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



MỤC LỤC

Mộc Lộc	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	23 35
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP	23 35 38
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1	23 35 38 38
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2	23
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài tập 02.2.	23
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài tập 03.1	23
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài tập 03.1 Bài tập 03.2	23 35 38 38 51 53 53 64
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài 03 Dịch Vụ Web Bài tập 03.1 Bài tập 03.2 Bài 04 Dịch Vụ Mail	23 35 38 38 51 53 53 64 67
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài tập 03.1 Bài tập 03.2 Bài tập 04.1	23 35 38 38 51 53 53 64 67
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài 03 Dịch Vụ Web Bài tập 03.1 Bài tập 03.2 Bài tập 04.1 Bài tập 04.2	23 35 38 38 51 53 53 64 64 67 67 69
Bài tập 01.1 Bài tập 01.2 Bài 02 Dịch Vụ FTP Bài tập 02.1 Bài tập 02.2 Bài 03 Dịch Vụ Web Bài tập 03.1 Bài tập 03.2 Bài tập 04.1 Bài tập 04.2 Bài 05 Dịch Vụ Proxy	23 35 38 38 51 53 53 64 64 67 67 69 96
Bài tập 01.1	23 35 38 38 51 53 53 64 67 67 69 96



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.

≻ <u>Yêu cầu :</u>

- 1. Cài đặt dịch vụ DNS trên máy chủ dns1.
- Cấu hình dns1 là một Primary Name Server cho domain name của mình với những dữ liệu đã cho.
- 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.

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

- 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.
- Cấu hình sdns-hbc (máy thứ 4) là một Secondary Name Server cho subdomain hbc.cscXX.edu.vn.
- 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 sdnshitech quản lý
- 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.
- Cấu hình sdns-hitech (máy thứ 6) là một Secondary Name Server cho subdomain hitech.cscXX.edu.vn.
- cấu hình forwarders cho máy dns-hitech để chuyển yêu cầu phân giải miền ngoài lên máy dns1.
- 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.
- 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).
- I. 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
- 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.
- 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



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.

 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)
 - o 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 nguời 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.
- 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.





- 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)
 - o 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:
 - o 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:







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 sẳn 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.
- 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. <u>Bài 1:</u>

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. <u>Bài 2:</u>

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.

<u>Chú ý</u>:

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:

DNS1 Event Viewer Forward Lookup Zones	🚊 DNS	Reverse Lookup Zones
The Domain Name System (DNS) allows a DNS namespace about one or more contiguous DNS domains. To add a new zone, on the Action menu, click New Zone.	DNS1 Control Viewer Control	Add a New Zone
To add a new zone, on the Action menu, click New Zone.	⊡ csc02.edu.vn _msdcs	The Domain Name System (DNS) allows a DNS namespace about one or more contiguous DNS domains.
⊻iew ► New <u>W</u> indow from Here	Reverse Loo	To add a new zone, on the Action menu, click New Zone.
	<u>V</u> iew New <u>W</u> indow I	from Here
Refresh Help	Refresh Help	

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

New Zone Wizard
Zone Type The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Secondary zone Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Styb zone Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in <u>A</u> ctive Directory (available only if DNS server is a domain controller)
< Back Next Cancel Help



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).

New Zone Wizard
Active Directory Zone Replication Scope You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
O To all DNS servers in the Active Directory forest csc02.edu.vn
\odot To all <u>D</u> NS servers in the Active Directory domain csc02.edu.vn
To all domain controllers in the Active Directory domain csc02.edu.vn
Choose this option if the zone should be loaded by Windows 2000 DNS servers running on the domain controllers in the same domain.
 To all domain controllers specified in the scope of the following application directory partition:
< Back Next Cancel Help

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).

New Zone Wizard	×
Reverse Lookup Zone Name A reverse lookup zone translates IP addres	ises into DNS names.
To identify the reverse lookup zone, type the set of Network ID: Image: Transmission of the ID The network ID is the portion of the IP anetwork ID in its normal (not reversed) If you use a zero in the network ID, it we network ID 10 would create zone 10.inzone 0.10.in-addr.arpa.	he network ID or the name of the zone. addresses that belongs to this zone. Enter the order. vill appear in the zone name. For example, addr.arpa, and network ID 10.0 would create
C Reverse lookup zone name: 45.29.172.in-addr.arpa For more information on creating a reverse	lookup zone, click Help.
< Back	Next Cancel Help

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.

New Host
Name (uses parent domain name if blank):
dns1
Fully qualified domain name (FQDN):
dns1.csc02.edu.vn.
I <u>P</u> address: 172 .29 .45 .167
Create associated pointer (PTR) record
Allow any authenticated user to update DNS records with the same owner name
Ald Host Cancel

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.





🚊 DNS	csc02.edu.vn 7 record(s)		
🖻 📑 DNS1	Name	Туре	Data
🗄 📲 Event Viewer	msdcs		
Forward Lookup Zones medes csc02 edu yp	(same as parent folder)	Start of Authority (SOA)	[19], dns1., hostmaster.
	🔳 (same as parent folder)	Name Server (NS)	dns1.
H msdcs	(same as parent folder)	Name Server (NS)	dns1.csc02.edu.vn.
domain02.com	≣ dns1	Host (A)	172.29.45.167
	1 🗏 ftp	Alias (CNAME)	dns1.csc02.edu.vn
172.29.45.x Subnet	1 www	Alias (CNAME)	dns1.csc02.edu.vn

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



	csc02.edu.vn 7 record(s)		
🖻 – 📑 DNS1	Name	Туре	Data
Event Viewer Forward Lookup Zones msdcs.csc02.edu.vn csc02.edu.vn msdcs domain02.com domain02.com 172.29.45.x Subnet	Image: Construction of the second	Start of Authority (SOA) Name Server (NS) Name Server (NS) Host (A) Alias (CNAME) Alias (CNAME)	[19], dns1., hostmaster. dns1. dns1.csc02.edu.vn. 172.29.45.167 dns1.csc02.edu.vn dns1.csc02.edu.vn



Mail Exchanger (MX) Host or child domain: mail By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank. Fully qualified domain name (FQDN): mail.csc02.edu.vn. Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn. Browse Mail gerver priority: 10	w Resource Record	2
Host or child domain: mail By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank. Fully qualified domain name (FQDN): mail.csc02.edu.vn. Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn Mail gerver priority: 10	Mail Exchanger (MX)	
mail By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank. Fully qualified domain name (FQDN): mail.csc02.edu.vn. Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn. Browse Mail server priority: 10	Host or child domain:	
By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank. Fully qualified domain name (FQDN): mail.csc02.edu.vn. Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn Browse Mail gerver priority: 10	mail	1
Fully qualified domain name (FQDN): mail.csc02.edu.vn. Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn Mail gerver priority: 10	By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank.	
mail.csc02.edu.vn. Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn Mail gerver priority: 10	Fully qualified domain name (FQDN):	
Eully qualified domain name (FQDN) of mail server: dns1.csc02.edu.vn Browse Mail gerver priority: 10	mail.csc02.edu.vn.	
10	dns1.csc02.edu.vn Browse Mail server priority:	
OK Cancel	OK Cancel	



🚊 DNS	csc02.edu.vn 8 record(s)		
⊡ 📑 DNS1	Name	Туре	Data
🕀 🔃 Event Viewer	msdcs		
Forward Lookup Zones	(same as parent folder)	Start of Authority (SOA)	[24], dns1., hostmaster.
	🗐 (same as parent folder)	Name Server (NS)	dns1.
E Cococioda Min	🗒 (same as parent folder)	Name Server (NS)	dns1.csc02.edu.vn.
domain02.com	🗒 dns1	Host (A)	172.29.45.167
	🗒 ftp	Alias (CNAME)	dns1.csc02.edu.vn.
172,29,45,x Subnet	🗒 mail	Mail Exchanger (MX)	[10] dns1.csc02.edu.vn.
<u>u</u> -	I www	Alias (CNAME)	dns1.csc02.edu.vn.

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



Internet Protocol (TCP/IP) Prope	rties ?
General	
You can get IP settings assigned a this capability. Otherwise, you nee for the appropriate IP settings.	utomatically if your network supports d to ask your network administrator
O Obtain an IP address automa	atically
\sim Use the following IP address:	·
IP address:	172 . 29 . 45 . 166
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	172 . 29 . 45 . 1
C Obtain DNS server address a	utomatically
┌ ⓒ Use the following DNS server	addresses:
Preferred DNS server:	172 . 29 . 45 . 167
Alternate DNS server:	· · ·
	Ad <u>v</u> anced
	OK Cancel

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

🖎 Command Prompt - nslookup
C:\>nslookup Default Server: dns1.csc02.edu.vn Address: 172.29.45.167
> ftp.csc02.edu.vn Server: dns1.csc02.edu.vn Add r ess: 172.29.45.167
Name: dns1.csc02.edu.vn Address: 172.29.45.167 Aliases: ftp.csc02.edu.vn
> mail.csc02.edu.vn Server: dns1.csc02.edu.vn Address: 172.29.45.167
Name: mail.csc02.edu.vn
> www.csc02.edu.vn Server: dns1.csc02.edu.vn Address: 172.29.45.167
Name: dns1.csc02.edu.vn Address: 172.29.45.167 Aliases: www.csc02.edu.vn
> www.unn.un Server: dns1.csc02.edu.un Address: 172.29.45.167
DNS request timed out. timeout was 2 seconds. DNS request timed out. timeout was 2 seconds. *** Request to dns1.csc02.edu.vn timed-out >

4. Bài 4: cấu hình forwarders lên server 203.162.4.1



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

🚊 DNS	csc02.edu.vn	7 record(s)	
	Csc02.edu.vn Configure a DNS Server Create Default Application Directory Partition New Zone Set Aging/Scavenging for All Zones Scavenge Stale Resource Records Update Server Data Files Clear Cache Launch nslookup All Tasks New Window from Here Delete Refresh	7 record(s) 15 97) 97)	Type Start of Authority (SOA) Name Server (NS) Host (A) Alias (CNAME) Mail Exchanger (MX) Alias (CNAME)
	Help		

Bước 2: chọn Tab Forwarders

S1 Properties			?)
Debug Logging Interfaces	Event Loggin Forwarders	g Monitoring Advanced	Security Root Hints
Forwarders are se server. Forward q	rvers that can resolv ueries for names in th	e DNS queries not a ne following DNS dor	nswered by this nains.
DNS do <u>m</u> ain:			
All other DNS do	mains		<u>N</u> ew
			R <u>e</u> move
Selected domain'	s forwarder I <u>P</u> addres	s list:	
	<u>R</u> emov	e	
	<u>Ц</u> р		
	Down		
, Num <u>b</u> er of secon □ Do not use re	ds before forward que	eries time out: in	5
	OK	Cancel	Apply

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):

S1 Properties			?
Debug Logging Interfaces	Event Loggi Forwarders	ng Monito Advanced	ring Security
Forwarders are serv server. Forward que	vers that can resolv eries for names in t	/ ve DNS queries r he following DNS	not answered by this domains.
DNS do <u>m</u> ain:			
All other DNS dom	ains		<u>N</u> ew
			Remove
Selected domain's f	orwarder IP addre	ss list:	warder s in address
203.162.4.190	<u>R</u> emov	/e	
	<u>Ш</u> р		
	Down	n	
Number of seconds	before forward qu	ieries time out:	5
🔲 Do not u <u>s</u> e recu	ursion for this doma	ain	

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

Phân giải tên miền yahoo.com

```
🗪 C:\WINDOWS\system32\cmd.exe - nslookup
                                                                                                                                                                                                                                                    _ 🗆 🗵
                                                                                                                                                                                                                                                                    ٠
  C:\>nslookup
 Address: 203.162.4.190
       set type=any
 > yahoo.com
Server: hcm-server01.vnn.vn
Address: 203.162.4.190
  Non-authoritative answer:
                                                       /e answer:
internet address = 216.109.112.135
internet address = 66.94.234.13
MX preference = 5, mail exchanger = mx4.mail.yahoo.com
MX preference = 1, mail exchanger = mx1.mail.yahoo.com
MX preference = 1, mail exchanger = mx2.mail.yahoo.com
MX preference = 1, mail exchanger = mx3.mail.yahoo.com
  yahoo.com
  yahoo.com
 yahoo.com
yahoo.com
  yahoo.com
  yahoo.com
                                                       nameserver = ns4.yahoo.com
nameserver = ns5.yahoo.com
nameserver = ns1.yahoo.com
nameserver = ns2.yahoo.com
   yahoo.com
  yahoo.com
   yahoo.com
  yahoo.com
                                                       nameserver = ns3.yahoo.com
  vahoo.com
                                                      nameserver = ns3.yahoo.com
nameserver = ns4.yahoo.com
nameserver = ns5.yahoo.com
nameserver = ns1.yahoo.com
nameserver = ns2.yahoo.com
com internet address =
com internet address =
  yahoo.com
  yahoo.com
  yahoo.com
yahoo.com nam
yahoo.com nam
mx1.mail.yahoo.com
mx1.mail.yahoo.com
mx1.mail.yahoo.com
mx2.mail.yahoo.com
mx2.mail.yahoo.com
mx2.mail.yahoo.com
mx2.mail.yahoo.com
mx3.mail.yahoo.com
mx3.mail.yahoo.com
mx3.mail.yahoo.com
mx3.mail.yahoo.com
   yahoo.com
                                                                                  Der = ns2.yahoo.com

internet address = 4.79.181.15

internet address = 67.28.113.10

internet address = 67.28.113.11

internet address = 4.79.181.14

internet address = 4.79.181.12

internet address = 67.28.114.13

internet address = 67.28.114.35

internet address = 67.28.114.36

internet address = 64.156.215.6

internet address = 64.156.215.8

internet address = 64.156.215.18

internet address = 64.156.215.18

internet address = 67.28.113.19
                                                                                                                                                                                           18
       •
                                                                                                                                                                                                                                                             Ъ
```

Phân giải địa chỉ vnn.vn

```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\\nslookup
Default Server: hcm-server01.vnn.vn
Address: 203.162.4.190
> set type=any
> vnn.vn
Server: hcm-server01.vnn.vn
Address: 203.162.4.190
Non-authoritative answer:
vnn.vn MX preference = 10, mail exchanger = m74.vnn.vn
vnn.vn MX preference = 10, mail exchanger = m74.vnn.vn
vnn.vn nameserver = hcm-server1.vnn.vn
vnn.vn nameserver = hcm-server1.vnn.vn
vnn.vn nameserver = hcm-server1.vnn.vn
m74.vnn.vn internet address = 203.162.0.74
vdc-hn01.vnn.vn internet address = 203.162.0.11
hcm-server1.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. <u>Bài 7:</u> <u>cấu hình DDNS cho phép máy trạm khi đăng nhập mạng có thể đăng ký</u> RR trực tiếp vào DDNS Server hoặc đăng ký RR thông qua DHCP Server.</u>

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

csc02.edu.vn Pr	? ×			
WINS General	Zone Transfers Start of Authority (SDA)	Security Name Servers		
Status: Ri	inning	Paus <u>e</u>		
Туре: Ас	tive Directory-Integrated	<u>C</u> hange		
Replication: Al	DNS servers in the Active Directory	domain <u>Ch</u> ange		
Data is stored i	1 Active Directory.			
Dy <u>n</u> amic updal	es: Secure only	•		
Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.				
To set aging/s	avenging properties, click Aging.	Aging		
	ОК С	ancel <u>Apply</u>		



Bài tập 01.2



<u>Miền csc02.edu.vn</u>

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))

<u>Chú ý</u>:

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:

ame Servers	
You can select one or more name servers to host th	ie delegated zone.
Specify the names and IP addresses of the DNS ser	vers you want to have host the
delegated zone.	
Ni	
Name servers:	
Server Fully Qualified Domain Name (FQDN)	IP Address
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]
Server Fully Qualified Domain Name (FQDN) dns-hitech.csc02.edu.vn.	IP Address [192.168.10.206]

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.

New Delegation Wizard		X
	Completing the New Delegation Wizard	
	You have successfully completed the New Delegation Wizard.	
	You specified the following settings:	
	Name: hitech.csc02.edu.vn	
	To close this wizard and create the delegation, click Finish.	
	< Back Finish Cancel Help	

2. <u>Bài 2:</u> c<u>ấu hình sdns là Secondary name server cho miền csc02.edu.vn,</u> <u>hbc.csc02.edu.vn, hitech.csc02.edu.vn</u>

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

<u>Chú ý:</u> Nếu gặp thông báo lỗi sau:




The DNS server encountered a problem while attempting to load the zone. The transfer of zone data from the master server failed.

Correct the problem then either press F5, or on the Action menu, click Refresh.

For more information about troubleshooting DNS zone problems, see Help.

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

csc02.edu.vn Prope	rties	<u>? ×</u>
General	Start of Authority (SDA)	Name Servers
WINS	Zone Fransfers	Security
A zone transfer sen	ds a copy of the zone to requesti	ng servers.
Allow zone tran	sfers:	
○ <u>I</u> o any serv	er	
Only to servers listed on the Name Servers tab		
Only to the	following servers	
I <u>P</u> address:	· · Add	
192.168.1	192.168.10.202	
To specify seco Notify.	ndary servers to be notified of zo	ne updates, click <u>N</u> otify
	ОК Са	ancel <u>A</u> pply

- <u>Miền con hitech.csc02.edu.vn.</u>
- 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. <u>Bài 1:</u>

Tham khảo bài tập 01.1

2. <u>Bài 2:</u>

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)



FTP Site Creation Wizard	×
FTP Site Description Describe the FTP site to help administrators identify it.	
Type a description of the FTP site. Description: Cau a	
< <u>B</u> ack	Next > Cancel

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

FTP Site Creation Wizard	×
IP Address and Port Settings Specify an IP address and port setting for the FTP site.	
Enter the IP address to use for this FTP site: 192.168.100.204 Type the TCP port for this FTP site (Default = 21): 21	
< <u>B</u> ack <u>N</u> ext >	Cancel

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



<u>Chú ý:</u>

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

FTP Site Creation Wizard	×
FTP Site Home Directory The home directory is the root of your FTP content subdirectories.	
Enter the path to your home directory.	
Path:	
C:\Inetpub\ftproot	Browse
< <u>B</u> ack <u>N</u> ext >	Cancel

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

FTP Site Creation Wizard		×
	You have successfully completed the FTP Site Creation Wizard.	
	To close this wizard, click Finish.	
	< <u>B</u> ack Finish Car	icel

<u>Kiểm tra lại:</u>

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

😰 ftp://192.168.100.204/ - Microsoft Internet Explorer				
<u>File Edit View Favorites To</u>	ools <u>H</u> elp			
🔇 Back 👻 🕤 👻 🦻 Search	n 🜔 Folde	ers 🕼 🎯 🗙 🍫		
Address 👰 ftp://192.168.100.204/				
Name 🔺	Size	Туре	Modified	
on thuc hanh 1-2.doc	23.5 KB	Microsoft Word Doc	6/9/2005 12:34 PM	



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:

cau a Properties	? ×
FTP Site Security Accounts Messages Home Directory Directory Security	
Allow anonymous connections	_]
Use the following Windows user account for anonymous access:	
User name: SERVER1\IUSR_NQBINH Browse	
Password:	
Allow only anonymous connections	
OK Cancel <u>A</u> pply He	ip

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.

cau a Properties	? X
FTP Site Security Accounts Messages Home Directory Directory Security	
Allow anonymous connections	
Use the following Windows user account for anonymous access:	
User name: SERVER1\IUSR_NQBINH Browse]
Password:	
I Aljow only anonymous connections	
OK Cancel Apply H	elp

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.

cau a Properties	<u>?</u> ×
FTP Site Security Accounts Messages Home Directory Directory Security	
FTP site messages	
Banner:	_
Welcome:	
Xin chào các bạn đã đến FTP Server của chúng tôi !	
E⊻it:	
Hẹn gặp lại lần sau	
Maximum connections:	
OK Cancel Apply He	ih.

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

cau a Properties	? ×
FTP Site Security Accounts Messages Home Directory Directory	Security
TCP/IP address access restrictions	
By default, all computers will be: 🥑 💽 Granted access	
Except those listed below: 🕄 🖸 Denied access	
Access IP address (Subnet mask)]
	<u>Ad</u> d
	Re <u>m</u> ove
	<u>E</u> dit,
OK Cancel Apply	Help

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

Grant Access	<u>.</u>
Туре:	
Single computer	
C Group of computers	
IP address:	
192 . 168 . 100 . 203	DNS Lookup
192 . 168 . 100 . 203	D <u>N</u> S Lookup



cau a Properties	? ×
FTP Site Security Accounts Messages Home Directory Directory S TCP/IP address access restrictions By default, all computers will be: Image: Computers of the second secon	Add
OK Cancel Apply	Help

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.

Virtual Directory Creation Wizard			×
Virtual Directory Alias Specify a short name, or alias, for this virt	tual directory.		
Type the alias you want to use to gain a naming conventions that you would for n	ccess to this virtu aming a directory	al directory. Use	the same
<u>A</u> lias: download			
	< <u>B</u> ack	Next >	Cancel

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

tual Directory Creation Wizard			2
TP Site Content Directory Where is the content you want to publish o	n the FTP site	?	
Enter the path to the directory containing the	ne content for I	this FTP site.	
Path:			
c:\Soft			Browse
	< Back	Next >	Cancel

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.

Virtual Directory Creation Wi	zard	×
	You have successfully completed the Virtual Directory Creation Wizard.	
	To close this wizard, click Finish.	
	< <u>B</u> ack Finish Can	cel

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:

🔯 ftp://192.168.100.204/ - Microsoft Internet Explorer				
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u>	ools <u>H</u> elp			
🔇 Back 👻 🕤 👻 🥬 🔎 Searc	:h 🌔 Folders 🛛 🕼 沙 🗙 🛎	2 ⊞-		
Address 2 ftp://192.168.100.204/				
Name 🔺 Size Type Modified				
on thuc hanh 1-2.doc	23.5 KB Microsoft Word Doc	6/9/2005 12:34 PM		

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

🗙 ftp://192.168.100.204/download/ - Microsoft Internet Explorer					
<u>File Edit V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp					
😋 Back 🝷 🕘 👻 🏂 🔎 Search 💫 Folders 🛛 🎲 🎯 🗙 🏹 🛄 🕇					
Address Aftp://192.168.100.204/download/					
Name 🔺	Size	Туре	Modified		
20051129-016-x86.exe	12.2 MB	Application	11/29/2005 8:33 PM		
MP9Setup.exe	13.3 MB	Application	12/12/2002 3:56 AM		
WM9Codecs.exe	1.35 MB Application 11/30/2005 8:11 AM				
WMBonusXP.exe	18.2 MB	Application	12/12/2001 1:27 AM		
WMEncoder.exe	9.45 MB	Application	12/12/2002 3:43 AM		

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



FTP Folde	er Error
8	An error occurred opening the folder on the FTP Server. Make sure you have permission to access this folder.
-	Details: 550 /soft: The system cannot find the file specified.
	()

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

Virtual Directory Creation Wizard			
Set the access permissions for this virtual of	directory.		E
Allow the following permissions:			
✓ <u>B</u> ead			
To complete the wizard, click Next			
	< Back	Next>	Cancel

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



o Các user còn lại có quyền đọc

Tham khảo hình sau:

ebdata Properties		2
General Sharing Security	Customize	
<u>G</u> roup or user names:		
CREATOR OWNER		
🖉 Users (SERVER1\Use	us)	
🕺 🥵 webmaster (SERVER1	\webmaster)	
1	1	
	Add <u>B</u> emove	;
Permissions	Allow Deny	
Full Control		
Modify		
Read & Execute		
List Folder Contents		
List i older contents		
Read		
Read		_
Read Write		-
Read Write For special permissions or for click Advanced	r advanced settings, Advanced	
Read Write For special Permissions or for click Advanced.	r advanced settings, Advanced	• •
Read Write For special Permissions or for click Advanced.	r advanced settings, Advanced	• •

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. <u>Bài 2:</u> c<u>ài đặt và cấu hình DNS trên dns1 là Primary name server của miền cscXX.edu.vn với:</u>

- o ftp.cscXX.edu.vn. Alias (CNAME) server1.cscXX.edu.vn.
- o vftp.cscXX.edu.vn Host (A) 172.16.XX.1

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

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"



- o 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

FTP Site Creation Wizard
FTP User Isolation Restrict FTP users to their own FTP home directory.
FTP user isolation prevents users from accessing the FTP home directory of another user on this FTP site.
Important: Because you cannot change the user isolation option after creating this FTP site, you should read about FTP user isolation in the IIS product documentation before choosing an isolation option.
 Do not isolate users (Users can access the FTP home directory of other users.)
 Isolate users (Users must be assigned an FTP home directory within the root of this FTP site.)
 Isolate users using Active Directory (Users must be assigned an FTP home directory that is configured using their Active Directory user account.)
< <u>B</u> ack <u>N</u> ext > Cancel

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

Web Site Creation Wizard			×
Web Site Desciption Describe the Web site to help administrators in	dentify it.		
Type a description of the Web site.			
Description:			
Site Chinh	_		
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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.

Web Site Creation Wizard	×
IP Address and Port Settings Specify an IP address, port setting, and host header for the new Web site.	
Enter the IP address to use for this Web site:	
172.29.14.141	
ICP port this Web site should use (Default: 80): 80 Host header for this Web site (Default: None):	
For more information, read the IIS product documentation.	
< <u>B</u> ack <u>N</u> ext >	Cancel

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.

Web Site Creation Wizard	×
Web Site Home Directory The home directory is the root of your Web content subdirectories.	
Enter the path to your home directory.	
<u>P</u> ath:	
c:\webdata	Browse
☑ Allow anonymous access to this Web site	
< <u>B</u> ack <u>N</u> ext >	Cancel

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.

Web Site Creation Wizard 🛛 🔀
Web Site Access Permissions Set the access permissions for this Web site.
Allow the following permissions:
Run scripts (such as ASP)
Execute (such as ISAPI applications or CGI)
☐ <u>W</u> rite
E Browse
To complete the wizard, click Next .
< <u>B</u> ack <u>N</u> ext > Cancel

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

Site Chinh Prope	erties		<u>?</u> ×			
Web Site	Performance	ISAPI Filters	Home Directory			
Documents	Directory Security	HTTP Headers	Custom Errors			
Enable def	ault <u>c</u> ontent page ix.htm ault.htm dex.htm	<u> </u>	jd			
	Move Up	Mo <u>v</u> e Down				
Enable document footer Append an HTML formatted footer to every document your Web server returns.						
		Bro	WSC			
	ОК	Cancel Apply	/ Help			

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.

Virtual Directory Creation Wizard	X
Virtual Directory Alias Specify a short name, or alias, for this virtual directory.	1 and
Type the alias you want to use to gain access to this Web virtual directory. L same naming conventions that you would for naming a directory.	lse the
Alias: Daotad	
< <u>B</u> ack <u>N</u> ext>	Cancel

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.



tual Directory Creation Wizard	
/eb Site Content Directory Where is the content you want to publish on the V	Web site?
Enter the path to the directory that contains the co	ontent for this Web site.
<u>P</u> ath:	
c:\daotao	Browse
,	
< P	Pack Nevt Cancel

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

Virtual Directory Creation Wizard 🛛 🔀
Virtual Directory Access Permissions Set the access permissions for this virtual directory.
Allow the following permissions:
✓ Bead
Run scripts (such as ASP)
Execute (such as ISAPI applications or CGI)
☐ <u>W</u> rite
E Browse
To complete the wizard, click Next .
< <u>B</u> ack <u>N</u> ext > Cancel

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) <u>Chú ý:</u>

Virtual Directory Creation Wizard	×
Virtual Directory Access Permissions Set the access permissions for this virtual directory.	
Allow the following permissions:	
✓ Bead	
✓ Run scripts (such as ASP)	
<u>Execute</u> (such as ISAPI applications or CGI)	
□ <u>W</u> rite	
To complete the wizard, click Next .	
< <u>B</u> ack <u>N</u> ext >	Cancel

Chon 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)

d:\soft		? ×
Security		
Group or user names: Administrators (BINH\Admini CREATOR OWNER SYSTEM Users (BINH\Users)	strators)	
, Permissions for Administrators	Add	<u>R</u> emove Denv
– Full Control Modify Read & Execute List Folder Contents Read Write	222	
For special permissions or for adva click Advanced.	anced settings,	Advanced
	OK	Cancel

- 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

IF	9 Address a	nd Domain Name	e Restrictions	×
	□IP address ac By default, al Except the fo	cess restrictions l computers will be: llowing:	C Granted access	
	Access	IP address (Subnet	mask)]
				<u>Add</u>
				Re <u>m</u> ove
				Ediţ,
		ОК	Cancel <u>H</u> elp	

Bước 3: chọn mục Granted access, chọn Add

Deny Access	×
Туре:	
O Single computer	
Group of computers	
C Domain name	
Network ID: Subnet mask:	
192 . 168 . 12 . 0 255 . 255 . 255 . 0	
OK Cancel <u>H</u> elp	



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

IP Address and	l Domain Name	e Res	trictior	IS	2
☐ [] IP address acces	ss restrictions				
By default, all co	omputers will be:	3	🖲 G <u>r</u> anl	ed access	
Except the follo	wing:	- 🔒	O De <u>n</u> ie	d access	
Access I	P address (Subnet	mask)			
🔒 Denied 📲	<u>a</u> 192.168.12.0 (2	255.25	5.255.0)		(A <u>d</u> d
					Re <u>m</u> ove
					Edi <u>t</u>
1					
	ок	Car	icel	Help	

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

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

World Wide Web Service	×					
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.						
Sub <u>c</u> omponents of World Wide Web Service:						
🗹 🔊 Active Server Pages	0.0 MB 🔺					
🔲 🔲 Internet Data Connector	0.0 MB					
🗹 📷 Remote Administration (HTML)	5.7 MB					
🔲 📴 Remote Desktop Web Connection	0.4 MB					
Server Side Includes	0.0 MB					
🔲 🗟 WebDAV Publishing	0.0 MB					
🔽 🧖 World Wide Web Service	1.9 MB 🗾					
Description: Includes support for remote administration of IIS Web servers over the Internet.						
Total disk space required: 2.9 MB	Details					
Space available on disk: 4000.8 MB						
ОК	Cancel					

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).



<u>Chú ý:</u>

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

Windows Compon	ents Wizard		×			
W 1 0				Size	<u>61.71MB</u>	
Windows Compo	nents			' 'sed	rarely	
You can add (Application Serve	5.P		¥II.	· · · · · ·	
		Internet Inform	World Wide Web Service			×
	To add or remove a					
To add or rem	of the component wi	I o add or remove a	To add or remove a component, c	lick the check box.	A shaded box me	ans that only part
part of the cor	Subcomponents of A	or the component w	of the component will be installed.	To see what's inclu	ided in a compone	ent, click Details.
Details.	Cabgoniperion S	Sub <u>c</u> omponents of	Subcomponents of World Wide W	/eb Service:		
Components:		🗆 較 FrontPage :	Active Server Pages			0.0 MB
	Morther Martiner	🗹 🚡 Internet Info	🔲 🔊 Internet Data Connector			0.0 MB
	Enable netw	🗆 🅁 Internet Prir	Remote Administration (HT	TML)		5.7 MB
Certific			Bernote Deskton Web Co	nnection		0.4 MB
			Server Side Includes	(Infoction)		0.41.15
	🗌 🚅 Message Qu					
ILL (@@ Eax 5)		M S World Wide	WebDAV Publishing			U.U MB
Description: 1			🛛 🗹 🚑 World Wide Web Service	1		1.9 MB 🗾
¢.	Description: IIS In	Descriptions A				
Total disk spa	TOFFI	Description: A co Web	Description: Allow ASP files, Ac	otive Server Pages i	s always installed.	
Space availab	Total disk space reg					
	Space available on (Total disk space rev	Total disk space required:	2.9 MB		Dieteile
	Space available of the	Space available on	Space available on disk: 4	4009.5 MB		Detaile
				000.0 MB		
					OK	Cancel
-						

Phải hiệu chỉnh lại trang mặc định là default.asp

forum Properties ?X
Virtual Directory Documents Directory Security HTTP Headers Custom Errors
Enable default content page
default.asp Add Remove
Move Up Ma <u>v</u> e Dawn
Enable document footer Append an HTML formatted footer to every document your Web server returns.
Browse,
OK Cancel Apply Help

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



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. <u>Bài 1:</u>

Tham khảo Bài tập 1 (Dịch vụ DNS)

2. <u>Bài 2:</u>

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)

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. <u>Bài 5: sử dụng tập lệnh SMTP & POP3 để thực hiện quá trình send/receive</u> 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 <u>thanh@csc.com</u> gởi mail đến <u>nvbinh@csc.com</u> (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

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

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.

lbox Store (¥HOST)	Propertie	5			?
Details	P	olicies		S	ecurity
General Da	tabase	Limits		Full-Te	ext Indexing
Storage limits					
✓ Issue warning all	(KB):			204	180
Prohibit send at (KB):					
Prohibit send and receive at (KB):					
Warning message inter⊻al:					
Run daily at Midnight					
Deletion settings					
Keep deleted items	ior (days):			0	
Keep deleted <u>m</u> ailboxes for (days):					
Do not permanently delete mailboxes and items until the store has been backed up					
L					
OK		ancel	Ap	oly	Help

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:

<u>Cách 1:</u> 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.

I	눰 First Organization (Exchange)	Mailt	boxes		
l	🖻 📴 Global Settings	Mail	box 🔻	Last Logged on By	Size (
l	Internet Message Formats	t	dnhon	CSC\tdnhon	2
l	Message Delivery	🔠 S	SystemMailbox{02FD102	NT AUTHORITY\SYSTEM	361
l		📇 S	öystem Attendant	NT AUTHORITY\SYSTEM	0
l	Administrative Groups	🛗 S	MTP (VHOST-{02FD1020	NT AUTHORITY\SYSTEM	0
l	🗄 🎯 First Administrative Group		ivbinh	NT AUTHORITY'SYSTEM	2
l	🖻 🧊 Servers	l 📸 h	102	Exchange rasks	14
l	🖻 🖷 🚦 VHOST	🧰 h 🗔 a	1V01	' <u>H</u> elp 'N	93
l			Connector for Lotus Note		0
I	Hirst Storage Group		Laiendar Connector (VHO	NT AUTHORITY (SYSTEM	0
1		- Carl H	Authiniscrator	COCIACIAININGCIACUT	237



Available Tasks		
The following is a list of tasks that can be a objects. Select the desired task and press N	pplied to one or more of the selected Next.	
Select a task to perform:		
🗃 Move Mailbox		
🔁 Delete Mailbox		
Configure Exchange Features	·····	
	43	
– Task Description		
Allows you to enable, disable and set pror	perties in Exchange Features.	
, man , , , , , , , , , , , , , , , , , , ,		
	<back next=""></back>	Cancel

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:

Mobile Services Enabled Outlook Mobile Access Enabled Isabled Disabled Outlook Mobile Access Disabled Protocols Disabled, using protocol defaults. POP3 Enabled, using protocol defaults. IMAP4 Enabled, using protocol defaults.		
Outlook Mobile Access Enabled User Initiated Synchronization Usabled Up-to-date Notifications Disabled Protocols Outlook Web Access Enabled, using protocol defaults. POP3 Enabled, using protocol defaults. APIP3 Enabled, using protocol defaults. APIP3 Enabled, using protocol defaults. APIP3 APIP3		Fueld
Image: Section and the section of t	Utlook Mobile Access	Enabled Disabled
* Protocols Image: Second	a Up-to-date Notifications	Disabled
Outlook Web Access Enabled, using protocol defaults. POP3	* Protocols	
POP3 Enabled, using protocol defaults. Af IMAP4 Enabled, using protocol defaults.	Soutlook Web Access	Enabled, using protocol defaults.
A Enabled, using protocol defaults.	🛋 POP3	Enabled, using protocol defaults.
	at IMAP4	Enabled, using protocol defaults.

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

Task In Progree The task is be	ss eing performed.			
Progress report:				
Object	State	%	Duration (sec)	Status
🔮 tdnhon		100 %	0.282	The op
Task finished.				

Bước 5: chọn Finish để kết thúc

😤 Exchange Task Wizard		×
	Completing the Exchange Task Wizard	
	Task Summary: Configure Exchange Features	
$\langle \mathbf{x} \rangle$	Results: Errors: 0 Successes: 2 Warnings: 0	
	View detailed report when this wizard closes	
	< Back Finish Cancel	

<u>Cách 2:</u> 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
🍜 Active Directory Users and Comp	uters	
🎻 Eile Action View Window He	łp	_B×
← → 🗈 💽 🐰 💼 🗙 😭	12 🗟 😰 🦉 🎆 🐚 🖓 🍕 🗑	
Active Directory Users and Computer:	Users 35 objects	
🗄 💼 Saved Queries	Name	Туре
⊡-∰ csc.com	🕵 Admin	Security Group - Global
ti 🔁 Ruiltin	🖸 Administrator	User
	Cert Publishers	Security Group - Domain Local
Tomain Controllers	DHCP Administrators	Security Group - Domain Local
	DHCP Users	Security Group - Domain Local
	2 DnsAdmins	Security Group - Domain Local
	2 DnsUpdateProxy	Security Group - Global
, i i i i i i i i i i i i i i i i i i i	Domain Admins	Security Group - Global
	Domain Computers	Security Group - Global
	Domain Controllers	Security Group - Global
	Domain Guests	Security Group - Global
	💯 Domain Users	Security Group - Global
	Enterprise Admins	Security Group - Global
	Exchange Domain Servers	Security Group - Global
	Exchange Enterprise Servers	Security Group - Domain Local
	Exchange Services	Security Group - Global
	GiamDoc	Security Group - Global
	Group Policy Creator Owners	Security Group - Global
	See Guest	User 🚽

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

	🕵 IWAM_VHOST		
l	🙎 ntmthao	Add to a group	
l	🕵 nttdung	Di <u>s</u> able Account	
l	🙎 nvbinh	Enable Account	
l	🕵 PhongMay	Mo <u>v</u> e	
	🕵 RAS and IAS Si	Exchange Tasks.	

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...

Administrative Groups First Administrative Gr First Administrative Gr Servers First Administrative Gr First Administr	roup		
⊕ i Tools	C <u>o</u> nnect to View <u>S</u> ystem Folders Send Hi <u>e</u> rarchy		
	New	•	Public Folder
	<u>V</u> iew New <u>W</u> indow from Here	•	



Properties ?	×
General Replication Limits Details	
Name: Publick	
Path:	
/	
P <u>u</u> blic folder description:	
Maintain per-user read and unread information for this folder	
OK Cancel Apply Help	

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

Public Properties
General Replication Limits Details
Storage limits Use public store defaults Issue warning at (KB):
Image: Prohibit post at (KB): Image: Imag
Deletion settings
✓ Use public store defaults
Keep deleted items for (days):
Age limits
✓ Use public store defaults
Age limit for replicas (days):
(used if the public folder store does not have an age limit)
OK Cancel Apply Help

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

 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

	Recipient Filteri	ng Details
General	Defaults	Sender Filtering
ock messages that cla	im to be from the following	senders.
	-	
enders:		
	k.	
	, , , , , , , , , , , , , , , , , , ,	
Add	lit <u>R</u> emove	
Add Ec	it <u>R</u> emove	
Add Ec Archive filtered mess Filter messages with	dit <u>R</u> emove ages <u>b</u> lank sender	
Add Ec Archive filtered mess Filter messages with Drog connection if a	dit <u>R</u> emove ages blank sender ddress matches filter	
Add Ec Archive filtered mess Filter messages with Drog connection if a Accept messages wi	dit <u>R</u> emove ages blank sender ddress matches filter thout notifying sender of fil	tering

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

Add Sender		×
<u>S</u> ender:		
abc@yahoo.com		
		1
	OK	Cancel

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

essage Delivery Proper	ties	3	2
Connection Filtering	Recipient Filte	ring Details	
General	Defaults	Sender Filtering	
Block messages that clair	m to be from the following	g senders.	
Senders:			-
abc@yanoo.com		4	
		4	
AddEd	t <u>R</u> emove]	
A <u>d</u> d <u>E</u> di	it <u>R</u> emove]	
Add Ed Archive filtered messa	it <u>B</u> emove iges glank sender]	
Add Ed Archive filtered messa Filter messages with b	it <u>B</u> emove Iges Iank sender Idress matches filter]	
Add Edi Archive filtered messa Filter messages with b Drop connection if ad	it <u>R</u> emove iges Jank sender Idress matches filter hout notifying sender of f	iltering	
Add Edi Archive filtered messa Filter messages with <u>b</u> Drop connection if ad Accept messages with	it <u>R</u> emove Iges Jank sender Idress matches filter hgut notifying sender of f	l	

Bước 5: chọn Ok để hoàn tất việc thiết lập

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

<u>Chú ý:</u>

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

Default SMTP Virtual Server Properties	? ×
General Access Messages Delivery	
Default SMTP Virtual Server	
I <u>P</u> address:	
172.29.14.151 Adve	inced
Limit number of connections to:	<u> </u>
Connection time- <u>o</u> ut (minutes):	
Active log format:	
W3C Extended Log File Format Propert	ies
OK Cancel Apply	Help

Bước 3: chọn nút Advanced

N	×
5	
es for this virtual server.	
TCP Port	Filter Enabled
25	No
fit Bemove	1
]
	es for this virtual server. TCP Port 25 it Remove OK

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

Identification		×
I <u>P</u> address:	172.29.14.151	•
<u>T</u> CP port:	25	
Apply Sender Filter		
Apply Recipien Filt	er	
Apply Connection F	ilter	
	OK Cancel Help	

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.

Default SMTP Virtual Server Properties	? ×
General Access Messages Delivery	
a ☐ Default SMTP Virtual Server	
I <u>P</u> address:	
172.29.14.151 Advanced]
Limit number of connections to:	
Connection time-out (minutes):	
Active log format:	
W3C Extended Log File Format	
OK Cancel Apply He	P

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

Default SMTP Virtual Server Properties		? ×
General Access Messages Delivery		
Enable anonymous access and edit the authentication methods for this resource.	Authentication	
Secure communication		
View or set the secure communications method used when this virtual server is	<u>C</u> ertificate	
accessed.	Communication	
Connection control		
Grant or deny access to this resouce using IP addresses or Internet domain names.	Co <u>n</u> nection	
Relay restrictions		
Grant or deny permissions to relay e-mail through this SMTP virtual server.	R <u>e</u> lay	
OK Cancel	Apply H	lelp

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).

Connection	× × ×	<	
Select which computers may access this virtual server:			
○ <u>O</u> nly the list bel	low		
 All except the lip 	ist below		
<u>C</u> omputers:			
Access	IP Address (Mask) / Domain Name		
Add	<u>i</u> emove		
	OK Cancel <u>H</u> elp		

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

Computer	×
Add one of the following to the list.	
O Single computer	
IP <u>a</u> ddress:	D <u>N</u> S Lookup
Group of computers	
S <u>u</u> bnet address:	Subnet <u>m</u> ask:
192.168.10.0	255 . 255 . 255 . 0
C <u>D</u> omain	
Nam <u>e</u> :	
ОК	Cancel <u>H</u> elp

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

Connection		×
Select which computers	may access this virtual server:	
 <u>O</u> hij the list below All except the list 	, pelow	
<u>C</u> omputers:		
Access	IP Address (Mask) / Domain Name	
Denied	192.168.10.0 (255.255.255.0)	
Add <u>R</u> er	nove	
	OK Cancel <u>H</u> elp	

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





Default SMTP Virtual Server Properties	? ×
General Access Messages Delivery	,
<u>First retry interval (minutes):</u>	10
Second retry interval (minutes):	10
T <u>h</u> ird retry interval (minutes):	10
S <u>u</u> bsequent retry interval (minutes):	15
Delay notification:	12 Hours 💌
Expiration timeout:	2 Days 💌
Local	
Delay <u>n</u> otification:	12 Hours 💌
Expiration timeout:	2 Days 💌
Outbound Security Outbound <u>c</u> onnec	tions Ad <u>v</u> anced
OK Cancel	Apply Help

Bước 3: chọn nút Advanced...

Advanced Delivery
Maximum hop count: 30
Masquerade <u>d</u> omain:
J
Eully-qualified domain name:
vhost.csc.com Check DNS
Smart host:
mail.hcm.vnn.vn
Eerform reverse DNS lookup on incoming messages
Configure external DNS Servers: Configure
OK Cancel <u>H</u> elp

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 2: chọn Tab Access, sau đó chọn nút Relay

Relay Restrictions	×		
Select which computer may relay through this virtual server:			
Only the list below			
C All except the list below			
Computers:			
Access IP Address (Mask) / Domain Name			
Add Bemove			
Allow all computers which successfully authenticate to relay, reg of the list above.	ardless		
Grant or deny relay permissions to specific users or Users			
OK Cancel <u>H</u> e	elp		

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

Computer	×
Add one of the following to the list.	
Single computer	
IP <u>a</u> ddress:	
	D <u>N</u> S Lookup
I Group of computers	
S <u>u</u> bnet address:	Subnet <u>m</u> ask:
172.29.0.0	255.255.0.0
O <u>D</u> omain	
Nam <u>e</u> :	
ОК	Cancel <u>H</u> elp

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

Relay Restrictions			
Select which computer may relay through this virtual server:			
C <u>O</u> nly the list below			
All except the list below			
Computers:			
Access IP Address (Mask) / Domain Name			
Denied 172.29.0.0 (255.255.0.0)			
Add <u>R</u> emove			
Allow all computers which successfully authenticate to relay, regardless of the list above.			
Grant or deny relay permissions to specific users or Users			
OK Cancel <u>H</u> elp			

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

3. <u>Bài 3:</u>

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).

🔏 MDaemon Server Domain Setup 🛛 🔀			
	What Is Your Domain Name?		
	Please enter your domain name here. Your domain name is the part to the right of the @ symbol in your email address.		
	Domain name csc02.edu.vn		
	Click here to register a domain using the DNS4Me dynamic DNS service DNS4Me is a dynamic DNS service which can provide you with a domain that will work even without a fixed IP address.		
	Next > Cancel		



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

Primary Domain
Dequeue Archival Pruning Pre-processing Unknown Mail Domain Delivery Ports DNS Timers Sessions
Primary domain properties Primary domain name csc02.edu.vr This is the primary domain name for your mail server. HELO domain name csc02.edu.vn When sending mail this value is used during the SMTP protocol. Machine name csc02.edu.vn This is a value used to uniquely identify this computer. The HELO and Machine name values will always default to the primary domain name.
Primary <u>d</u> omain IP 192.168.11.212
If you do not know your computer's IP address then you can leave this field blank or use 127.0.0.1.
OK Cancel Apply

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.

Account	Editor - nttd	ung		? 🔀
Web Accour Persona	Auto Re nt Mailbox al information —	sp IMAP Mail R Forwarding	iules MultiPOF Admin Quotas	P Options Restrictions
£	Eull name nttdung This account was created on: Thu Dec 01 10:38:11 2005 This account was last accessed on: <unknown></unknown>			
POP/IM	IAP account info	mation		
	<u>M</u> ailbox	nttdung	@ csc02.edu.vn	•
N	<u>P</u> assword	******		
	The account is	NOT currently using D	ynamic NT Authentic	ation.
	🔲 <u>D</u> isable all a	access to this account		
	Disable POI	P and IMAP access for	this account	
	L Enable MU	aemon GroupWare sup	port for this account	
Notes/	comments on this	account		
Ő				
Aliases				
Click here to edit any aliases configured for this account				
			OK	Cancel

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).

Content Filter
Content Filter Admins/Attachments File Compression Notifications
Content filtering rules
Enable rules processing engine
When active, the content filtering system will test all new messages using the
Fulles specified below and perform the requested action in a match is made.
✓ Message/Partial vulnerability [Move to bad message gueue]
▼IFRAME vulnerability [Move to bad message queue]
New rule Edit rule Copy rule Delete rule Move up
Click the checkbox to the left of each rule to enable/disable it. Move down
Rule Description: Message/Partial vulnerability (Enabled)
Apply this rule to messages in the LOCAL & REMOTE queue
If the message has an attachment with a CONTENT-TYPE of 'message/parti
then send note <u>"to <postmaster@\$primarydomain\$>","from <mdaemc< u=""></mdaemc<></postmaster@\$primarydomain\$></u>
and move message to bad message directory
OK Cancel

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



Create Rule	×
Give this rule a name	_
Ngan abc@yahoo.com send vao mail server	
Define new content filter rule Select Conditions For This Rule If the FROM HEADER contains If the TO HEADER contains If the SUBJECT HEADER contains If the REPLY-TO HEADER contains If the REPLY-TO HEADER contains	ļ
Select one or more conditions that will trigger this rule into action. Select Actions For This Rule	
Delete the message Stip all attachments from the message Move the message to bad message directory Skip the next 'n' rules Stop processing rules	ļ
Select one or more actions that this rule will take. NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed. Rule Description	
Apply this rule to messages in the <u>LOCAL & REMOTE</u> queue If the FROM HEADER <u>contains specific strings</u> then delete this message	
OK Cancel	

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.

Specify Search Text	
Specify strings that this content filter rule should look for Check for this string	
abc@yahoo.com	Add
Currently specifed strings (right click on the strings to remove)	1
If the FROM HEADER <u>contains</u>	
OK	Cancel

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



Create Rule
Give this rule a name
Ngan abc@yahoo.com send vao mail server
Define new content filter rule Select Conditions For This Rule If the FROM HEADER contains If the SUBJECT HEADER contains If the CUBJECT HEADER contains If the REPLY-TO HEADER contains Select one or more conditions that will trigger this rule into action.
Select Actions For This Rule
Select one or more actions that this rule will take. NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed. Rule Description
Apply this rule to messages in the <u>LOCAL & REMOTE</u> queue If the FROM HEADER <u>contains 'abc@yahoo.com'</u> then delete this message
OK Cancel

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)

🔗 Alt-N MDaemon PRO for Windows - Document - [Message Router - csc02.ed	du.vn 192.16	8.11.212]
Eile Edit Setup Security Accounts Lists Gateways Catalogs Queues Windows	Help	
📗 💻 🛝 🗛 😜 Anti <u>V</u> irus	Ctrl+A	0 0
Content filter	Ctrl+F5	
V 🔊 💙 🖆 🕱 Spam blocker	Alt+P	
🖻 🕋 RAW messa 🕄 Spam filter	Ctrl+P	
E Spam accep SSL / TLS / Certificates ⊡ ∰ Spam refus	Ctrl+L	
🖻 😰 Queued mail 🛛 🚦 Relay / Trusts / Tarpit / Reverse lookups / SPF / LAN IPs	Alt+F1	
Inbound qu 🚯 Address suppression / IP screening / Host screening	F4	
Remote que 🛞 IP shielding / AUTH / POP Before SMTP	Ctrl+F8	
Bad gueue:	Ctrl+T	

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.

Security		? 🗙			
Address S	uppression IP Screening Host Screening	1			
Current If	^o screen entries	New IP screen entry			
	🖃 🖓 IP Addresses	Local IP All IPs			
-		Select the IP that this new screen will belong to.			
	······································	Remote IP 192.168.10.* Add			
		Wildcards of the form 192.168.0.* or 192.168.*.1 are acceptable.			
		◯ <u>I</u> his remote IP can connect			
		This remote IP can not connect <u>R</u> emove			
		Default For Undefined IPs			
		C Undefined IPs can connect to this local IP			
		C Undefined IPs can not connect to this local IP			
IP Screening works by comparing the IP of the incoming connection to the IPs specified in this dialog. If a match is made the incoming connection is either allowed or disallowed based on how you have things configured here.					

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

Security		? 🔀		
Address S	uppression IP Screening Host Screening	ı],		
Current If	New IP screen entry Local IP All IPs Select the IP that this new screen will belong to. Remote IP Add Wildcards of the form 192.168.0.* or 192.168.*.1 are acceptable. C I his remote IP can connect Image: This remote IP can not connect Default For Undefined IPs C Undefined IPs			
Undefined IPs can not connect to this local IP IP Screening works by comparing the IP of the incoming connection to the IPs specified in this dialog. If a match is made the incoming connection is either allowed or disallowed based on how you have things configured here. OK Cancel Apply				

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

Học phần III - Môn Học: Dịch Vụ Mạng Windows 2003

Bước 1: bạn chọn Menu Gatewa	ay, chọn "New gateway…" (phír	n tăt là Alt+B)	
🤗 Alt-N MDaemon PRO for Windows - Doc	ument - [Message Router - csc02.e	du.vn 192.168.11.212]	
🏀 Eile Edit Setup Security Accounts Lists	$\underline{G}ateways \underline{C}atalogs \underline{Q}ueues \underline{W}indows$	Help	
E E \land 🚱 🧕 🕼 🛱 🔤 😋	Automatic gateway creation	Ctrl+G)
문 🔊 🔇 智 음 名 🛱 😵 🐒 🔞	🔂 New gateway	Alt+B	
	🔑 Edit gateway	Alt+K	_
E ⊕ AW messages: 3 ▲ Thu 2005- Thu 2005-	🗙 Delete gateway	Alt+V	

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.

Gateway	Editor - mail.hcm.vnn.vn	?	X
Gateway	LDAP ETRN ATRN POP/IMAP Quotas Options		
Domain	name		-
	mail.hcm.vnn.vn		
nut s	Messages arriving destined for all users of this domain will be place common mailbox directory. Wildcards ? and * are ok.	ed into a	
Mail dire	ctory		-
	Place message files for all users of this domain here		.
	C:\MDaemon\Gateways\mail.hcm.vnn.vn\	<u>B</u> rowse	
	Automatically extract embedded attachments		
	Extracted attachments will be stored in the FILES directory stemmi the message directory.	ing from	
	$\hfill\square$ Deliver messages at each scheduled remote mail processing is	nterval	
	Click here and MDaemon will try to deliver these messages each t outbound mail is processed. If this switch is disabled you must del directory from the Queues Queues dialog first.	time lete the	
Apply th	is MBF file to incoming messages		-
	BEC822 Messages which arrive for this		
	to this MBF script.	rding	
	OK Cancel	Apply	

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







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. <u>Bài 1: cài đặt ISA Firewall trên máy tính chủ có ít nhất hai card mạng để tổ</u> 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).

system Policy Allowed Sites Properties				
General				
Name: System Policy Allowed Sites				
i) If the DNS is not configured correctly, rules using domain name				
Domain names included in this set:				
<pre>*.microsoft.com *.windows.com *.windowsupdate.com</pre>				
Ne <u>w</u> <u>R</u> ename <u>D</u> elete				
Description (optional):				
OK Cancel Apply				

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

System Policy Allowed	Sites Properties	? X
General		
Name:	System Policy Allowed Sites	
If the DNS is no sets may not be Do <u>m</u> ain names include	t configured correctly, rules using domain name applied as expected. d in this set:	,
<pre>*.microsoft.com *.windows.com *.windowsupdat *.*</pre>	e.com	
New	Rename Delete	
De <u>s</u> cription (optional):	Predefined domain name set used to allow acc	ess >
	OK Cancel App	ly

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.

Microsof Interr Accel Standard	te net Security & leration Server 2 lédition	004				Firewall Policy
	Apply Disce	ard T	o save changes an	id update the config	guration, c	lick Apply.
Firewall			[[=		Toolbox Tasks Help
0 ×	Allow remote SQ	Action Allow	Microsoft S	From / Listener	<u>10</u>	Firewall Policy
🖃 💽 17	Allow HTTP/HTTP	🖉 Allow	HTTP HTTPS	👍 Local Host	Đ	Create New Access Rule
🗖 💽 18	Allow HTTP/HTTP	🥝 Allow	Щ НТТР Щ НТТРS	📥 Local Host	*	Publish a Web Server
□ [19	Allow access fro	🧭 Allow	Microsoft Microsoft NetBios Da NetBios Na NetBios Se	_म Internal		Server Publish a Mail Server Create New Server Publishing Rule
🖃 💦 20	Allow remote per	🥑 Allow	NetBios Da NetBios Na NetBios Se	🚑 Remote Man		System Policy Tasks

<u>Yêu cầu 3</u>: 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.

Microsoft Internet Security and Ac	celeration Server 2004	
<u>Eile Action View H</u> elp		
← → 🗈 🖬 😫 🖉 × י	€ €	
Microsoft Internet Security and Acceler DN51 Monitoring Firewall Policy Virtual Private Networks (VPN)	Microsoft Internet Security & Acceleration Server 2004 Standard Edition	Firewall Policy
E → 🔆 Configuration		Toolbox V Tasks V Help
	O A Name Action Protocols From / Liste	Protocols 🛞
Cache	Last Default rule 🚫 Deny 🐰 All Traffic 😤 All Netw	<u>U</u> sers 🛞
General		Content Types 🛞
_		Schedules 🛞
		Networ <u>k</u> Objects 🛛 🛞
		<u>N</u> ew ▼ <u>E</u> dit <u>D</u> elete
		 Networks Network Sets Computers Address Ranges Subnets Computer Sets URL Sets Domain Name Sets Microsoft Error Reporting sil System Policy Allowed Sites Web Listeners
Done		

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

New Access Rule Wizard		X
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Access Rule Wizard This wizard helps you create a new access rule. Access rules define the action that is taken, and the protocols that may be used, when specified clients from one network attempt to access specific destinations or content on another network. Access rule name: Chia se ket noi Internet To continue, click Next.	
	< <u>₿</u> ack. <u>N</u> ext > Cancel	

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

New Access Rule Wizard	×
Rule Action Select how client requests for content from the specified destination are dea if the conditions specified in the rule are met.	alt with
Action to take when rule conditions are met:	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

ew Access Rule Wizard			×
Protocols Select the protocols this rule applies to.			
<u>I</u> his rule applies to:			
All outbound traffic			
Protocols:			
			<u>A</u> dd
			<u>E</u> dit
			Remo <u>v</u> e
			Po <u>r</u> ts
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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)

New Access Rule Wizard	×
Access Rule Destinations This rule will apply to traffic sent from the rule sources to the destinations in this page.	specified
This rule applies to traffic sent to these destinations:	
	<u>A</u> dd
	<u>E</u> dit
	Remove
< <u>B</u> ack <u>N</u> ext>	Cancel

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



Bước 10: chọn Next để tiếp tục

New Access Rule Wizard	×
Access Rule Destinations This rule will apply to traffic sent from the rule sources to the destination in this page.	s specified
This rule applies to traffic sent to these destinations:	· ······
Sector Se	<u>Add</u>
	<u> </u>
	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext>	Cancel

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.

New Access Rule Wizard		X
Microsoft Internet Security & Acceleration Server 2004	Completing the New Access Rule Wizard You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:	
	Name: Chia se ket noi Internet Action: Allow Traffic: All outbound traffic Source: Internal Destination: External Accepted user sets: To close the wizard, click Finish.	
	< <u>B</u> ack Finish Cance	

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.

Firewall Policy Rules	5		
🚺 1 🛛 Chia se kel	t noi In 🧭 Allow	All Outbou	👍 Internal 🛛 🎯
💓 Last Default rul	e 🚫 Deny	鷆 All Traffic	🚖 All Networks 🚖

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



OK

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 dialup 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)

Internet Options
General Security Privacy Content Connections Programs Advanced
Constant of the set of
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration. Automatically detect settings
Use automatic configuration <u>s</u> cript Add <u>r</u> ess
Proxy server Use a proxy server for your LAN (These settings will not apply to dial a or VPN connections).
Address: 172.29.45.167 Port: 8080 Advanced
Bypass proxy server for local addresses
OK Cancel
OK Cancel Apply

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

New Network Wizard		×
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Network Wizard This wizard helps you create a new network. Networks specify one or more ranges of IP addresses as a network object that can be used in rules.	
	N <u>e</u> twork name: Subnet 192.168.02.0 To continue, click Next.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

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



lew Network Wizard	×
Network Type Specify the type of network you are defining.	
Internal Network	
Internal networks contain client computers that IS	SA Server will protect.
© Perimeter Network	
A Perimeter network usually contains servers that be less trusted than internal networks.	t are published to the Internet. It will usually
○ <u>V</u> PN Site-To-Site Network	
A VPN site-to-site network represents a network i link.	in a remote site, connected through a VPN
C External Network	
An external network represents an untrusted netw default external network.	vork, such as the Internet. ISA Server has a
	< <u>B</u> ack <u>N</u> ext> Cancel

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

New	Network Wizard		×
	Network Addresses Define the IP addresses for th address ranges associated w	nis network. You can add IP address ra ith a network adapter, and private IP ra	anges, IP anges.
1	Address ranges:		
[Start Address	End Address	<u>A</u> dd
			<u>E</u> dit
			<u>R</u> emove
			A <u>d</u> d Adapter
			Add <u>P</u> rivate
		< <u>B</u> ack <u>N</u> e	xt > Cancel

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

IP Address Range Properties	<u>?</u> ×
Specify the range of IP address	es:
Starting address:	Ending address:
192 . 168 . 2 . 0	192 . 168 . 2 . 255
ОК	Cancel

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

w Network Wizard		
Network Addresses Define the IP address address ranges asso	ses for this network. You can add IP add ciated with a network adapter, and privat	Iress ranges, IP te IP ranges.
Address ranges:		
Start Address	End Address	<u>A</u> dd
192.168.2.0	192.168.2.255	
		<u> </u>
		<u>R</u> emove
		Add Adapter
		Add <u>P</u> rivate

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

New Network Wizard		×
Microsoft Internet Security & Acceleration Server 2004	Completing the New Network Wizard You have successfully completed the New Network Wizard. The new network will have the following configuration:	
	Name: Subnet 192.168.02.0 Network Type: Internal Network Addresses: 192.168.2.0 - 192.168.2.255	
	For traffic to pass through this network, further configuration steps are required. Help about <u>further configuration steps</u> To close this wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

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

SE RECHULT	ncernec Pro	percies		
Users		Schedule	Conte	ent Types
General	Action	Protocols	From	To
This rule appl	ies to traffic fro	om these sources:		
📥 Internal				A <u>d</u> d
				<u>E</u> dit
				<u>R</u> emove
, Exceptions:				
				Add <u>.</u>
				E djt
				Remo⊻e

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

A	dd Network Entities	X
	Network entities:	
	<u>N</u> ew ▼ <u>E</u> dit <u>D</u> elete	
	 Networks External Internal Local Host Quarantined VPN Clients Subnet 192,168.02.0 VPN Clients VPN Clients Network Sets All Networks (and Local Host) All Protected Networks Computers Address Ranges Subnets Computer Sets 	
	Add Close	

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:

hia se ket noi Inte	ernet Prope	rties		<u>? ×</u>
Users	So	hedule	Con	tent Types
General	Action	Protocols	From	To
This rule applies	to traffic from	these sources	:	
📥 Internal				A <u>d</u> d
				<u>E</u> dit
				<u>R</u> emove
Exceptions:	100.00.0			ا بىر
	. 168.02.0			Add <u>.</u>
				Edįt
				Remo <u>v</u> e
		OK	Cancel	Apply

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





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

Yêu cầu 1: 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)

New Subnet Rule Element	<u>? ×</u>
Name: Duong mang 192.168.2.0 Specify the network address and the mask to define the range	
Network add <u>r</u> ess: 192 . 168 . 2 . 0 / 24 - Network <u>m</u> ask: 255 . 255 . 255 . 0	
Description (optional):	
OK Cancel	

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

ew Access Rule Wizard	×
Rule Action Select how client requests for content from the specified destination are dealt with if the conditions specified in the rule are met.	
Action to take when rule conditions are met:	
O Allow	
• Denv	
	1
< <u>B</u> ack <u>N</u> ext>	Cancel

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



Select the protocols this rule applies to.	
This rule applies to:	
All outbound traffic	_
Protocols:	
	<u>A</u> dd
	<u>E</u> dit
	Remo <u>v</u> e
	Ports

Bước 5: chọn Add để thêm đường mạng vào

New Access Rule Wizard		×
Access Rule Sources This rule will apply to traffic originating from	the sources specified in this pag	е.
This rule applies to traffic from these sources:		bb
		<u>E</u> dit
		<u>R</u> emove
	< <u>B</u> ack <u>N</u> ext >	Cancel

Bước 6: sau khi thêm vào



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

New Access Rule Wizard	×
Access Rule Destinations This rule will apply to traffic sent from the rule sources to the destinations in this page.	specified
This rule applies to traffic sent to these destinations:	
External	<u>A</u> dd
	<u>E</u> dit
	Bamaua
< <u>B</u> ack <u>N</u> ext >	Cancel

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



You can apply the rule to request specific user sets.	ts from all users. Or, you can limit acce	ess to
This rule applies to requests from the I	iollowing user sets:	
📇 All Users		<u>A</u> dd
		<u>E</u> dit
		Removie
		Demove

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

New Access Rule Wizard	X
Microsoft Internet Security & Acceleration Server 2004	Completing the New Access Rule Wizard You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:
	Name: Chang duong mang 192.168.2.0 Action: Deny Traffic: All outbound traffic Source: Duong mang 192.168.2.0 Destination: External Accepted user sets: To close the wizard, click Finish.
	< <u>B</u> ack Finish Cancel



c. 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.

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.



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.

Khong duoc phep Prope	rties	<u>?</u> ×
General		
Mame:	Khong duoc phep	
sets may not be	applied as expected.	
Do <u>m</u> ain names include	d in this set:	
 *.yahoo.com *.vnn.vn *.vnexpress.net 	I	
New	<u>R</u> ename <u>D</u> elete	
De <u>s</u> cription (optional):		
	OK Cancel App	ly

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







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







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

New Access Rule Wizard			×
Rule Action Select how client requests for content from the sp if the conditions specified in the rule are met.	pecified de:	stination are dealt	with
Action to take when rule conditions are met:			
C Allow			
• Denv			
	(<u>B</u> ack	<u>N</u> ext >	Cancel

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

New Access Rule Wizard	×
Protocols Select the protocols this rule applies to.	
Ihis rule applies to:	
All outbound traffic	
<u>P</u> rotocols:	
	<u>A</u> dd <u>E</u> dit Remo <u>v</u> e
	Ports

Bước 5: chọn địa chỉ nguồn của gói tin

New Access Rule Wizard			X
Access Rule Sources This rule will apply to traffic originating from t	he sources specil	fied in this pa	ge.
This rule applies to traffic from these sources:			
[Internal			<u>A</u> dd
			<u>E</u> dit
			<u>R</u> emove
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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)

w Access Rule Wizard	×
Access Rule Destinations This rule will apply to traffic sent from the rule sources to the destinations in this page.	specified
This rule applies to traffic sent to these destinations:	
E Khong duoc phep	<u>A</u> dd
	<u>E</u> dit
	Bemove
	Transis
,	
< <u>B</u> ack <u>N</u> ext>	Cancel

Bước 7: chọn các User sẽ được áp dụng



User Sets You can apply the rule to requests from a specific user sets.	ll users. Or, you car	i limit access to	
This and the first the second to first the following			
All Users	user sets:		<u>A</u> dd
			<u>E</u> dit
			Remove

Bước 8: kiểm tra lại thông tin lần nữa

New Access Rule Wizard		×
Microsoft Internet Security & Acceleration Server 2004	Completing the New Access Rule Wizard You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:	
	Name: Trong gio hanh chanh Action: Deny Traffic: All outbound traffic Source: Internal Destination: External Accepted user sets:	
	To close the wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

- Yêu cầu 3: Chọn thời gian áp dụng cho luật
 - Bước 1: kích chuột phải vào Rule vừa mới tạo, chọn Properties



Firewall Policy Ru	lles	
💽 1 🛛 Trong	Properties	📲 Outbou 🚣 Internal 🛛 🔋
💽 2 🛛 Chia se	Delete	،ll Outbou 👍 Internal 🛛 🧃
💽 Last Defaul	Сору	ll Traffic 🛛 🎂 All Networks 🔹
•	Export Selected Import to Selected	
📑 Microsoft Inl	<u>M</u> ove Down Disa <u>b</u> le	Prompt

Bước 2: chọn Tab Schedule

Tro	ng gio hanh	chanh Prop	erties		? ×
	General	Action	Protocols	From	To
	Users		schedule	Lonter	it i ypes j
<u>S</u> chedule:			Always	•	<u>N</u> ew
	<u>D</u> escription:				
	1	2 • 2 • 4 •	6 • 8 • 10 •	<mark>.</mark> 12•2•4•6	• 8 • 10 • 12
	All				
	Sunday				
	Monday				
	Tuesday				
	Wednesday				
	Thursday				
	Friday				
	Saturday				
	From: Sunday To: Saturday Time: 12 AM -	, 12 AM	_		
	Ac	Active Inactive			
			OK	Cancel	Apply

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.











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)

New Access Rule Wizard	×
Rule Action Select how client requests for content from the specified destination are dealt with if the conditions specified in the rule are met.	
Action to take when rule conditions are met:	
< <u>B</u> ack <u>N</u> ext >	Cancel

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.



New Access Rule Wizard		×
Protocols Select the protocols this rule applies to.		
∐his rule applies to:		
Selected protocols		
Protocols:		
		<u>A</u> dd
		<u>E</u> dit
		Remo <u>v</u> e
		Ports
1		1 0[13
	< <u>B</u> ack	Next > Cancel

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

A	dd Protocols	X
	Protocols:	
	<u>N</u> ew ▼ <u>E</u> dit <u>D</u> elete	
Common Protocols DNS HTTP HTTPS HTTPS HTTPS Server MSN Messenger POP3 POP3 POP3 Server POP3 Server SMTP SMTP Server SMTP Server SMTP Server Tabat		
	🗄 🛄 Infrastructure	-
	Add Close	

Bước 6: chọn Next để tiếp tục cấu hình



Protocols Select the protocols this rule applies to.	 	
<u>I</u> his rule applies to:		
Selected protocols		•
Protocols:		
QU Ping	 	<u>A</u> dd
		<u>E</u> dit
		Remo <u>v</u> e
		Ports
		-

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

New Access Rule Wizard	×
Access Rule Sources This rule will apply to traffic originating from the sources specified in this pa	age.
This rule applies to traffic from these sources:	
	<u>A</u> dd
	<u>E</u> dit
	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext>	Cancel



Access Rule Destinations This rule will apply to traffic in this page.	: sent from the rule sources to th	e destinations specified	
his rule applies to traffic sent t	o these destinations:	Ad	ld
		Ed	lit
		Ber	nove
		1101	

Bước 9: chọn các User cần áp đặt Rule

New Access Rule Wizard	×
User Sets You can apply the rule to requests from all users. Or, you can limit access specific user sets.	s to
This rule applies to requests from the following user sets:	
All Users	<u>A</u> dd
	<u>E</u> dit
	Bemove
	Tionio ve
< <u>B</u> ack <u>N</u> ext ≻	Cancel

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

ew Access Rule Wizard	×
Rule Action Select how client requests for content from the specified destination are dealt with if the conditions specified in the rule are met.	
Action to take when rule conditions are met:	
Denu	
< Back Next > 0	ancel
Contraction Contraction Contraction	

Bước 7: chọn tất cả các đường mạng

New Access Rule Wizard	×
Access Rule Sources This rule will apply to traffic originating from the sources specified in this pa	age.
This rule applies to traffic from these sources:	
All Networks (and Local Host)	<u>A</u> dd
	<u>E</u> dit
	<u>R</u> emove
< <u>B</u> ack <u>N</u> ext>	Cancel

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

Firewall P	Firewall Policy Rules						
🥐 1	Chan PING	🚫 Deny	🐫 Ping	🔹 All Networks	-4-		
🥐 2	Cho phep PING n	🕜 Allow	🖳 Ping	👍 Internal	4		
🖃 📝 З	Trong gio hanh c	🚫 Deny	🜉 All Outbou	👍 Internal	Ē.		

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**.

Move Selected Rules Up
 Move Selected Rules Down
 Disable Selected Rules

Kết quả sau khi thực hiện sẽ như sau:

Firewall Policy Rules I Cho phep PING n... ② Allow Image: Ping Image: Internal Image: Ping Image: Ping Chan PING Openy Image: Ping Image: All Networks ... Image: Ping Image: Ping

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.

Toolbox Tasks Help						
Protocols 🛞						
<u>U</u> sers	8					
<u>C</u> ontent Types	8					
<u>S</u> chedules	0					
Networ <u>k</u> Objects	8					
<u>N</u> ew ▼ <u>E</u> dit <u>D</u> elete						
🛨 🧰 Networks						
표 🚞 Network Sets						
🖃 🗁 Computers						
🔜 ip chu						
🚞 Address Ranges						
🖃 🦾 Subnets						
💐 Duong mang 192,168,	2.0					
🖃 🗁 Computer Sets						
🛃 Anywhere						
IPSec Remote Gatewa	iys					
💐 Remote Management	Comp					
🕀 🛄 URL Sets						
🛨 🚞 Domain Name Sets						
📄 Web Listeners						

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

ew Computer Set Ru	le Element	? ×
Name:	Truy cap NAT	
Computers, address r set:	anges and subnets included in this computer	
Name	IP Addresses	
Ad <u>d</u>	Edit Remo <u>v</u> e	
Desc <u>r</u> iption (optional):		
	OK Cancel	

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.

]	Ad <u>d</u>	Edit
	Computer	
Description	<u>A</u> ddress Range	
(optional):	<u>S</u> ubnet	

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

New Cor	nputer Rule Element	? ×
	Name:	
	May 1	
	Computer IP Address:	
	172 . 29 . 45 . 166 Browse	
	Description (optional):	
	1	
	OK Cancel	

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

Name: 14.144 -> 14.158	
Name: 14.144 -> 14.158	
Sperify the range of IP addresses	
Specify the range of IP addresses:	
Spearly the range of in data esses.	
Start Address: End Address:	
172 . 29 . 14 . 144 172 . 29 . 14 . 158	
Description (optional):	
(optional).	
OK Cancel	

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.

New Computer Set Rule	e Element	<u>?×</u>
Name:	Truy cap NAT	
Computers, address rai <u>s</u> et: 	nges and subnets included in this computer	
Name	IP Addresses	
📕 May 1	172.29.45.166	
Ad <u>d</u>	Edit Remo <u>v</u> e	_
Desc <u>r</u> iption (optional):		
	OK Cancel	

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).



Yêu cầu 3: 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.

New Network Rule Wizard		×
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Network Rule Wizard This wizard helps you create a new Network rule. Network rules define the relationship between network entities as either route or network address translation (NAT).	
	<u>N</u> etwork rule name: Cho phep NAT To continue, click Next.	
	< <u>B</u> ack <u>N</u> ext > Cance	

Bước 2: chọn Add để nhập địa chỉ nguồn

New Network Rule Wizard			x
Network Traffic Sources This rule will apply to traffic originating fro	om the sources spec	cified in this pa	ge.
This rule applies to traffic from these sources:			·····
			<u>Add</u> Edit
			<u>R</u> emove
	< <u>B</u> ack	<u>N</u> ext>	Cancel

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

New Network Rule Wizard	×
Network Traffic Sources This rule will apply to traffic originating from the sources specified in this pa	age.
This rule applies to traffic from these sources:	
Truy cap NAT	<u>A</u> dd
	<u>E</u> dit
	Bemove
	<u>Tiennove</u>
< <u>B</u> ack <u>N</u> ext >	Cancel

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

v Network Rule Wizard		
Network Traffic Destina This rule will apply to trai	tions ffic arriving at the destinations specified in this page	
This rule applies to traffic ser	it to these destinations:	
S External		<u>A</u> dd
		<u>E</u> dit
		Pomorro
		Tiennove
		1
	< <u>B</u> ack <u>N</u> ext>	Cancel

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

New Network Rule Wizard	×
Network Relationship Specify how traffic is sent between the source and destination network entities.	
Network Address Iranslation (NAT)	
ISA Server hides computers in the sources by replacing their network IP addresses i outgoing traffic with its own external IP address.	า
◯ <u>R</u> oute	
ISA Server routes traffic between the sources and destinations (no network address translation is used). Route relationships are bi-directional.	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

efault rule Properti	es		? :		
General Action To Bridging					
Process requests b	γ; ————————————————————————————————————				
C <u>R</u> etrieving them	n directly from t	the specified destination	ation		
Redirecting the	m to a specifie	d upstream server			
🗖 Allow deleg	ation of basic a	uthentication crede	ntials		
	Upstream ser	ver	S <u>e</u> ttings		
<u>B</u> ackup route:	None	•	Setti <u>n</u> gs		
C Redirecting the	m to a hosted s	site			
Si <u>t</u> e:			Bro <u>w</u> se		
<u>P</u> ort:	80	<u>S</u> SL Port:	443		
Automatic dial-up -					
Use automatic dial-up for the primary route					
Se automatic dial-up for the backup route					
Help about automatic dial-up connections					
)K Cance	el <u>A</u> pply		

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

Up	stream Server Setting		? ×
	- Specify upstream server	configuration	
	<u>S</u> erver:	192.168.11.1	<u>B</u> rowse
	<u>P</u> ort:	8080	
	SS <u>L</u> Port:	8443	
	Automatically poll ups	tream server for the configuration	
	Server <u>U</u> RL:	http://192.168.11.1:8080/array.dll	
	☐ <u>U</u> se this account: Aut <u>h</u> entication:		S <u>e</u> t Account
	[OK Cancel	

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

eneral Action To	Bridging	
Process requests c	γγ:	
C <u>R</u> etrieving ther	n directly from the specified d	destination
• Redirecting the	em to a specified upstream se	rver
I Allow deleg	ation of basic authentication	credentials
	Upstream server	S <u>e</u> ttings
Backup route:	None	 Settings
	,	
C Redirecting the	m to a hosted site	
Si <u>t</u> e:		Bro <u>w</u> se.
Port	SSL Port	

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

Apply Discard To save changes and update the configuration, click Apply.

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.

I will dial the connection myself	
Allow automatic dialing to this network:	
Help about creating networks	
Dial-up connection Use the following dial-up connection:	Select
teln about creating dial-up connections	
Help about <u>creating dial-up connections</u>	
Help about <u>creating dial-up connections</u>	
Help about <u>creating dial-up connections</u> Dial-up account Use this a <u>c</u> count:	

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)

ling Configuration	?
ial-up Preferences	
C I will dial the connection myself	
Allow automatic dialing to this network:	
External	•
Help about creating networks	
Configure this dial-up connection as the default gat	eway
Dial-up connection	
Use the following dial-up connection:	
<u>S</u> el	ect
Help about creating dial-up connections	
Dial-up account	
Use this account:	
Set Ar	ccount
	- Applu
OK Cancer	

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

Select I	Network Dial-up Connection	<u>? ×</u>
Net serv	work dial-up connections which are defined or er.	i the
	Network Dial-up Connection	
	Vnn1269	
	OK Cancel	

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

Dialing Configuration	? ×
Dial-up Preferences	
 I will dial the connection myself Allow automatic dialing to this network: 	
External	-
Help about creating networks	
Configure this dial-up connection as the default gateway	
Dial-up connection	
Use the following dial-up connection:	
Vnn1269 <u>S</u> elect	
Help about <u>creating dial-up connections</u>	
Dial-up account	
Use this account:	
Set Account	
OK Cancel	Apply

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

Set Account				<u>?</u> ×
Use the following account	:			
<u>U</u> ser:	vnn1269		Browse	
<u>P</u> assword:	•••••			
Confirm password:	•••••			
		ОК	Cancel	



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

ing Configuration		<u></u>
ial-up Preferences		
 I will dial the connection myself Allow automatic dialing to this network: 		
External		•
Help about creating networks		
Configure this dial-up connection as	the default <u>c</u>	lateway
Use the following dial-up connection:		
Use the following dial-up connection:		<u>.</u> elect
Use the following dial-up connection: Vnn1269 Help about <u>creating dial-up connections</u>		jelect
Use the following dial-up connection: Vnn1269 Help about <u>creating dial-up connections</u> Dial-up account Use this a <u>c</u> count: vnn1269		elect

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).

📰 Microsoft Internet Secur 🖮 🤯 DNS1	Microsoft Internet Security	& 001/2004			Cache
	Standard Edition	ei 2004			
Virtual Private N	Cache Rules Content	Download Jobs			(Taska) (Inka)
🖻 🔆 Configuration		To.	Object Size	SSI Respon	
Networks	I act Default rule	💠 All Networks	(a All Objects	Cache	
Add-ins				Cache	Cache Rules Tasks
🛄 General					Define Cache Drives (enable
					Particulus Particulus Particulus
					Figure 2 Contract Selected Rule

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:

Define Cache Driv	es			? ×
Cache Drives				
•• dns1				
Drive	Туре	Disk Space	Free Space	Cache Size
C:	NTFS	2000	229	100
1				
<u>M</u> aximum cache :	size (MB):		100	Set
		,		- De seb
				<u>R</u> eset
Total disk space	on NTFS drives (MB):	2000	
Current total cad	the size (MB):		100	
			Capital	Apply
		OK		

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

This rule applies to content requested from these network entities:		
	Add	rule applies to content requested from these network entities:
<u>B</u> err	<u>E</u> dit	
	<u>R</u> emove	

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

New Cache Rule Wizard
Content Retrieval Specify how objects stored in the cache are retrieved when requested.
Retrieve the requested object from the cache:
Image: Description of the object exists in the cache. If no valid version exists, route the request to the server.
If any version of the object exists in the cache. If none exists, route the request to the server.
○ If any version of the object exists in the cache. If none exists, drop the request (never route the request to the server).
< <u>B</u> ack <u>N</u> ext > Cancel

Bước 5: chọn các nội dung cần lưu Cache

ew Cache Rule Wizard	×
Cache Content Specify whether retrieved content is stored in the cache. By default, an object is stored in the cache only if its source and request headers indicate to do so.	
Select when content should be stored in the cache:	
O Never, no <u>c</u> ontent will ever be cached.	
If source and request headers indicate to cache	
In addition, also cache:	
Vynamic content	
Content for offline browsing (302, 307 responses)	
Content requiring user authentication for retrieval	
\	
< <u>B</u> ack <u>N</u> ext>	Cancel

Bước 6: chọn giới hạn kích thước Cache

New Cache Rule Wizard		×
Cache Advanced Configuration Specify advanced configuration.		
Do not cache objects larger than:	1	мв
Cache SSL responses		
	< Back Next :	Cancel

Bước 7: chỉ định thời gian lưu trữ Cache

New Cache Rule Wizard					×
HTTP Caching When HTTP caching is en accordance with the policy	abled, HTTP objec	ts are stored ir) the cache,	in	
 Enable HTTP caching Unless the source specifies expi 	ration, update objec	cts in the cach	ie according	to TTL:	
Set TTL of objects (% of the con	tent age):			20	_
Content age is the amount of tim	e since an object v	vas created or	modified.		
TTL time boundaries:					
N <u>o</u> less than:	15	Minutes	-		
No <u>m</u> ore than:	1	Days	•		
🔲 Also apply these TTL bound	aries to sources tha	it specify expir	ation		
Time-To-Live (TTL) is the amour	it of time content re	mains in the c	ache before	expiring.	
		< <u>B</u> ack	<u>N</u> ext >		Cancel

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

New Cache Rule Wizard Image: Comparison of the cache in the cache with the policy.
Ime-To-Live for FTP objects: 1 Days
Time-To-Live (TTL) is the amount of time content remains in the cache before expiring.
< Back Next > Cancel

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

New Cache Rule Wizard		X
New Cache Rule Wizard	Completing the New Cache Rule Wizard You have successfully completed the New Cache Rule Wizard. The new cache rule will have the following configuration: Name: Cau 3b Destination: All Networks (and Local Host) Cache Retrieval Configuration: Only if a valid version of the object exists in the Cache Content Configuration: If source and request headers indicate to cach Cached Objects Size Configuration:	X
	To close this wizard, click Finish.	

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





New Web Publishing Rule Wizard	×
Select Rule Action Specify how you want this rule to respond when the rule conditions are met.	
Action to take when rule conditions are met:	

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 thực mục muốn truy xuất vào Web Server nội bộ
- o 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"

New Web Publishing Rule	e Wizard			×
Define Website to P Specify the comput publish the entire w	'ublish er (Web server) on whit ebsite or limit access to	ch the website is lo a specified folder.	ocated. You car	
Computer name or IP ad	dress: 172.29.4	5.167		Br <u>o</u> wse
Fo <u>r</u> ward the origina	al host header instead o	f the actual one (s	pecified above)	
Enter the name of the I within a folder use 7*. B	file or folder you want to Example: folder/*.	publish. To includ	de all files and si	ubfolders
<u>P</u> ath:				
Based on your selectio	on, the following Web si	e will be published	±:	
Site:	http://172.29.45.167/			
Set the port to which re page.	equests should be redire	ected on the Bridg	ing tab of the ru	le properties
		,		
		< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Public Name Details Specify the public domain name (FQDN) or IP address users will type to reach the published site. Accept requests for: This domain name (type below): Only requests for this public name or IP Any domain name Any domain name This domain name (type below): Public name: Image: I	Public Name Details Specify the public domain name (FQDN) or IP address users will type to reach the published site. Accept requests for: This domain name (type below): Only requests for this public name or IP Any domain name Public name: Image: Comparison of the public name	w Web Publishing Rule Wizard		
Accept requests for: This domain name (type below): Only requests for this public name or IP Any domain name Any domain name This domain name Public name: Image: Comparison of the second	Accept requests for: This domain name (type below): Only requests for this public name or IP Any domain name This domain name This domain name This domain name Public name: Path (optional): Based on your selections, requests sent to this site (host header value) will be accepted: Site:	Public Name Details Specify the public domain name (F published site.	QDN) or IP address users will type to reach the	
Public name:	Public name:	Accept requests for: Only requests for this public name or IP example www.microsoft.com.	This domain name (type below): Any domain name This domain name (type below):	-
Based on your selections, requests sent to this site (host header value) will be accepted:	Based on your selections, requests sent to this site (host header value) will be accepted: Site:	P <u>u</u> blic name: <u>P</u> ath (optional):		
	Site:	Based on your selections, requests sen	t to this site (host header value) will be accepted:	



New Web Publishing Rule Wi	zard		×
Select Web Listener The Web listener specifi computer listens for inco	es the IP addresses and port of ming Web requests.	on which the ISA Server	
Web listener:			
	_	<u>E</u> dit	
Listener properties:		New	
Property	Value		
	< <u>B</u> ac	sk <u>N</u> ext>	Cancel

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

New Web Listener Definition	Wizard	×
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Web Listener Wizard	
	This wizard helps you create a new Web listener. Web listeners are used in Web publishing rules. A Web listener specifies the IP addresses and port on which the ISA Server computer listens for incoming Web requests. <u>W</u> eb listener name: Web Listener 80	
	< <u>B</u> ack. <u>N</u> ext > Cancel	



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

New Web Listener Definition Wizard		×
IP Addresses A Web listener can include all IP addres Server, or you can select specific IP add	uses associated with a network on the ISA dresses.	
Listen for requests from these networks:		
Name	Selected IPs	
🗹 📥 External	<all addresses="" ip=""></all>	
🗖 📥 Internal	<all addresses="" ip=""></all>	
🗖 📥 Local Host	<all addresses="" ip=""></all>	
🔲 📥 Quarantined VPN Clients	<all addresses="" ip=""></all>	
🗖 📥 VPN Clients	<all addresses="" ip=""></all>	
🗖 📥 All Maximulia (an all an all land)	AIL 0	ے بے
Help about <u>Web listener IP addresses</u>	Address	
	< <u>B</u> ack <u>N</u> ext > (Cancel

Bước 9: chọn Port lắng nghe.

New Web Listener Definition Wizard	×
Port Specification Specify the port that the ISA Server computer will use to listen on the selected IP addresses for incoming Web requests.	
HTTP F Enable HTTP HTTP port: 80	
SSL Enable <u>S</u> SL SSL port: 443 <u>C</u> ertificate: <u>Select</u>	
Help about <u>Web listener port specification</u>	
< <u>B</u> ack <u>N</u> ext≻	Cancel

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

w Web Publishing Rule Wi	zard			
Select Web Listener The Web listener specif computer listens for inco	ies the IP address ming Web reques	es and port on w	hich the ISA Server	
Web listener:				
Web Listener 80		•	<u>E</u> dit	
Listener properties:			New	
Property	Value	_	<u></u>	
Description Networks Port(HTTP) Port(HTTPS) Authentication methods Always authenticate	External 80 Disabled Integrated No	_		
		< <u>B</u> ack	<u>N</u> ext >	Cancel

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





New Web Publishing Rule Wiz	ard	×
Microsoft Internet Security & Acceleration Server 2004	Completing the New Web Publishing Rule Wizard You have successfully completed the New Web Publishing Rule Wizard. The new Web Publishing Rule will have the following configuration:	
	Name: Publish Web Server Action: Allow Site: 172.29.45.167 Public Name: All incoming names Listener: Web Listener 80 Accepted user sets: To close the wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

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

New Mail Server Publishing R	ule Wizard	×
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Mail Server Publishing Rule Wizard	
	This wizard helps you publish mail servers such as SMTP, or Web mail services such as Outlook Web Access.	
	This wizard publishes a single server. Run this wizard for each mail server that you are publishing.	
	Mail Server Publishing Rule name:	
	Publish Mail Server	
	To continue, click Next.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

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

New Mail Server Publishing Rule Wizard
Select Access Type Select the type of access this mail server will provide for clients.
Web client access: Outlook Web Access (OWA), Outlook Mobile Access, Exchange Server ActiveSync
◯ _lient access: RPC, IMAP, POP3, SMTP
C ≦erver-to-server communication: SMTP, NNTP
< <u>B</u> ack <u>N</u> ext > Cancel

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

New Mail Server Publishing Rule Wizard	×
Select Services Select the services that you are publishing on this mail server.	
Web client mail services:	
Exchange ActiveSync	
☑ Enable high bit characters used by non-English character sets	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

New Mail Server Publishing Rule Wizard	×
Specify the Web Mail Server Specify the mail server that is hosting the Web mail site.	
Enter the name or IP address of the mail server publishing the Web ma	il site.
Web mail server: webmail.csc.edu.vn	Br <u>o</u> wse
Set the port to which requests should be redirected on the Bridging tab o page.	of the rule properties
< <u>B</u> ack <u>N</u> ext	: > Cancel

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

New Mail Server Publishing Rule Wizard			×
Public Name Details Specify the public domain name (FQDN) or published site.	IP address user:	; will type to reach	n the
Accept requests for:	ny domain name		
Incoming Web requests will be forwarded to the domain name.	e published websi	te without checkir	ng for the
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Mail Server Publishing I	Rule Wizard	×
elect Web Listener The Web listener specifi computer listens for inco	es the IP addresses and port on which the ISA S oming Web requests.	erver
Web listener:		
Web Listen Port	<u>E</u> dit	
istener properties:	Ne <u>w</u>	
Networks Port(HTTP) Port(HTTP) Authentication methods.	External, Internal, Local H 8080 Disabled Integrated ener is not configured to use OWA forms-based ener does not listen on an HTTPS port.	
	< <u>B</u> ack <u>N</u> ext >	Cancel

Bước 9: chọn các user sẽ bị áp dụng

You can apply the rule to requ	uests from all users. Or, you can limit a	ccess to
specific user sets.		
ais rule applies to requests from l	the following user sets:	
All Users	no rolowing data acta.	<u>A</u> dd
		Edit
		Pemove
		- Zemove

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

New Server Publishing Rule ¥	/izard	×
Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Server Publishing Rule Wizard This wizard helps you create a new server publishing rule. Server publishing rules map incoming client requests to the appropriate internal server.	
	<u>S</u> erver publishing rule name: Public FTP To continue, click Next.	
	< <u>B</u> ack. <u>N</u> ext > Cancel	

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

New Server Publishing Rule Wizard	×
Select Server Specify the network IP address of the server you are publishing.	
<u>S</u> erver IP address: 172 . 29 . 45 . 166 <u>Br</u> owse	
< <u>B</u> ack <u>N</u> ext >	Cancel

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

New Server Publishing Rule Wizard	×
Select Protocol Select the protocol used by the published server.	
Selected protocol:	
FTP Server	Properties
DNS Server	
Exchange RPC Server	Po <u>r</u> ts
HTTPS Server	New
IKE Server	146 <u>97</u>
IMAP4 Server	
IMAPS Server	
IPSec ESP Server	
IPSec NAT-T Server	
L2TP Server	
Microsoft SUL Server	
NNTE Server	
PNM Server	
POP3 Server	
POP3S Server	
PPTP Server	
RDP (Terminal Services) Server	xt > Cancel
RPC Server (all interfaces)	
RTSP Server	
SMTP Server	
SMTPS Server	
Teinet Server	





Bước 6: bảng tổng kết về Publish FTP Server

New Server Publishing Rule V	Vizard	x
Microsoft Internet Security & Acceleration Server 2004	Completing the New Server Publishing Rule Wizard You have successfully completed the New Server Publishing Rule Wizard. The new Server Publishing Rule will have the following configuration: Name: Public FTP Published Server: 172.29.45.166 Published Service: FTP Server Listen on: External	
	× ×	
	To close the wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

f. Cài đặt Publish DNS Server

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