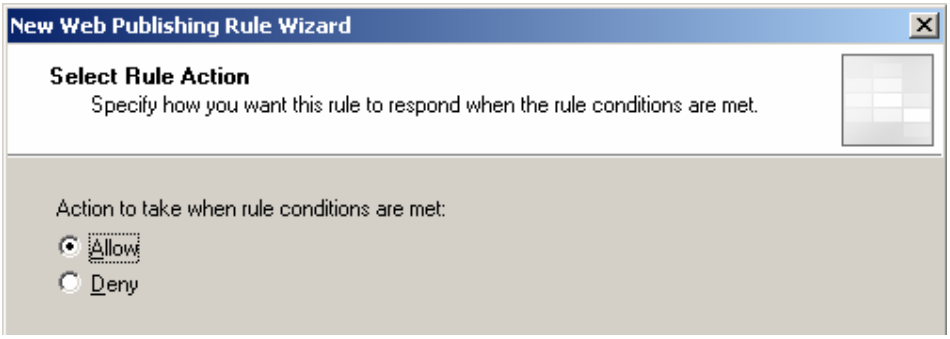
c. Cài đặt Publish Web Server

Bước 1: chạy ISA Server Management lên, chọn tên Server, kích chuột phải vào Firewall Policy



Bước 2: trên Tasks tab, chọn liên kết "Publish a Web Server", chương trình sẽ hiện lên hộp thoại "Welcome to the New Web Publishing Rule Wizard" để bạn nhập tên cho Web Publishing Rule, bạn nhập tên cho Rule (ví dụ: Publish Web Server), sau đó chọn Next để tiếp tục

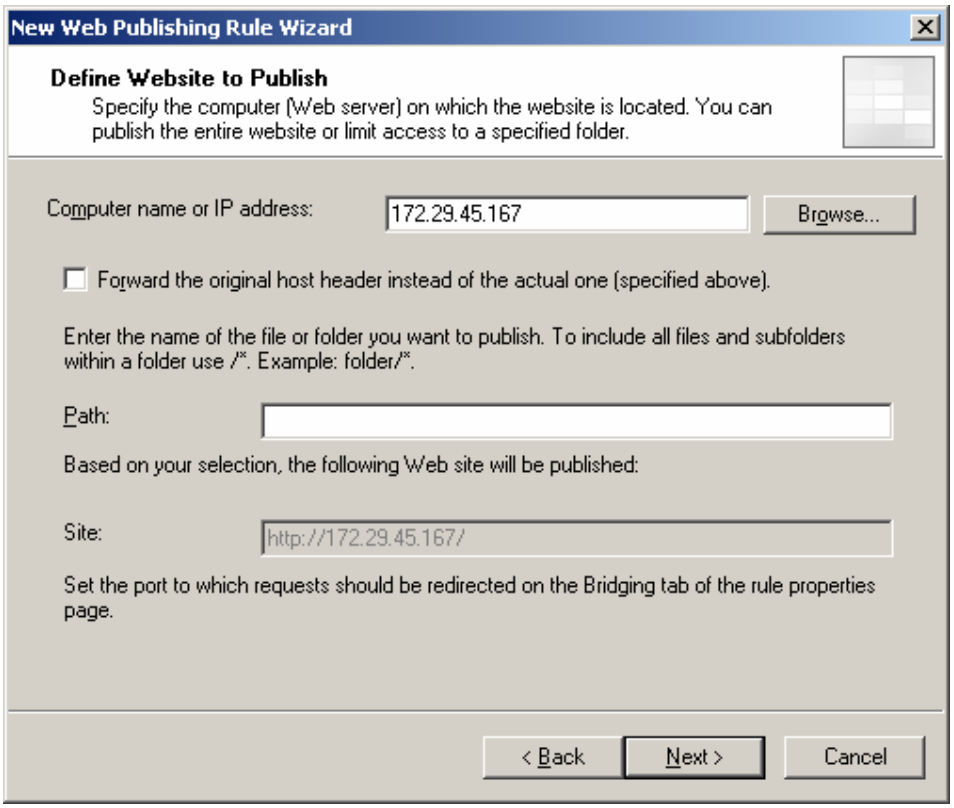
Bước 3: chọn hành động Allow, sau đó chọn Next



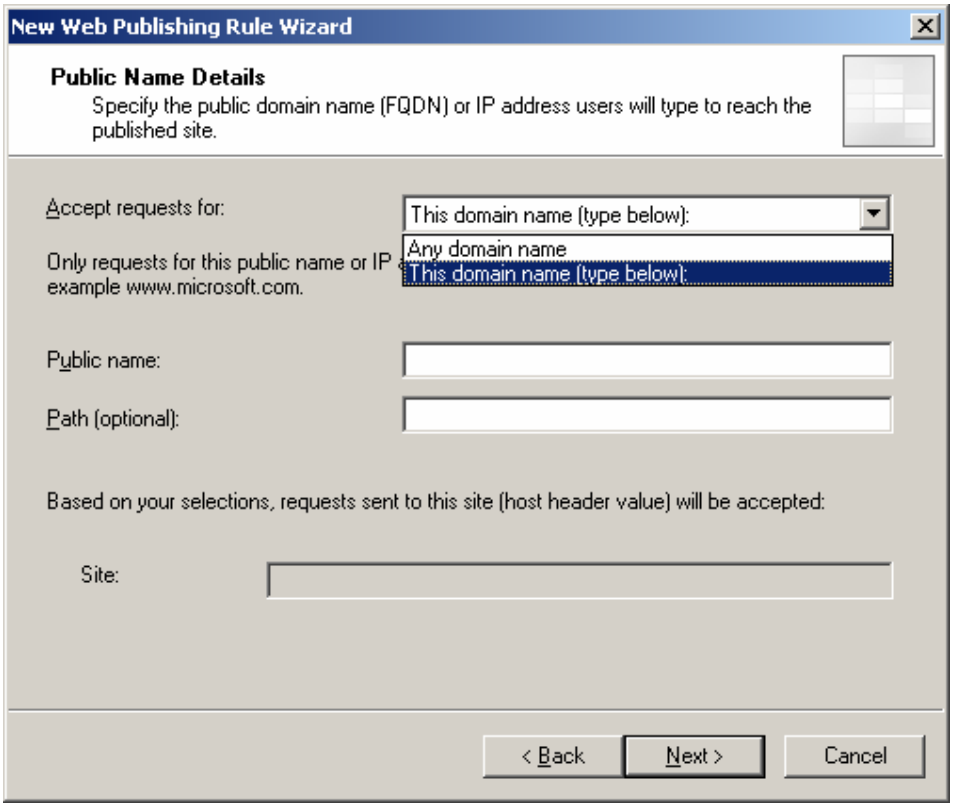
Bước 4: cung cấp một số thông tin cần khi muốn Publish Web Server:

- Địa chỉ của Web Server nội bộ
- Chỉ định Host header name (khi cần thực hiện Web Hosting cho Web Server)
- Tên file hoặc thư mục muốn truy xuất vào Web Server nội bộ
- Chỉ định tên Web Site được Publish

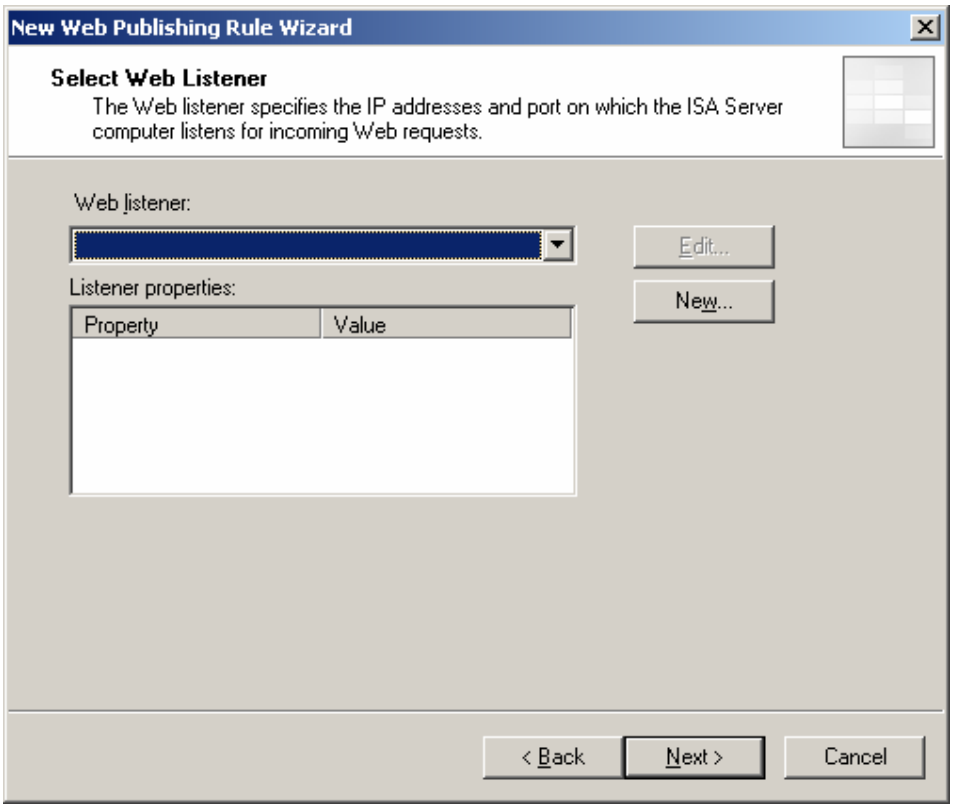
Trong trường hợp chỉ cần Publish Web Server thì bạn chỉ cần điền địa chỉ IP vào mục "Computer name or IP address"



Bước 5: trong mục Accept request fỏ, bạn chọn Any Domain Name, sau đó chọn next

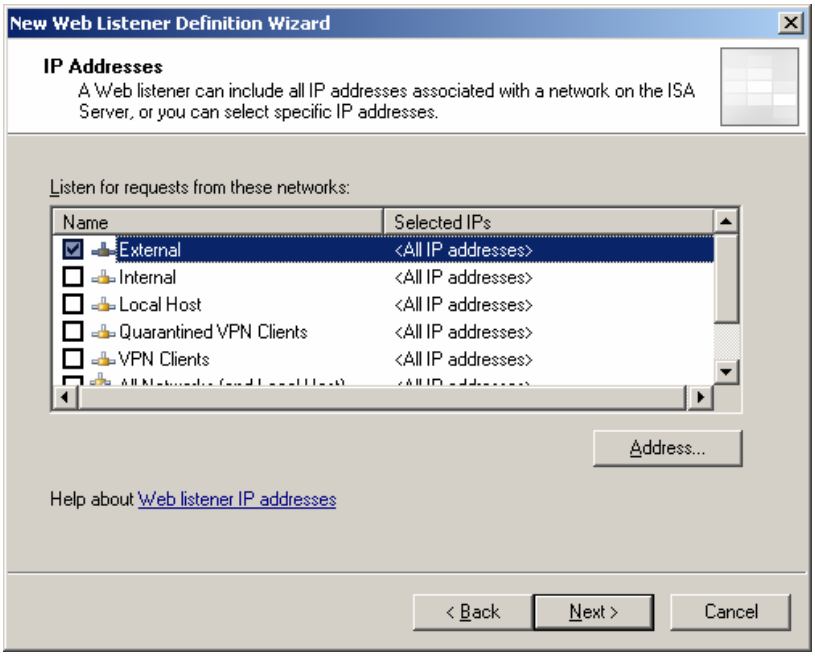


Bước 6: bạn chọn Web Listener.

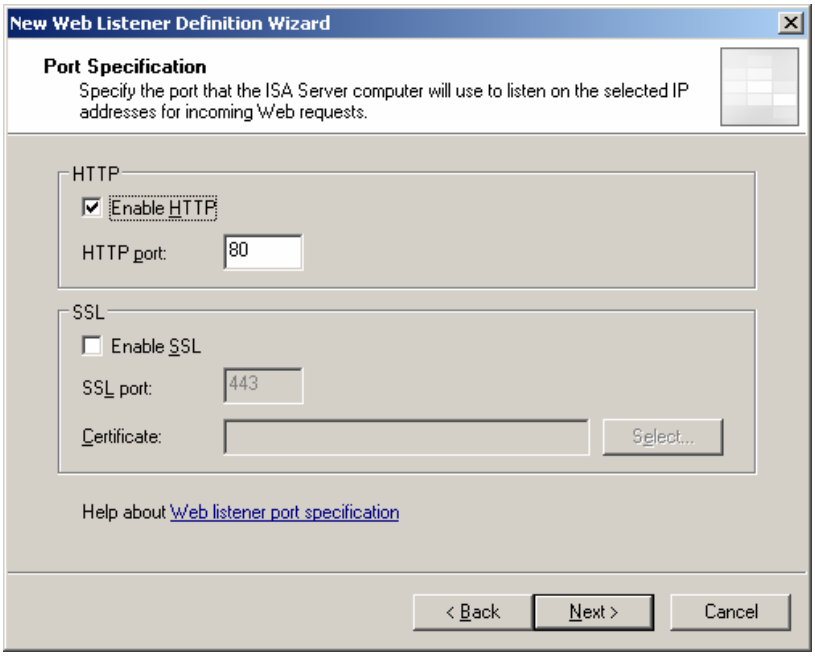


Bước 7: nếu đã có sẵn Web Listener thì bạn có thể chọn Web Listener tương ứng, nếu không thì bạn chọn New để tạo mới một Web Listener, nhập tên cho Web Listerner này và chọn Next để tiếp tục

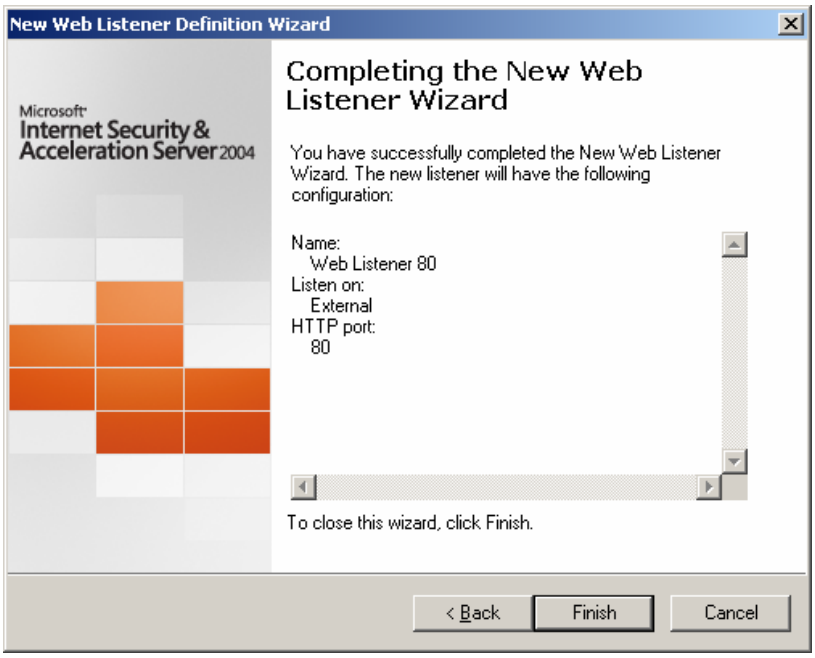
Bước 8: chọn vùng lắng nghe, do đang cấu hình Public Server nên bạn chọn vùng External. Chọn Next để tiếp tục



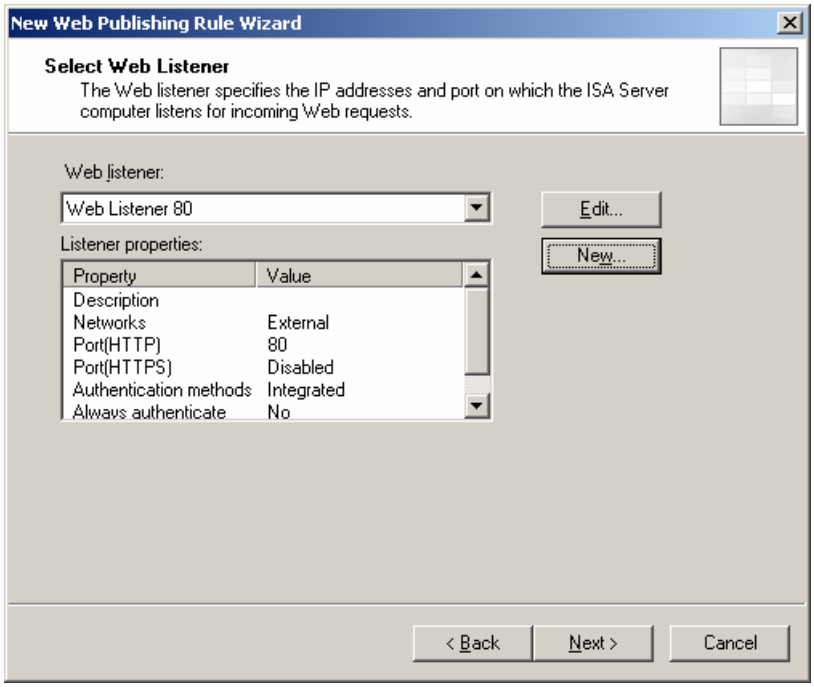
Bước 9: chọn Port lắng nghe.



Bước 10: thông tin tổng kết về Web Listener. Chọn Finish để kết thúc việc tạo mới một Web Listener

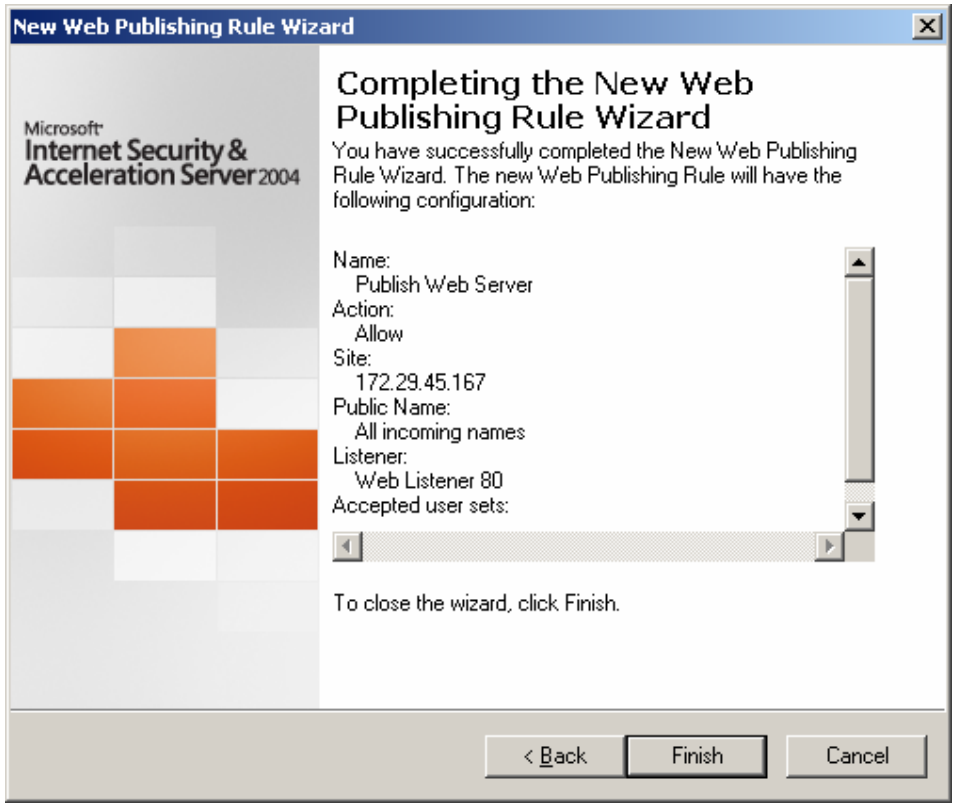


Bước 11: Web Listener vừa mới tạo sẽ tự động được chọn. Chọn Next để tiếp tục cấu hình Publish Web Server



Bước 12: chọn user sẽ bị ảnh hưởng bởi Rule này, sau đó chọn Next để tiếp tục

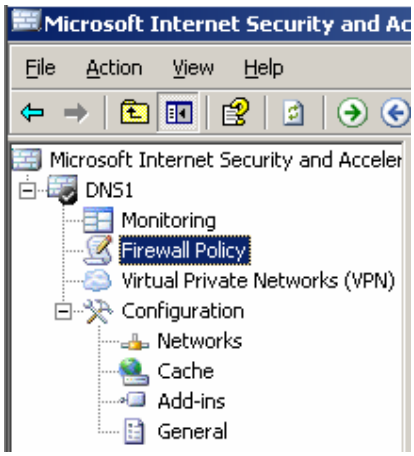
Bước 13: thông tin tổng kết về việc Publish Web Server.



d. Cài đặt Publish Mail Server

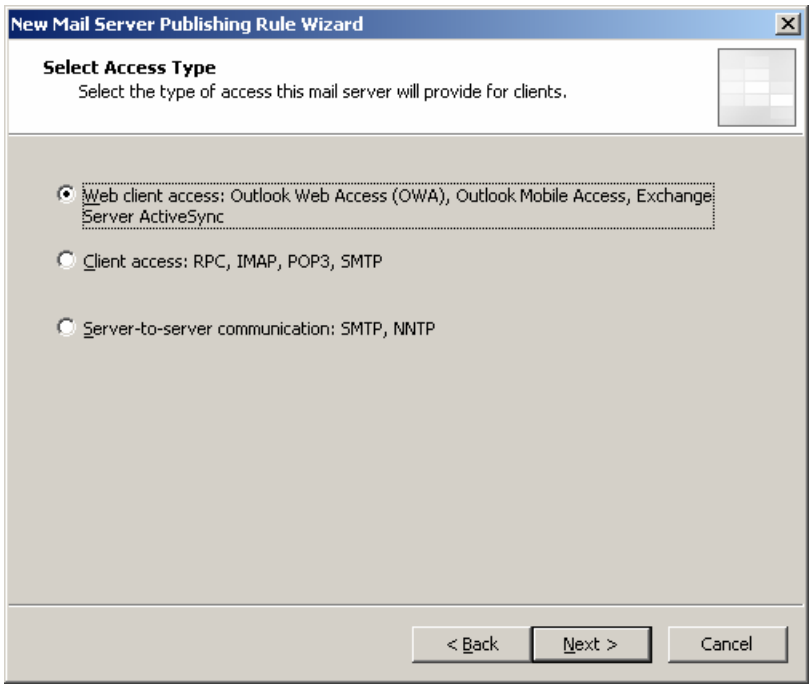
Tham khảo giáo trình "Dịch vụ mạng Windows 2003" (chương 5 – phần V.5.3 – trang 190)

Bước 1: chạy ISA Server Management lên, chọn tên Server, kích chuột phải vào Firewall Policy

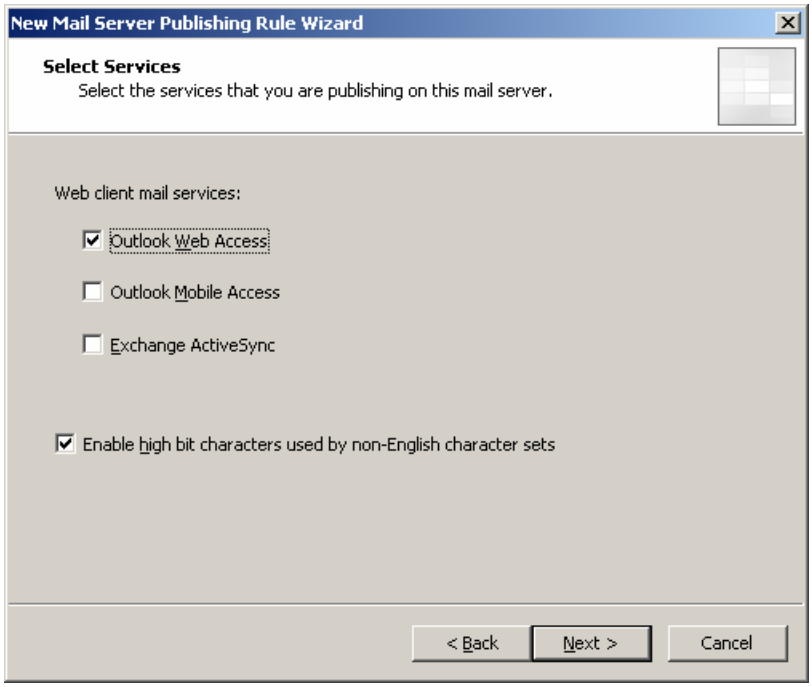


Bước 2: trên Tasks tab, chọn liên kết "Publish a Mail Server", chương trình sẽ hiện lên hộp thoại "Welcome to the New Mail Server Publishing Rule Wizard" để bạn nhập tên cho Mail Publishing Rule, bạn nhập tên cho Rule (ví dụ: Publish Mail Server), sau đó chọn Next để tiếp tục

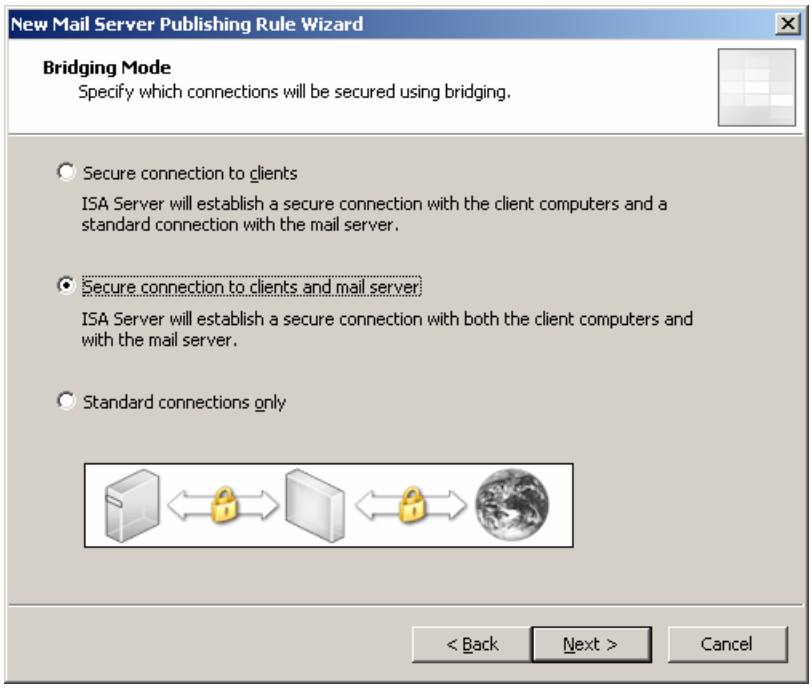
Bước 3: chọn cách thức cho phép Client truy cập vào. Giả sử chỉ muốn Client truy cập thông qua Web thì bạn chọn mục "Web Client Access", sau đó chọn Next để tiếp tục



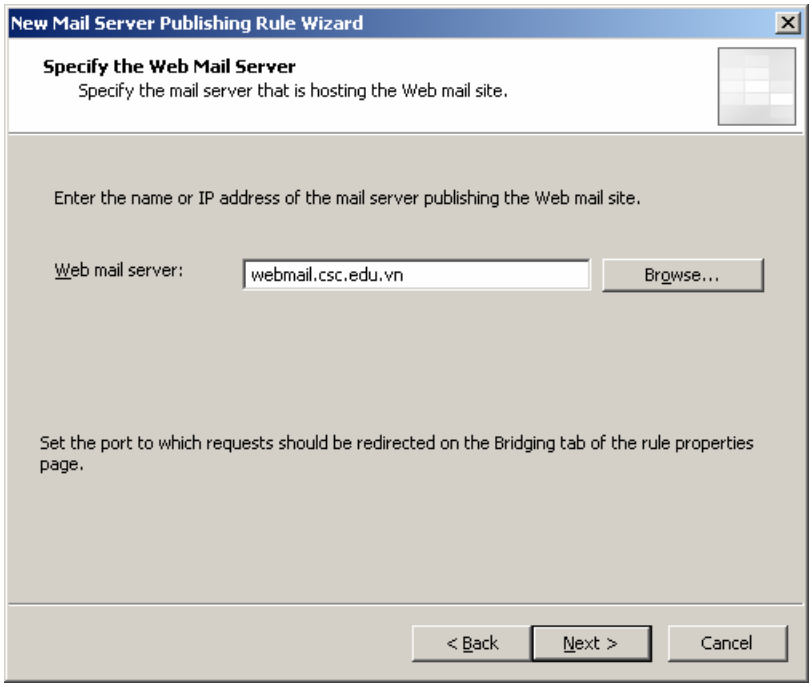
Bước 4: chọn các dịch vụ Web Exchange Service, ví dụ chỉ chọn mục Outlook Web Access, sau đó chọn Next để tiếp tục



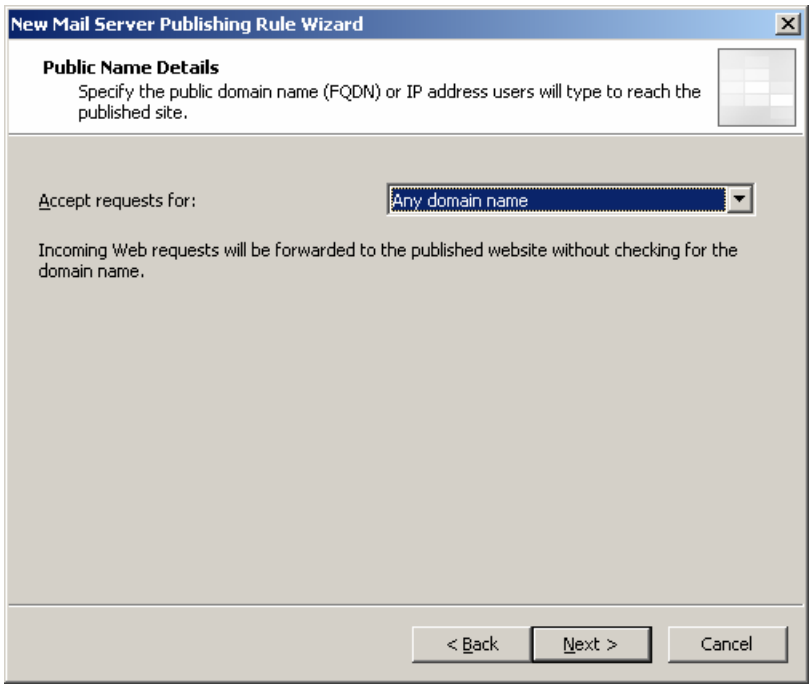
Bước 5: chọn các kết nối được bảo mật. Giả sử chọn cả 2 hướng.



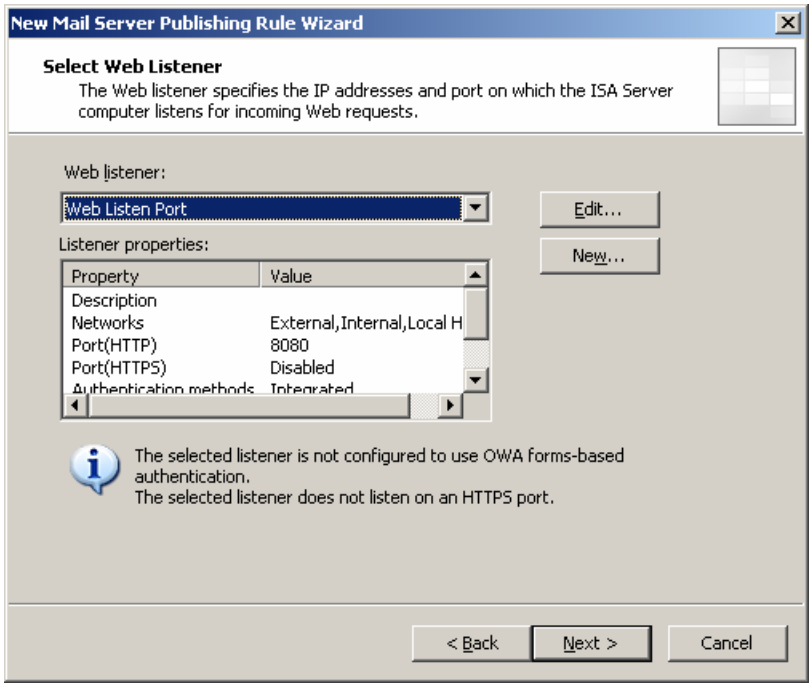
Bước 6: chọn địa chỉ mail cần Publish, chọn Next để tiếp tục



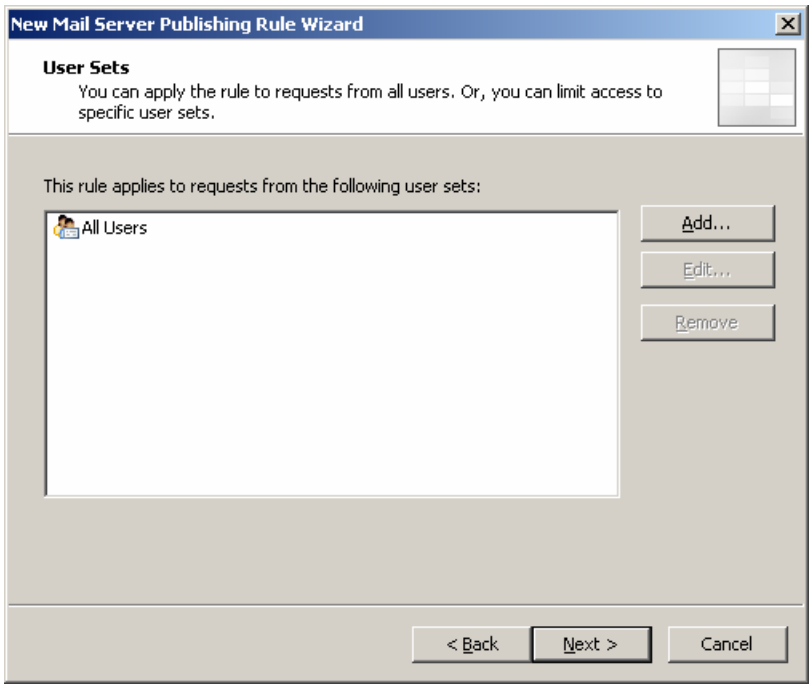
Bước 7: chọn vùng domain sẽ được chấp nhận. Bạn chọ Any Domain name khi muốn yêu cầu từ tất cả các nơi khác đều được chấp nhận



Bước 8: chọn Web Listener Port (chú ý: Port lắng nghe này phải khác với các Port đã được áp dụng)



Bước 9: chọn các user sẽ bị áp dụng



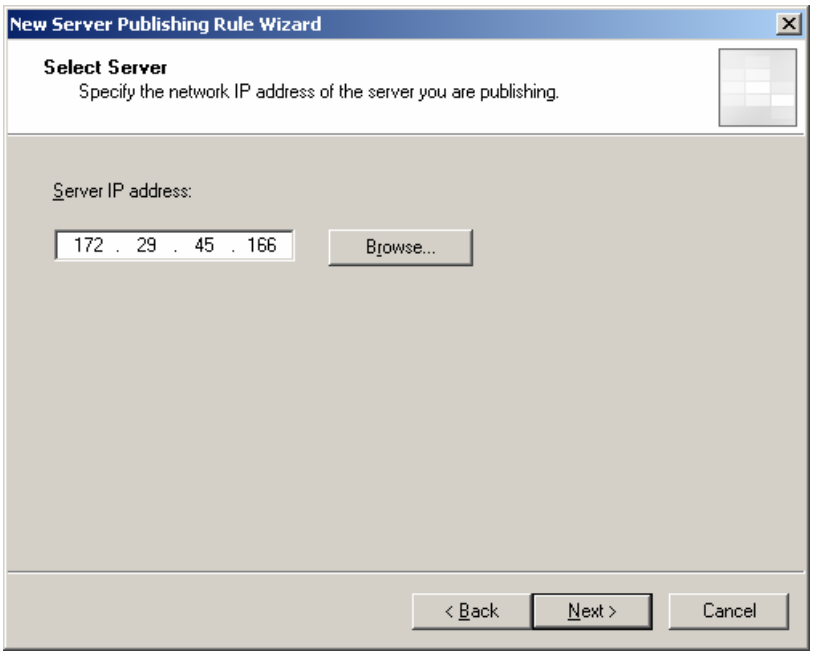
Bước 10: tổng kết quá trình Publish Mail Server

e. Cài đặt Publish FTP Server

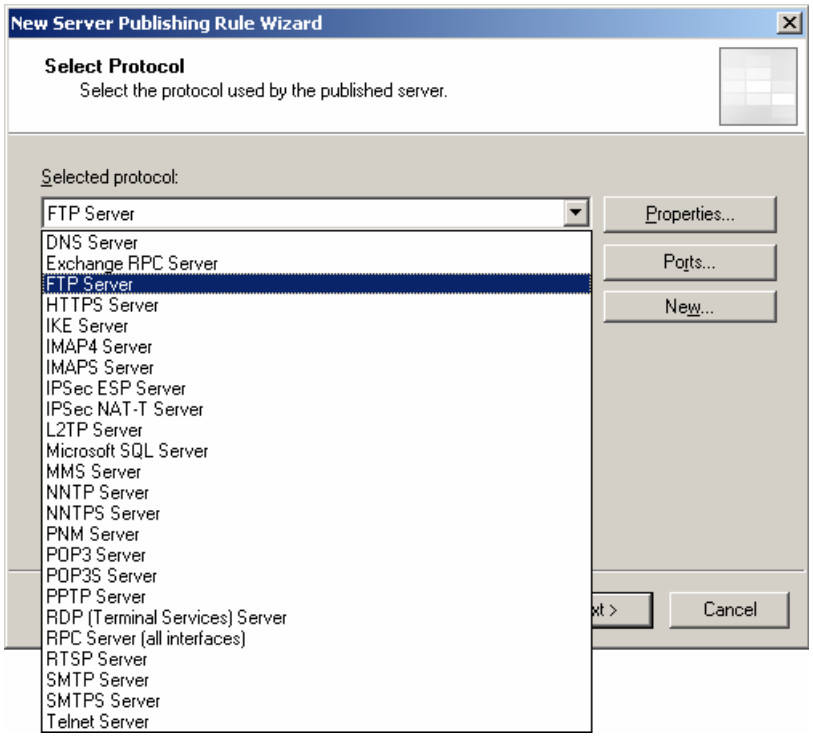
Bước 1: giống câu 1a

Bước 2: trong Task tab, chọn mục Create New Server Publishing Rule, sau đó nhập tên của Rule

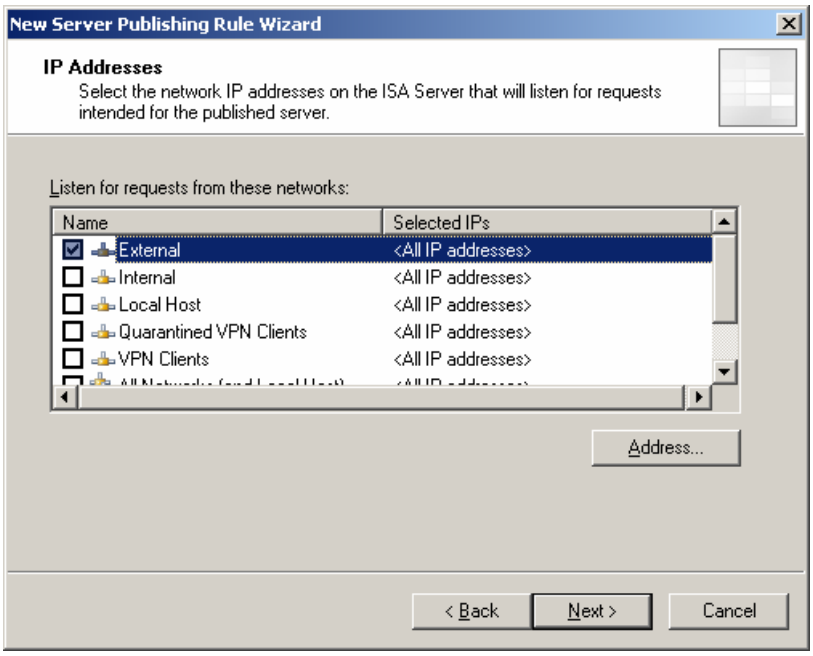
Bước 3: nhập địa chỉ IP của Server mà bạn muốn thực hiện Publish



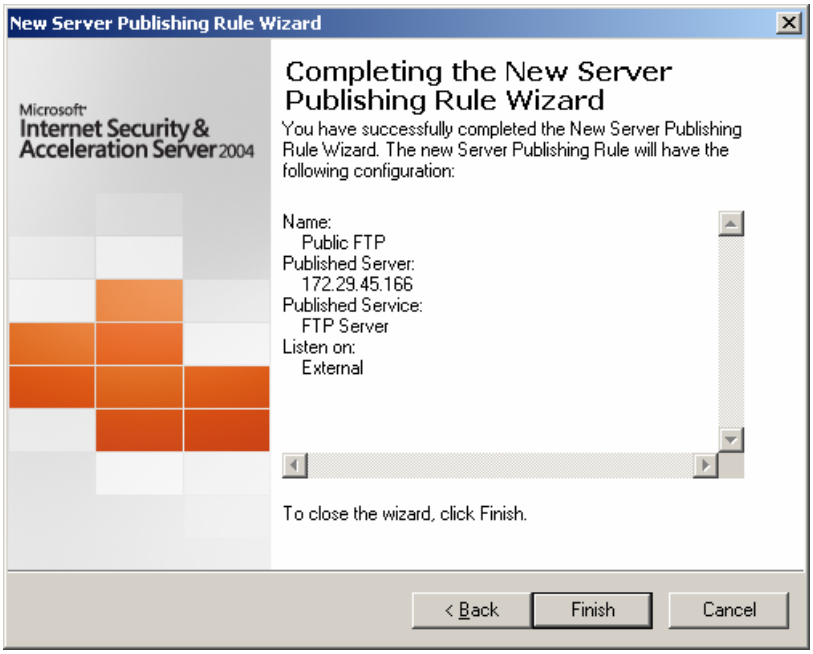
Bước 4: chọn giao thức sẽ được áp dụng. Vì đang tạo Publish FTP Server nên ta sẽ chọn giao thức FTP



Bước 5: chọn vùng sẽ lắng nghe yêu cầu FTP Server



Bước 6: bảng tổng kết về Publish FTP Server



f. Cài đặt Publish DNS Server

Tương tự câu 1c, chỉ khác ở bước 4 bạn sẽ chọn DNS Server