TRƯỜNG CAO ĐẲNG NGHỀ CÔNG NGHIỆP HÀ NỘI
Tác giả: Dương Ngọc Việt (chủ biên).
Trần Thị Ngân.

GIÁO TRÌNH
Quản trị mạng 2
(Lưu hành nội bộ)

Hà Nội năm 2012

Tuyên bố bản quyền

Giáo trình này sử dụng làm tài liệu giảng dạy nội bộ trong trường cao đẳng nghề Công nghiệp Hà Nội

Trường Cao đẳng nghề Công nghiệp Hà Nội không sử dụng và không cho phép bất kỳ cá nhân hay tổ chức nào sử dụng giáo trình này với mục đích kinh doanh.

Mọi trích dẫn, sử dụng giáo trình này với mục đích khác hay ở nơi khác đều phải được sự đồng ý bằng văn bản của trường Cao đẳng nghề Công nghiệp Hà Nội

LỜI GIỚI THIỆU

Giáo trình "***Quản trị mạng 2***" được biên soạn dựa vào Chương trình khung Quản trị mạng máy tính đã được Bộ Lao động – Thương binh và Xã hội ban hành. Giáo trình được biên soạn nhằm tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình giảng dạy.

Để thuận lợi trong quá trình tiếp thu các kiến thức và kỹ năng một cách đầy đủ, người học cần trang bị kiến thức cơ bản theo giáo trình "Quản trị mạng 1" thuộc chương trình khung Quản trị mạng máy tính.

Giáo trình gồm 10 chương được chia làm 2 phần:

Phần 1 – từ chương 1 đến chương 5 – cung cấp kiến thức và kỹ năng liên quan đến công tác giám sát mạng, triển khai và quản trị hệ thống từ xa; Ngoài ra, khả năng phát hiện và khôi phục khi server bị hỏng hóc cũng được đề cập đến. Chức năng của Group Policy trên Domain Controller mang tầm quan trọng rất lớn đối với hệ thống; Do vậy, tạo và quản lý các đối tượng trong Group Policy Object là kỹ năng không thể thiếu đối với người quản trị mạng.

Phần 2 – từ chương 6 đến chương 10 – giúp người học có kiến thức và kỹ năng bảo vệ hệ thống mạng với các tính năng quan trọng trên ISA Server; Bên cạnh đó, việc triển khai hệ thống mạng riêng ảo cho phép truy xuất tài nguyên khi người dùng không ở trong mạng nội bộ là công cụ tối ưu đối với người dùng. Khi không ở trong mạng, vấn đề sử dụng tài khoản của mình để gửi nhận mail trong mạng cục bộ cũng là công việc cấp thiết. Sự cố xảy ra đối với máy ISA là điều khó tránh khỏi; thao tác phát hiện và khắc phục kịp thời giúp hệ thống hoạt động một cách hoàn hảo.

Trong quá trình biên soạn giáo trình, chúng tôi đã tham khảo một số giáo trình và tài liệu của đồng nghiệp. Xin chân thành cảm ơn và mong được lượng thứ khi trích dẫn chưa được phép.

Giáo trình xuất bản đã đáp ứng kịp thời nhu cầu của người học; Tuy nhiên, khó tránh khỏi những khiếm khuyết. Nhóm biên soạn rất mong nhận được góp ý từ người đọc để hoàn thiện.

Tháng 05 năm 2012

MỤC LỤC

ĐỀ MỤC **TRANG**

MÔ ĐUN: QUẢN TRỊ MẠNG 2

Mã mô đun: MĐ 36

Vị trí, tính chất, ý nghĩa của mô đun:

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong môn, mô đun: Mạng máy tính, Quản trị mạng 1.
- Tính chất: Là mô đun chuyên ngành bắt buộc.
- Ý nghĩa: là mô đun giúp sinh viên Quản trị chuyên sâu hệ thống mạng; cài đặt, triển khai và cấu hình đảm bảo an toàn cho hệ thống mạng.

Mục tiêu của mô đun:

- Có khả năng tinh chỉnh và giám sát mạng Windows Server;
- Triển khai được dịch vụ Routing and Remote Access (RRAS);
- Có khả năng phát hiện và khôi phục Server bị hỏng;
- Có khả năng cài đặt và quản lý máy tính từ xa thông qua RAS;
- Xây dựng được một mạng riêng ảo VPN;
- Trình bày được các tính năng và những nét đặc trưng của ISA Server;
- Cài đặt và cấu hình được ISA Server trên Windows Server;
- Thực hiện được các Rule theo yêu cầu;
- Cài đặt và cấu hình được các chính sách mặc định của Firewall, thực hiện chính xác thao tác sao lưu cấu hình mặc định của Firewall;
- Trình bày được các cơ chế sao lưu, phục hồi toàn bộ máy ISA Server;
- Thực hiện được thao tác xuất, nhập các chính sách của Firewall ra thành file;
- Hiểu được các loại ISA Server Client đồng thời cài đặt và cấu hình đúng qui trình cho từng loại ISA Server Client và những tính năng riêng trên mỗi loại.
- Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.

Nội dung chính của mô đun:

Mã bài	Tên các bài trong mô-đun	Thời lượng			
		Tổng số	Lý thuyết	Thực hành	Kiểm tra
MĐ 36-01	Dịch vụ Windows terminal services	10	3	7	
MĐ 36-02	Tinh chỉnh và giám sát mạng Windows Server	10	3	7	
MĐ 36-03	Khôi phục server khi bị hỏng	5	2	2	1
MĐ 36-04	Cài đặt và quản lý remote access services (RAS) trong Windows Server	10	6	4	
MĐ 36-05	Group Policy Object	10	2	7	1
MĐ 36-06	Giới thiệu về ISA Server	4	4		
MĐ 36-07	Cài Đặt và cấu hình sử dụng các Rule trong ISA	13	2	11	
MĐ 36-08	Dịch vụ Virtual Private Network	8	3	4	1
MĐ 36-09	Publishing	13	3	9	1
MĐ 36-10	Monitor ISA Server	7	2	5	
Tổng cộng		**90**	**30**	**56**	**4**

YÊU CẦU VỀ ĐÁNH GIÁ HOÀN THÀNH MÔ ĐUN

- Về kiến thức:
  Có khả năng phát hiện các sự cố;
  Thực hiện được các biện pháp sao lưu dự phòng;
  Đánh giá được các thông lượng đường truyền;
  Có khả năng cài đặt, cấu hình kết nối Internet;
  Trình bày được các tính năng và những nét đặc trưng của ISA Server;
  Trình bày được các cơ chế sao lưu, phục hồi toàn bộ máy ISA Server;
  Hiểu được các loại ISA Server Client đồng thời cài đặt và cấu hình đúng qui trình cho từng loại ISA Server Client và những tính năng riêng trên mỗi loại.
- Về kỹ năng:
  Cài đặt, gỡ bỏ được các phần mềm yểm trợ Terminal service;
  Xác định được các nguyên nhân gây ra hỏng;
  Sử dụng được các biện pháp sao lưu dữ liệu;
  Giải quyết được các sự cố trên mạng;

Có khả năng cài đặt, quản lý các dịch vụ RAS;
Có khả năng kết nối một mạng riêng ảo VPN;
Có khả năng tiếp nhận các cuộc gọi ở xa;
Cài đặt và cấu hình được ISA Server trên windows Server;
Thực hiện được các Rule theo yêu cầu;
Cài đặt và cấu hình được các chính sách mặc định của Firewall, thực hiện chính xác thao tác sao lưu cấu hình mặc định của Firewall.

- Về thái độ: Cẩn thận, thao tác nhanh, chuẩn xác, tự giác trong học tập.

BÀI 1: DỊCH VỤ WINDOWS TERMINAL SERVICES

Mã bài: MĐ 36-01

Giới thiệu:

Bài học này cung cấp cho người học cách thức cài đặt, cấu hình và gỡ rối với dịch vụ Terminal Service của Windows Server. Trong đó, có thể quản trị server từ xa với bằng Terminal Service; Cấu hình Terminal Service và quản lý các phiên làm việc của Terminal Service.

Mục tiêu của bài:

- Có khả năng cài đặt và gỡ bỏ các phần mềm hỗ trợ;
- Có khả năng tạo máy khách Terminal Services;
- Quản lý được các dịch vụ của Terminal Services;
- Thực hiện các thao tác an toàn với máy tính.

1. Tại sao phải dùng Terminal Services

Mục tiêu: Giới thiệu cho người học về chức năng của dịch vụ Terminal Services cùng với các lợi ích đạt được khi sử dụng dịch vụ này.

Terminal Services là dịch vụ quản trị từ xa (*remote administration*). Thông qua Terminal Services, người quản trị có thể thực hiện các tác vụ quản trị từ bất kỳ một client nào.

Terminal Services đòi hỏi máy tính dùng làm Terminal Services Server đủ mạnh để giải quyết tất cả các người dùng kết nối tới nó và các client có thể chạy các phần mềm khách (*client software*) trên nó. Khi chạy Terminal Services cần phải mua và cấu hình tất cả các đăng ký một cách chính xác.

Sau khi cấu hình Terminal Services, chúng ta có thể bắt đầu triển khai các phần mềm khách và chủ. Terminal Services bao gồm một tiện ích cấu hình, một tiện ích quản trị và một công cụ tạo client để quản lý các server và client.

Trong bài học này, người học sẽ biết Terminal Services làm việc như thế nào, cách cài đặt, cấu hình và quản lý máy chủ và máy khách của Terminal Services.

Terminal Services

Terminal Services có thể chạy bằng một trong hai chế độ sau:

• Trong chế độ quản trị từ xa (*remote administration mode*), người quản trị có thể thực hiện các tác vụ quản trị từ bất kỳ máy khách nào trong mạng.

• Trong chế độ chương trình ứng dụng của máy chủ (*application server mode*), người dùng phải truy cập từ xa đến các chương trình ứng dụng có trên server. Dùng chế độ này, Terminal Services phân phát môi trường Windows Desktop cho các máy tính có thể không chạy được Windows bởi các hạn chế về phần cứng hay lý do khác.

Trong chế độ *application server mode*, các giao diện đồ họa của máy chủ được truyền cho các máy khách ở xa; các máy này gửi các tín hiệu bàn phím và tín hiệu chuột cho máy chủ. Các máy khách gọi là các *thin client*. Người dùng đăng nhập vào thông qua bất cứ máy khách nào trên mạng và chỉ nhìn thấy các phiên làm việc (*session*) của riêng họ.

Terminal Services quản lý các session duy nhất của client một cách trong suốt. Rất nhiều loại thiết bị phần cứng có thể chạy trên các phần mềm của *thin client*, gồm cả các thiết bị đầu cuối và máy tính nền Windows.

Lợi ích của Terminal Services

Terminal Services cung cấp nhiều lợi ích làm cho nó trở thành giải pháp ưu việt nhất cho mạng:

Sự phát triển rộng hơn của Windows Server - Thay vì cài đặt một phiên bản đầy đủ của Windows Server trên các máy, có thể triển khai Terminal Services. Các máy tính có phần cứng không dùng được phiên bản đầy đủ của Windows Server hỗ trợ vẫn có thể sử dụng nhiều đặc tính của Windows Server.

Sự hoạt động đồng thời của cả phần mềm thin client và các hệ điều hành độc lập - Với Terminal Services, người dùng mạng có thể tiếp tục sử dụng hệ thống có sẵn trong máy của họ, và có thể dùng các lợi ích của môi trường Windows Server.

Sự phát triển các ứng dụng được đơn giản hoá - Thay vì cài đặt và cập nhật các ứng dụng trên tất cả các máy trong mạng thì người quản trị có thể cài đặt một bản sao trên Terminal Services server. Điều này đảm bảo rằng mọi người dùng đều truy cập được vào phiên bản mới nhất của ứng dụng.

Việc quản trị từ xa của máy chủ - Terminal Services cho phép quản trị server từ xa. Điều này rất hữu ích nếu người quản trị cần phải rời xa máy chủ trong một khoảng thời gian nào đó.

2. Mô hình xử lý của Terminal Services

Mục tiêu: Giới thiệu các thành phần của Terminal cùng với chức năng của mỗi thành phần. Ngoài ra, người học sẽ biết được yêu cầu xác định ứng dụng nào sẽ được chia xẻ và loại phần cứng nào sẽ được sử dụng.

2.1. Các thành phần của Terminal Services

Terminal Services bao gồm 3 thành phần: Terminal Services server, giao thức Remote Desktop, và Terminal Services client. Terminal Services server giao tiếp với Terminal Services client bằng cách sử dụng giao thức Remote Desktop.

- Terminal Services server

Hầu hết các hoạt động của Terminal Services xảy ra trên Terminal Services server (hay gọi là Terminal server). Khi Terminal Services ở trong chế độ ứng dụng của máy chủ, tất cả các ứng dụng đều chạy trên server. Terminal server sẽ gửi các thông tin về màn hình tới client và chỉ nhận các input từ chuột và bàn phím. Server phải theo dõi các session đang hoạt động.

- Giao thức Remote Desktop

Khi cài đặt Terminal Services, giao thức Remote Desktop (RDP) được tự động cài đặt. RDP là một kết nối duy nhất cần phải cấu hình để client có thể kết nối tới Terminal server. Chúng ta có thể cấu hình chỉ một kết nối RDP trên mỗi card mạng.

Có thể sử dụng công cụ cấu hình của Terminal Services để cấu hình các thuộc tính của kết nối RDP; có thể thiết lập mật mã và quyền, và hạn chế lượng thời gian mà các session của client có thể còn hoạt động.

- Terminal Services client

Terminal Services client (hay Terminal client) sử dụng công nghệ *thin client* để phân phối Windows Server Desktop tới người dùng. Client chỉ cần thiết lập một kết nối tới server và hiển thị thông tin về giao diện đồ họa mà server gửi tới. Quá trình này cần chạy một phần trên máy khách và nó có thể chạy trên các máy tính cũ không thậm chí cả những máy không thể cài Windows Server.

2.2. Lập kế hoạch cấu hình Terminal Services

Trước khi sử dụng Terminal Services, cần phải xác định ứng dụng nào sẽ được chia xẻ và loại phần cứng nào sẽ được sử dụng. Những yêu cầu này để chạy Terminal Services quan trọng hơn nhiều so với chạy Windows server bình thường, đặc biệt là nếu người dùng đang sử dụng chế độ ứng dụng của server.

Cần phải xem xét phạm vi và giá thành của việc đăng ký cấu hình Terminal Services. Mỗi client kết nối tới Terminal server phải có một chứng nhận đặc biệt của Terminal Services client.

Xác định ứng dụng client

Các ứng dụng sử dụng cùng với Terminal Services được cài đặt trên cơ sở mỗi máy (per-computer) thay vì trên cơ sở mỗi người dùng (per-user). Chúng phải có sẵn với mọi người dùng truy cập Terminal Services trực tiếp hay từ một session ở xa.

Terminal Services thường đòi hỏi thêm tài nguyên hệ thống để quản trị tất cả các lưu thông của client. Cần phải biết được các đặc tính của các chương trình nào đó mà có thể yêu cầu nhiều tài nguyên từ server. Các chương trình trên nền Intel chạy trên máy Apple, các chương trình có nhiều hình ảnh video, các chương trình MS-DOS, và liên tục chạy các bit mã (như là các bộ kiểm tra lỗi chính tả) có thể làm cạn tài nguyên hệ thống. Cần phải hạn chế các truy cập tới các loại chương trình này chỉ cho những người dùng thật sự cần chúng và tắt tất cả các đặc tính tuỳ chọn của chương trình mà có thể đè nặng lên hệ thống một cách không cần thiết.

Windows Server là một môi trường 32 bit. Để chạy một chương trình 16 bit, Windows Server cần phải dùng đến hệ thống "Windows trên Windows" (WOW), sẽ rất tốn tài nguyên hệ thống. Sử dụng các ứng dụng 16 bit làm giảm số lượng người dùng mà một bộ xử lý đơn lẻ có thể giải quyết khoảng 40% và có thể tăng lượng bộ nhớ cho mỗi người dùng khoảng 50%. Rõ ràng, tốt nhất là nên sử dụng ứng dụng 32 bit mỗi khi có thể.

3. Yêu cầu đối với Server và Client

Mục tiêu: cho phép xác định các yêu cầu về phần cứng đối với server và client để đảm bảo hiệu suất hoạt động dịch vụ Terminal Services.

3.1. Các yêu cầu đối với Terminal Services server

Các yêu cầu phần cứng cho một Terminal server phụ thuộc vào số client sẽ kết nối cùng lúc và nhu cầu sử dụng của client. Sau đây là một số hướng dẫn:

• Một Terminal server cần ít nhất một bộ xử lý Pentium và 128MB RAM để hoạt động được đầy đủ. Ngoài ra, cần cung cấp thêm 10 hay 20MB RAM cho mỗi kết nối của client, tuỳ thuộc vào ứng dụng mà client sử dụng. Terminal server chia xẻ các tài nguyên có tính khả thi giữa các người dùng, do vậy bộ nhớ cần cho các người dùng bổ sung chạy cùng ứng dụng ít hơn bộ nhớ cần cho người dùng đầu tiên tải chương trình.

• Nên sử dụng một kiến trúc bus hoạt động cao như là EISA, MCA, hay PCI. Bus ISA (AT) không thể chuyển đầy đủ dữ liệu cho kiểu lưu thông mạng sinh ra do một cách cài đặt Terminal Services thông thường.

• Phải cân nhắc việc sử dụng ổ đĩa SCSI, hay loại tốt hơn là FAST SCSI hay SCSI-2. Để hoạt động tốt nhất thì nên dùng loại đĩa SCSI với RAID sẽ tăng thời gian truy cập đĩa bằng cách đặt dữ liệu lên trên nhiều đĩa.

• Vì nhiều người dùng có thể truy cập vào Terminal server cùng một lúc; Do đó, cần sử dụng bộ điều hợp mạng tốc độ cao. Giải pháp tốt nhất là cài đặt 2 bộ điều hợp trong máy và dành một cái cho lưu thông mạng RDP.

3.2. Các yêu cầu đối với Terminal Services client

Terminal Services client chạy tốt trên nhiều máy khác nhau kể cả các máy lỗi thời và các thiết bị đầu cuối đã cũ không thể cài đặt hay chạy Windows Server. Phần mềm phía client phải chạy trên các máy sau:

• Các thiết bị đầu cuối nền Windows (nhúng)

• Các máy nền Intel và Alpha chạy Windows for Workgroup 3.11, Windows 95, Windows 98, Windows NT 3.51, Windows NT 4.0, Windows 2000

• Các máy Macintosh và Unix (với các phần mềm của các hãng thứ 3)

3.3. Xác định yêu cầu đăng ký chính xác

Terminal Services sử dụng phương pháp đăng ký riêng của nó. Một Terminal client phải nhận được một đăng ký hợp lệ từ Terminal Services licence server trước khi logon vào Terminal server. Điều này chỉ áp dụng cho application server mode. Khi sử dụng chế độ quản trị từ xa, hai session của client đồng thời được cho phép một cách tự động mà không cần phải nhận một đăng ký từ một server cấp đăng ký (license server).

Có thể tạo quyền cho Terminal Services Lisensing ngay khi cài đặt Windows Server hay sau đó thông qua biểu tượng Add/Remove Program trong Control Panel. Khi kích hoạt Terminal Services Lisensing, có thể chọn giữa hai loại license server:

• Một enterprise license server có thể phục vụ Terminal server trên bất kỳ miền nào của Windows server, nhưng không thể phục vụ các nhóm làm việc hay các miền của Windows NT 4.

• Một Domain license server chỉ có thể phục vụ Terminal server trong cùng miền.

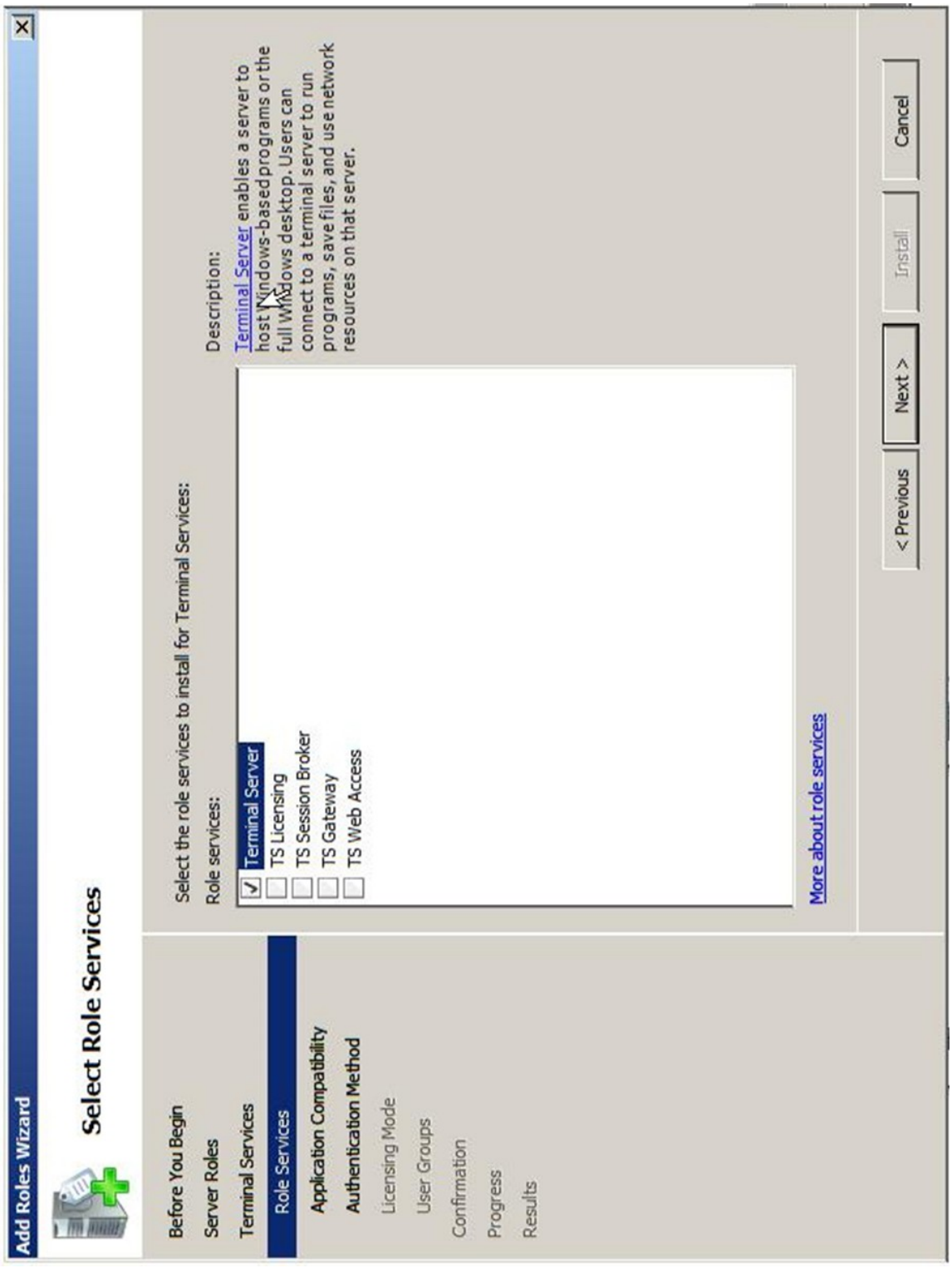
Trong các miền của Windows server, các Domain license server phải được cài đặt trên một máy điều khiển miền (domain controller). Trong các nhóm làm việc hay trên miền của Windows NT4, domain license server có thể được cài đặt trên bất cứ server thành viên nào.

4. Cài đặt Terminal Services

Mục tiêu: Trình bày các thao tác cài đặt Terminal Services Server, thêm người dùng vào danh sách người dùng được phép sử dụng Remote Desktop.

4.1. Cài đặt Terminal Services Server

Terminal server có thể được cài đặt từ *Server Manager*. Trong *Server Manager*, bấm vào *Roles* trong ngăn bên trái và nhấp vào *Add Roles* trong màn hình kết quả để gọi *Add Roles Wizard*. Nếu màn hình giới thiệu xuất hiện, bấm vào *Next* để liệt kê các roles có sẵn. Trên màn hình *Select Server Roles* , chọn Terminal Services và bấm vào *Next* để chọn các dịch vụ được yêu cầu.



Lựa chọn dịch vụ để cài đặt

Sau khi nhấp vào *Next*, màn hình cảnh báo sẽ xuất hiện đề xuất rằng bất kỳ ứng dụng nào nhằm mục đích được truy cập bởi người sử dụng Terminal Services không được cài đặt cho đến khi các quy tắc của Terminal Services role được cài đặt. Sau khi đọc thông tin, bấm *Next* để tiếp tục đến màn hình lựa chọn xác thực. Chọn *Require Network Level Authentication* sẽ ngăn chặn người dùng chạy trên hệ thống cũ hơn mà không cần xác thực mức mạng truy cập vào Terminal Services. Việc xác thực được thực hiện trước khi phiên làm việc từ xa được thành lập. Nếu xác thực ít nghiêm ngặt là chấp nhận được, hoặc một số người dùng đang chạy hệ

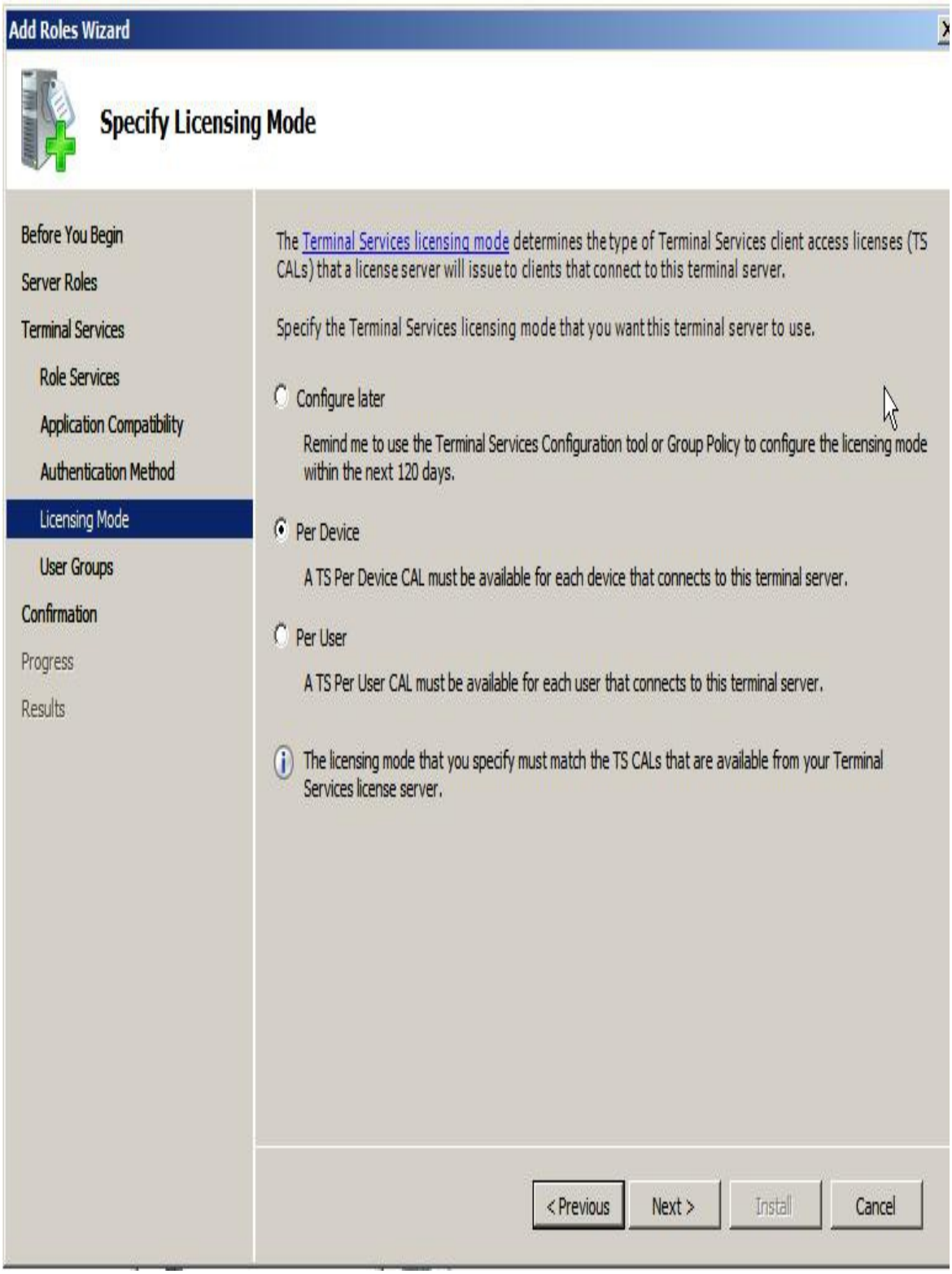
thống cũ hơn. Chọn tùy chọn *Do not require Network level Authentication* rồi nhấp vào *Next* để tiến hành.

Màn hình *Specify Licensing Mode* cho phép chỉ định phương án cấp phép.

- *Configure later*: cho phép sử dụng 120 ngày mà không cần cung cấp license (sử dụng công cụ Terminal Services hoặc Group Policy để cấu hình)

- *Per Device*: cho phép chỉ định số thiết bị kết nối bất kỳ lúc nào

- *Per user: hạn chế người dùng truy nhập*



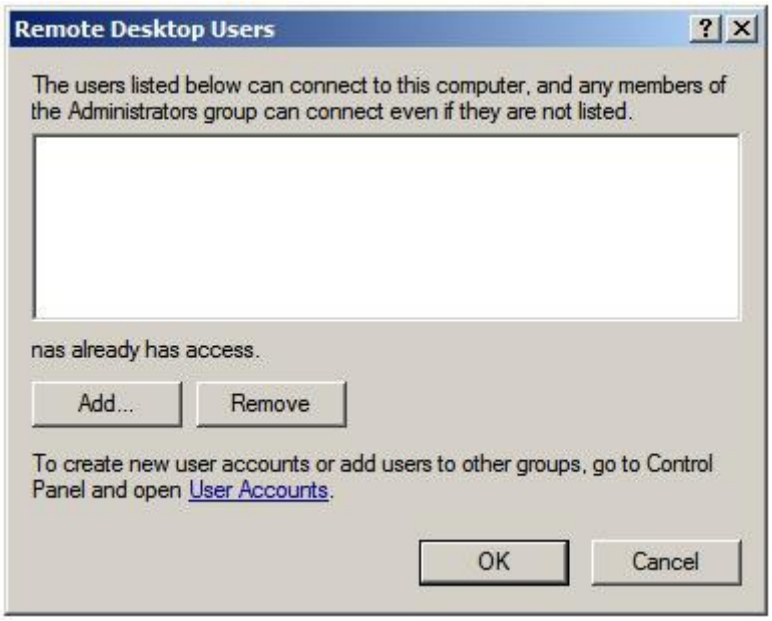
Lựa chọn license để sử dụng

Cuối cùng, người dùng và nhóm được phép truy cập vào terminal server phải được xác định, mặc dù người dùng có thể được thêm vào và loại bỏ bất kỳ lúc nào bằng cách thay đổi các thành viên của *Remote Desktop Users Group*. Nhấp vào *Add...* để thêm bất kỳ người dùng. Nhấp vào Next để chuyển đến màn hình *Confirmation,* chọn *Install* bắt đầu tiến trình cài đặt.

Sau khi cài đặt, khởi động lại hệ thống và đăng nhập với quyền administrator.

4.2. Thêm người dùng vào nhóm Remote Desktop Users

Mặc định, tất cả các thành viên của nhóm Administration đều được kết nối từ xa. Để thêm hay loại bỏ người dùng được phép truy cập từ xa, mở Control Panel -> System and Maintenance -> System -> Remote settings, chọn Select Users. Trong hộp thoại Remote Desktop Users, chỉ định những người dùng cần thêm vào hay xóa bỏ khỏi danh sách.



Hộp thoại liệt kê người dùng được phép truy cập từ xa

Lưu ý: mặc định người dùng với quyền quản trị có thể truy cập từ xa vào máy tính này nên không cần thêm vào danh sách.

5. Cấu hình và truy cập từ client vào Terminal Server

Mục tiêu: Trình bày các bước thực hiện truy cập vào server thông qua Remote Desktop, cách thoát khỏi phiên làm việc đối với server từ máy client. Bên cạnh đó, ý nghĩa của các tùy chọn cấu hình cũng được giải thích.

5.1. Truy cập từ client vào Terminal Server

Sau khi được cài đặt và cấu hình trên server, có thể truy cập từ client vào Terminal Server bằng một trong hai cách:

- *Start -> All Programs -> Accessories -> Remote Desktop Connection*
- Start -> Run, gõ mstsc

Hộp thoại chỉ định tên hay địa chỉ máy server cần kết nối

5.2. Tùy chọn cấu hình máy khách Remote Desktop

Trong hộp thoại Remote Desktop Connection, chọn Options:

- **General**: Lưu trữ thông tin đăng nhập và thông tin section.
- **Display**: sử dụng các thiết lập trên server với máy client.
- **Local Resources**: chỉ định tài nguyên cục bộ được sử dụng trong suốt phiên Remote Desktop.
- **Programs:** cho phép các chương trình cụ thể được tự động kích hoạt mỗi khi một phiên từ xa được thiết lập.
- **Experience**: điều khiển các tính năng được kích hoạt hoặc vô hiệu hoá cho phiên làm việc từ xa. Tại đây cũng cung cấp các tùy chọn để có thể tự động tái lập kết nối khi phiên làm việc bị ngắt.
- **Advanced**: kích hoạt hoặc vô hiệu hoá xác thực từ xa.

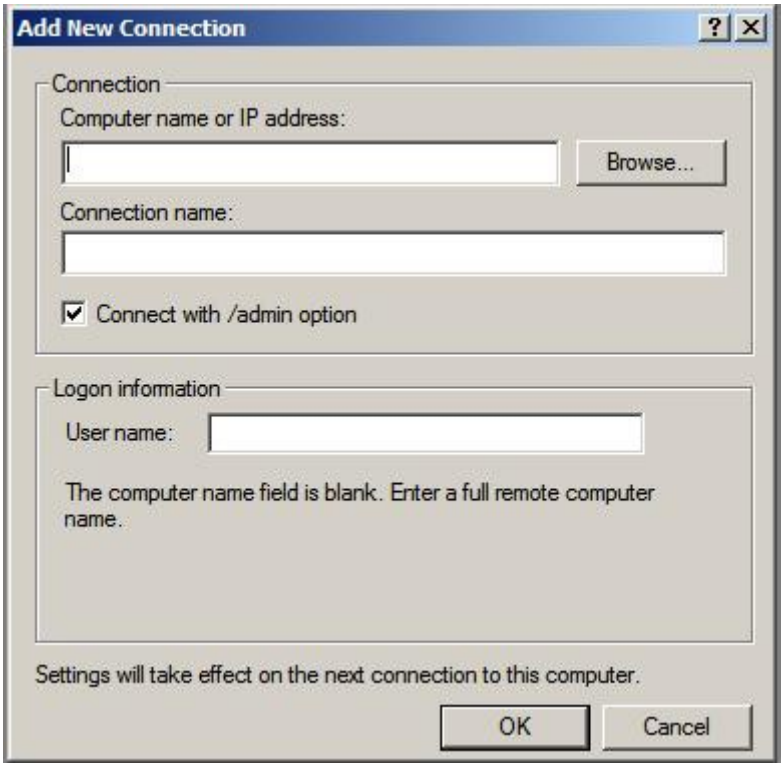
5.3. Thoát khỏi phiên truy cập từ xa

Khi nhấn vào biểu tượng "X" trên bảng điều khiển tại máy client, phiên truy cập từ xa vẫn còn tiếp tục chạy trên server; nghĩa là nếu người dùng kết nối trở lại, phiên truy cập từ xa vẫn tiếp tục. Để kết thúc phiên truy cập từ xa, chọn Start -> chọn Log Off để đóng phiên truy cập từ xa này.

6. Thực hiện đa kết nối truy cập từ xa

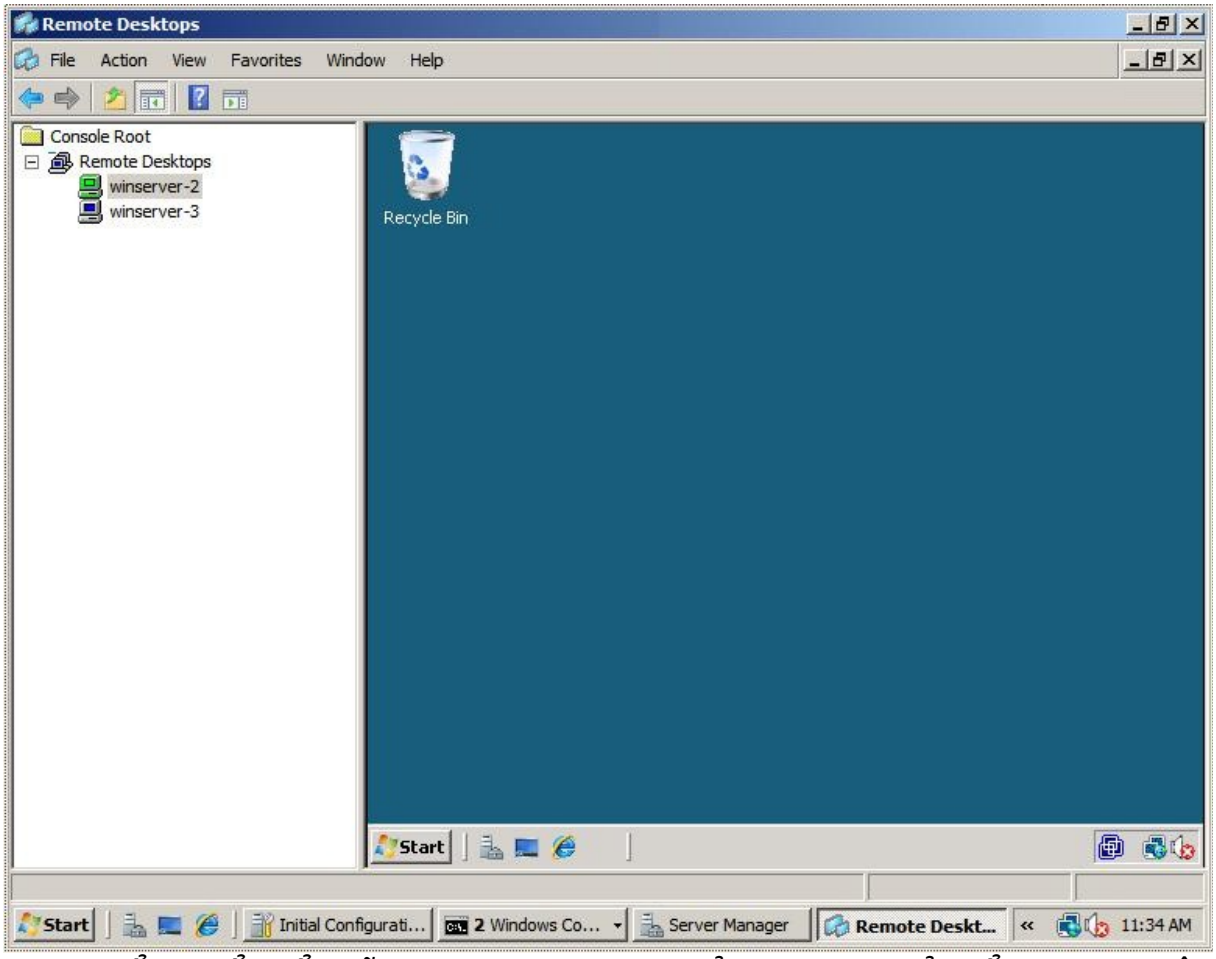
Mục tiêu: Trình bày cách quản lý các phiên kết nối đến các server đồng thời qua công cụ Remote Desktop.

Để thực hiện đồng thời nhiều kết nối truy cập từ xa trong cùng một cửa sổ, sử dụng MMC *Remote Desktops*. Từ Start -> Run, gõ tsmmc.msc, chọn *Remote desktops* ở khung trái, chọn Add a new connection từ menu.



Thêm kết nối truy cập từ xa (đồng thời)

Sau khi thêm kết nối, phiên kết nối truy cập từ xa sẽ xuất hiện trên cửa sổ chính.



Để chuyển đổi giữa các phiên, chọn tên của phiên bên cửa sổ trái, giao diện

tương ứng sẽ được hiển thị.

Câu hỏi

1. Terminal Services là gì ? Trình bày các lợi ích của Terminal Services.

2. Trình bày các thành phần của Terminal Services và chức năng của mỗi thành phần.

Bài tập thực hành

1. Cài đặt Terminal Services.

   Các bước thực hiện:
   - Cài đặt Terminal Services Server
   - Cài đặt Terminal Services Licence Server
   - Cho phép account có quyền sử dụng Terminal Services
   - Cài đặt Terminal Services Client

2. Cấu hình và quản lý Terminal Services.

   Các bước thực hiện:
   - Khởi động Terminal Services Manager
   - Theo dõi và quản lý các user đang connect

3. Thực hiện Remote Desktop từ client.

BÀI 2: TINH CHỈNH VÀ GIÁM SÁT MẠNG WINDOWS SERVER

Mã bài: MĐ 36-02

Giới thiệu:

Trên một hệ thống mạng, máy chủ đóng vai trò rất quan trọng. Trong đó việc giám sát hệ thống và quản lý dữ liệu được xem là phần không thể thiếu trong quá trình quản trị hệ thống.

Bài học này sẽ cung cấp các vấn đề liên quan đến các công cụ chính để giám sát là System Monitor và các phương án giải quyết các vấn đề bằng Event Viewer và Performance.

Mục tiêu của bài:

- Hiểu được vai trò chức năng của các công cụ System Monitor, Performance Logs and Alerts;
- Giải quyết được các sự cố mạng thông qua Event Viewer;
- Kiểm tra được tần suất hoạt động của hệ thống tại từng thời điểm khác nhau Task Manager;
- Thực hiện các thao tác an toàn với máy tính.

1. Tổng quan về công cụ tinh chỉnh

Mục tiêu: Giới thiệu sơ lược về các công cụ dùng để quan sát và tinh chỉnh hệ thống với hệ điều hành Windows Server.

Là một nhà quản trị mạng với hệ thống mạng bao gồm một máy chủ chứa dữ liệu rất quan trọng. Máy chủ có thể chạy liên tục, nhưng khi người quản trị truy cập vào máy chủ thì báo lỗi từ chối dịch vụ do không thể kết nối. Khi xem xét tình hình thì thấy một số dữ liệu đã bị mất, lúc này cần xem ai đã gây ra vấn đề trên, việc ghi lại log của hệ thống ngoài việc cho phép người quản trị phát hiện ra các lỗi trong quá trình hoạt động của hệ thống còn cho phép phát hiện ra những truy cập bất hợp pháp.

Toàn bộ các vấn đề liên quan tới log hệ thống được tích hợp trên Windows với hai công cụ chính đó là Event Viewer và Reliability and Performance Monitor.

2. Quan sát các đường biểu diễn hiệu năng bằng Reliability and Performance Monitor (perfmon.msc)

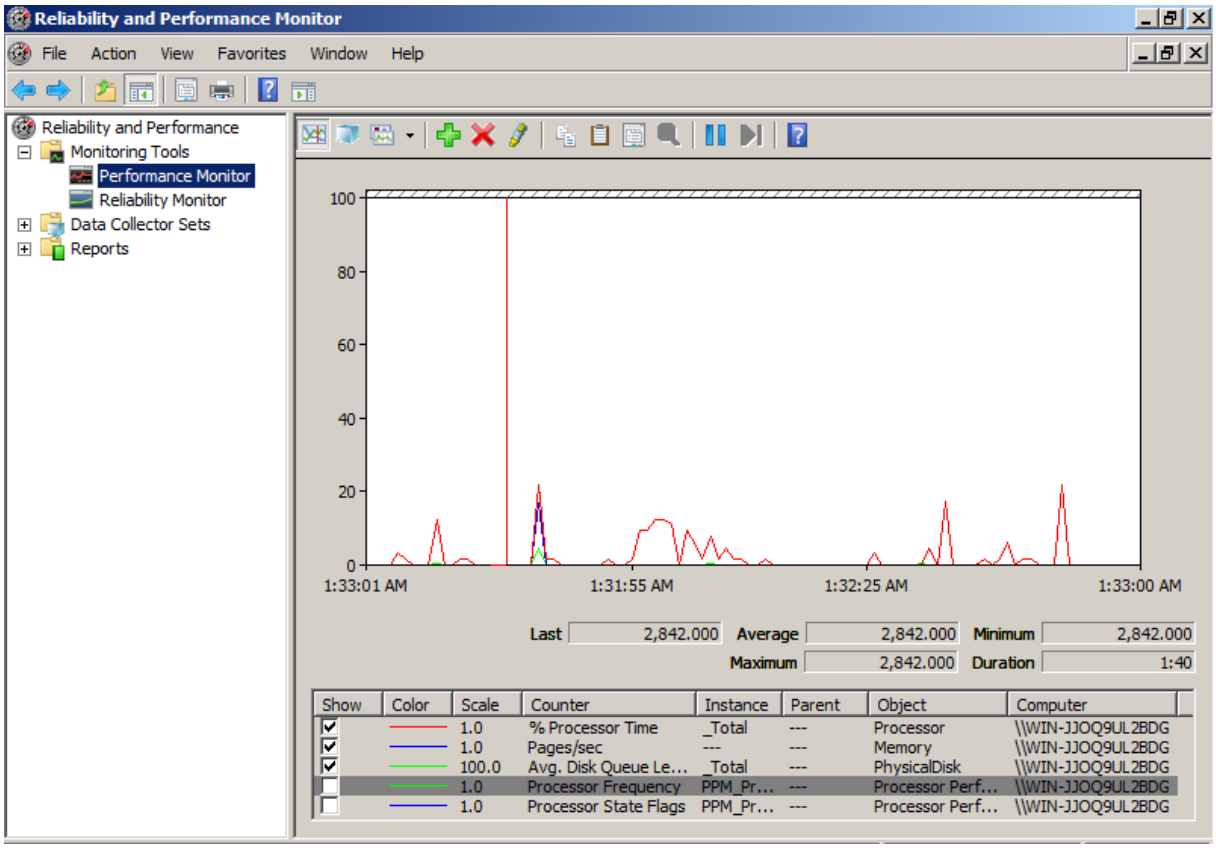
Mục tiêu: Trình bày chi tiết cách dùng công cụ Performance Monitor để giám sát các counter chi tiết của những đối tượng; công cụ Reliability Monitor để giám sát độ tin cậy của một hệ thống.

Khi nói đến giám sát hệ thống người ta sẽ nghĩ ngay tới công cụ chủ yếu là Performance Monitor và Reliability Monitor của Monitoring Tools trong Reliability and Performance Monitor.

Để sử dụng công cụ Reliability and Performance Monitor, từ menu Start, chọn Run; khi hộp thoại Run xuất hiện, gõ perfmon.msc

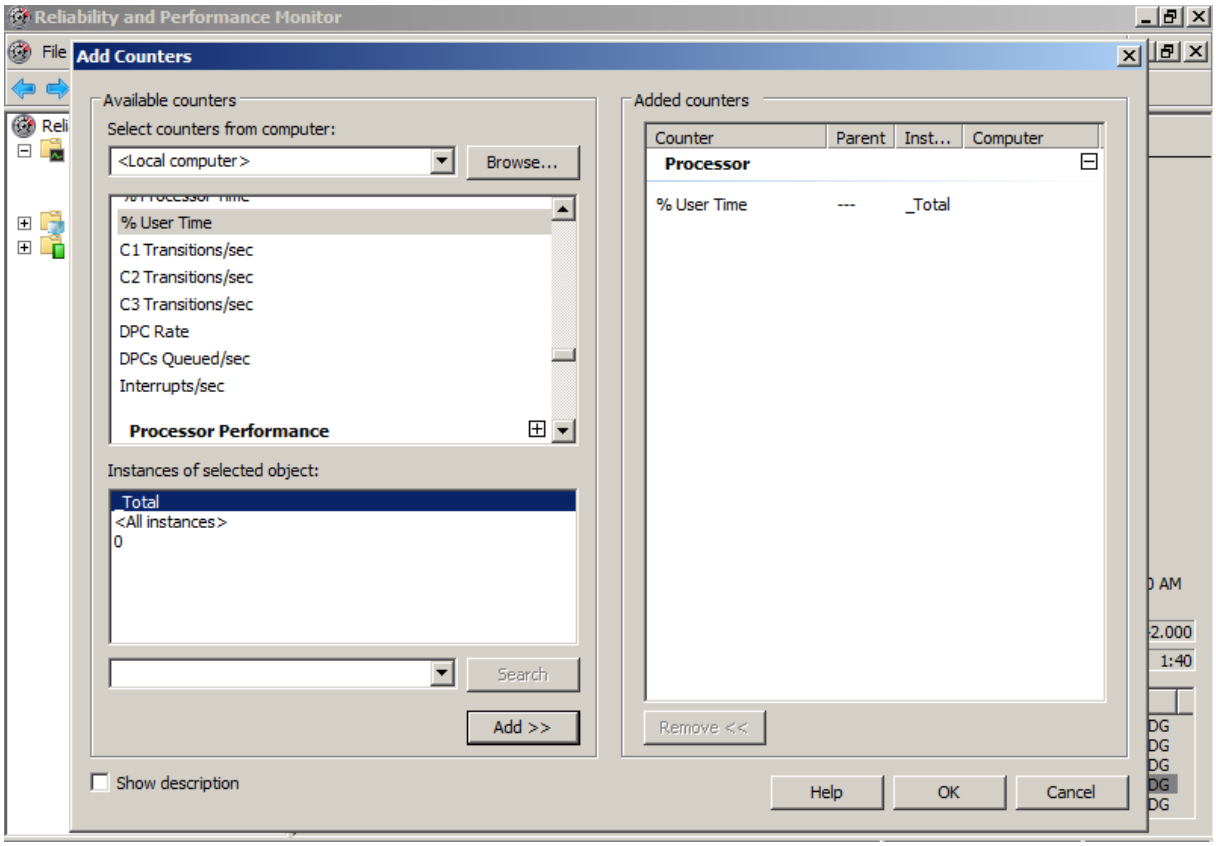
2.1. **Performance Monitor**

Performance Monitor là một công cụ rất mạnh để giám sát các counter chi tiết của những đối tượng khác nhau, với tính năng thêm bớt rất linh hoạt cho phép người dùng có thể chỉ cần nhấn vào dấu + để add thêm các counter khác, hoặc có thể nhấn X để không giám sát những counter không cần thiết. Mặc định hệ thống sẽ giám sát ba đối tượng là: Memory, PhysicalDisk, và Processor. Các thuộc tính đặc trưng của mỗi đối tượng là: Memory với thuộc tính Pages/sec, PhysicalDisk với thuộc tính AVG Disk Queue Length, với Processor có thuộc tính % Preccessor Time (hình 2.1)



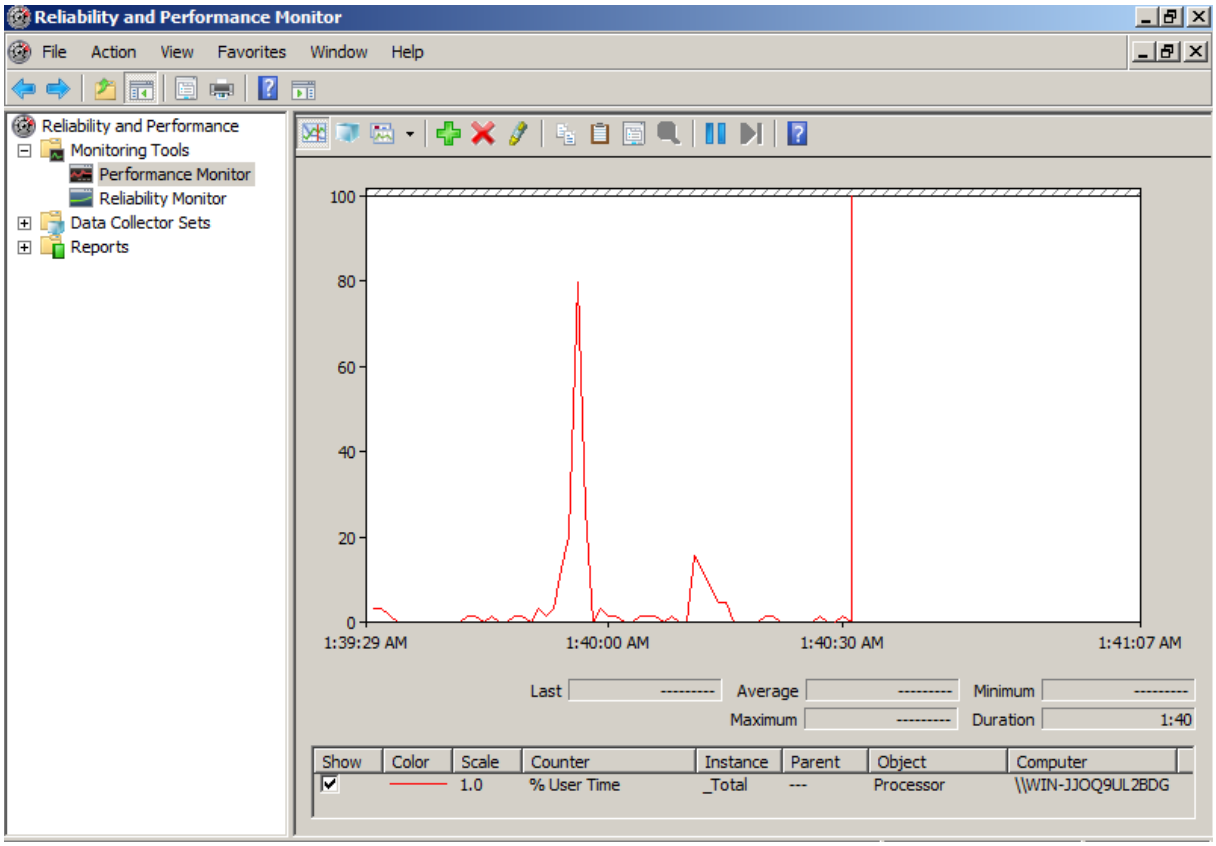
Hình 2.1 – Giao diện Performance Monitor

Khi muốn thêm các counter của một object cụ thể, nhấn vào nút + sẽ suất hiện cửa cửa sổ. Hình 2.2 minh họa việc add thêm thuộc tính %user time của Processor.



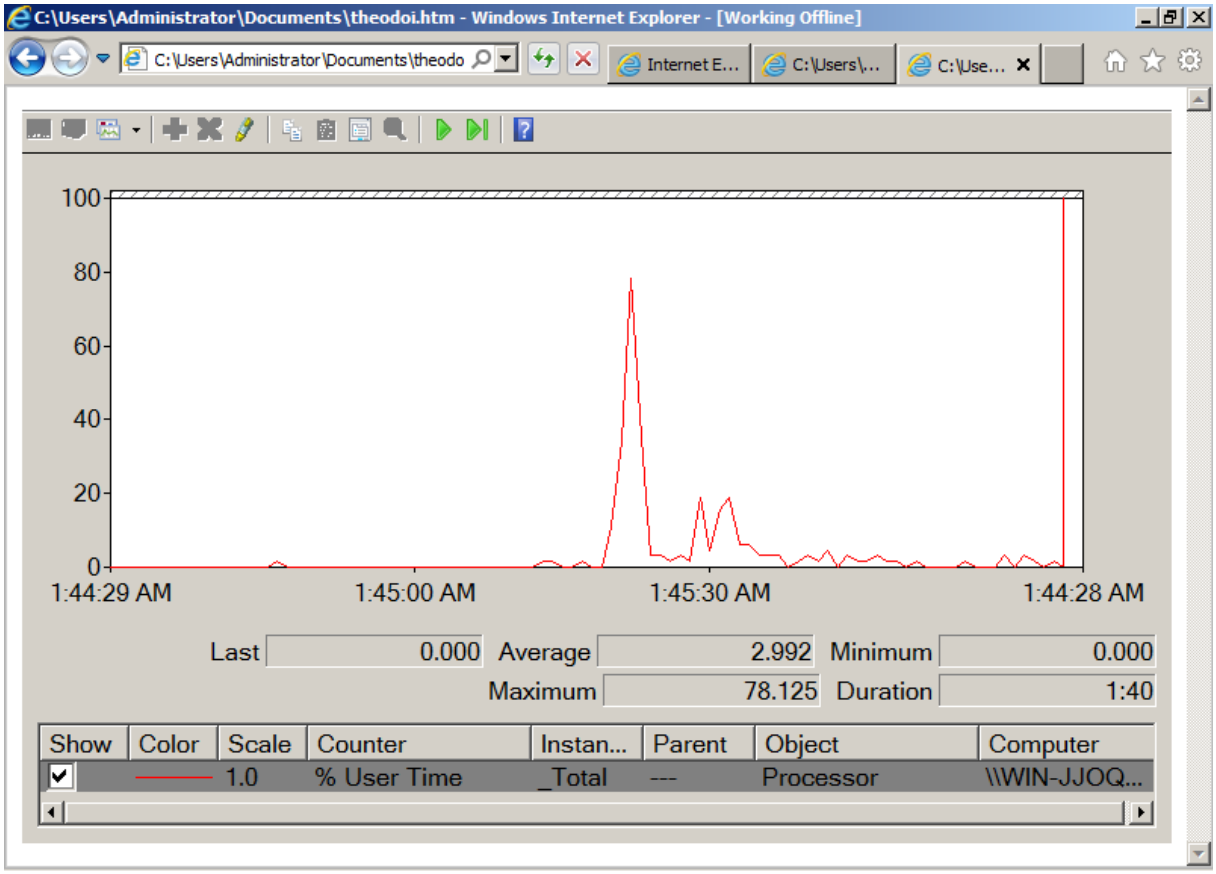
Hình 2.2 – Thêm các counter vào theo dõi

Sau đó loại bỏ toàn bộ các counter khác của các đối tượng khác và chỉ giám sát mỗi counter % User Time của processor mà thôi – xem hình 2.3



Hình 2.3 – Giám sát counter % User Time của đối tượng Processor

Khi cần xem lại, nhấp chuột phải vào cửa sổ, chọn Save Settings As… để lưu với định dạng html. Với định dạng này có thể view trực tiếp hoặc có thể xem các quá trình đã được ghi lại trong hệ thống (hình 2.6.)



Hình 2.6 – Xem lại các thiết lập đã được ghi lại bởi định dạng file html

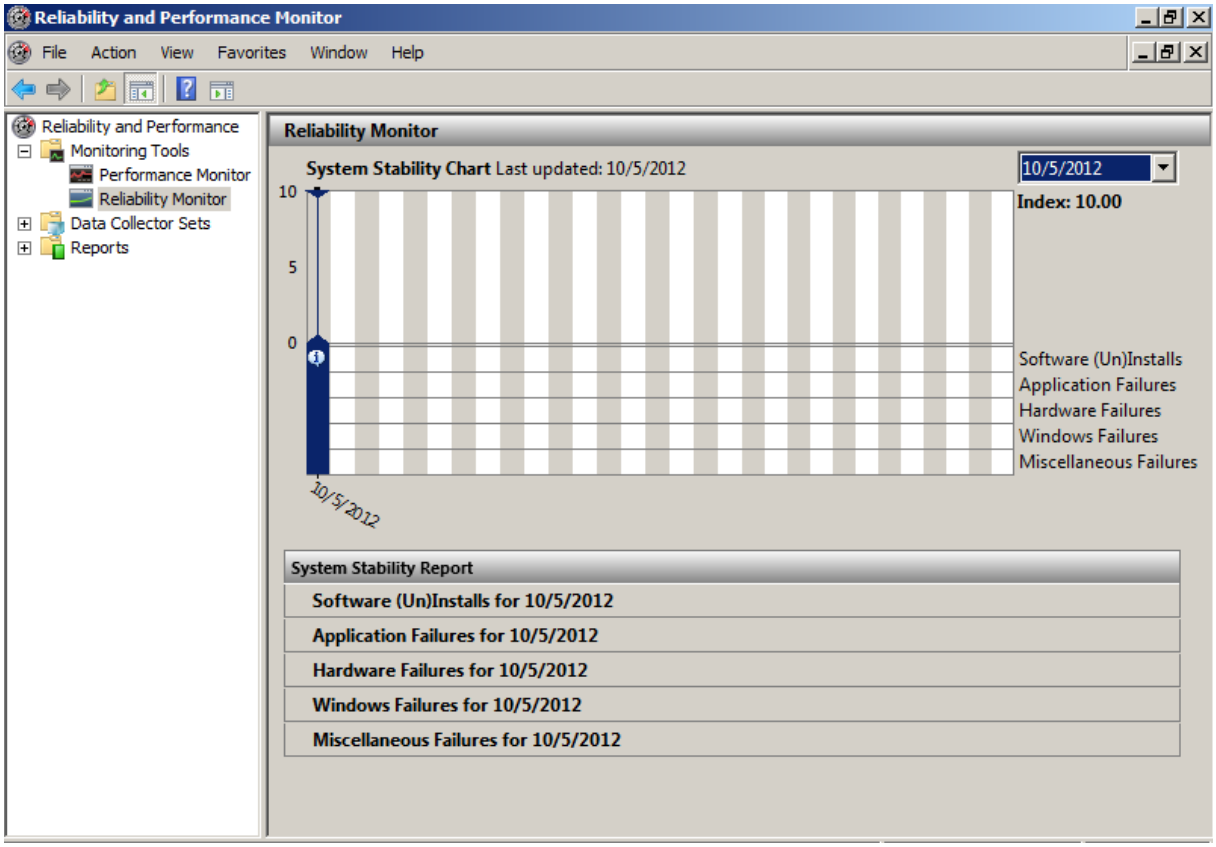
2.2. **Reliability Monitor**

Độ tin cậy của một hệ thống là thước đo mức độ thường xuyên hệ thống hoạt động như là cấu hình và dự kiến sẽ thực hiện. Độ tin cậy có thể giảm khi ứng dụng ngừng đáp ứng, dừng và khởi động lại các dịch vụ, khởi tạo các trình điều khiển bị lỗi, hoặc trong trường hợp xấu nhất, khi hệ điều hành bị lỗi.

Reliability Monitor cung cấp thông tin tổng quát một cách nhanh chóng. Ngoài ra, nó theo dõi sự kiện sẽ giúp xác định những gì gây ra lỗi. Bằng cách ghi lại các lỗi (bao gồm cả lỗi bộ nhớ, đĩa cứng, ứng dụng và hệ điều hành), nhưng cũng có các sự kiện quan trọng về cấu hình của hệ thống (bao gồm cả việc cài đặt ứng dụng mới, cập nhật hệ điều hành.

Reliability Monitor ước tính chỉ số ổn định hệ thống (System Stability Index) với một biểu đồ chỉ số ổn định để xác định một cách nhanh chóng các vấn đề có thể xảy ra. Các báo cáo kèm theo cung cấp một cách chi tiết giúp xác định và khắc phục sự cố các nguyên nhân xảy ra lỗi. Khi xem các thay đổi trên hệ thống từ báo cáo (cài đặt / loại bỏ các ứng dụng, cập nhật hệ điều hành hay lỗi phần cứng)

người quản trị có thể có chiến lược để giải quyết các vấn đề một cách nhanh chóng.



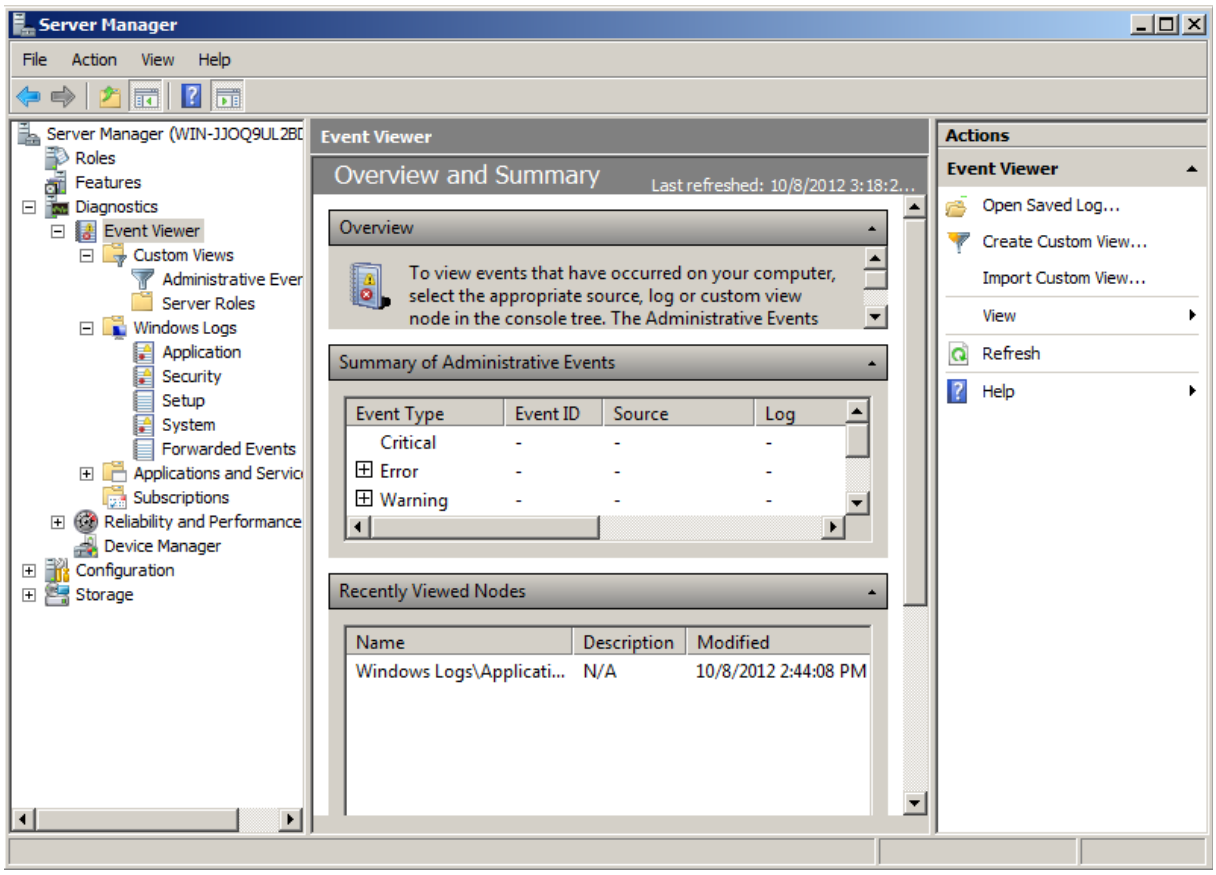
3. Ghi lại sự kiện hệ thống bằng công cụ Event Viewer

Mục tiêu: Quản lý hệ thống mạng không thể thiếu phần giám sát hệ thống. Ngoài việc ghi lại các tiến trình trong hệ thống, người quản trị còn phải biết điều chỉnh thiết lập chỉ ghi lại những yếu tố cần thiết. Chẳng hạn một máy chủ File Server chỉ cần giám quá trình truy cập tài nguyên, máy chủ Active Directory giám sát quá trình log on vào hệ thống. Trong phần này sẽ giới thiệu công cụ Event Viewer - một công cụ ghi lại các event của hệ thống.

Event Viewer là một công cụ tích hợp trong Windows cho phép xem lại các sự kiện đã xảy ra trong hệ thống một cách chi tiết với nhiều tham số cụ thể như: user, time, computer, services… Các sự kiện rời rạc được lọc lại thành những sự kiện giống nhau giúp chúng ta lấy được những thông tin cần thiết một cách nhanh nhất.

Trong Event Viewer đã phân vùng các sự kiện riêng biệt cho từng ứng dụng, một máy chủ cài đặt mặc định sẽ có các phân vùng trong Event Viewer: Application, Security, System

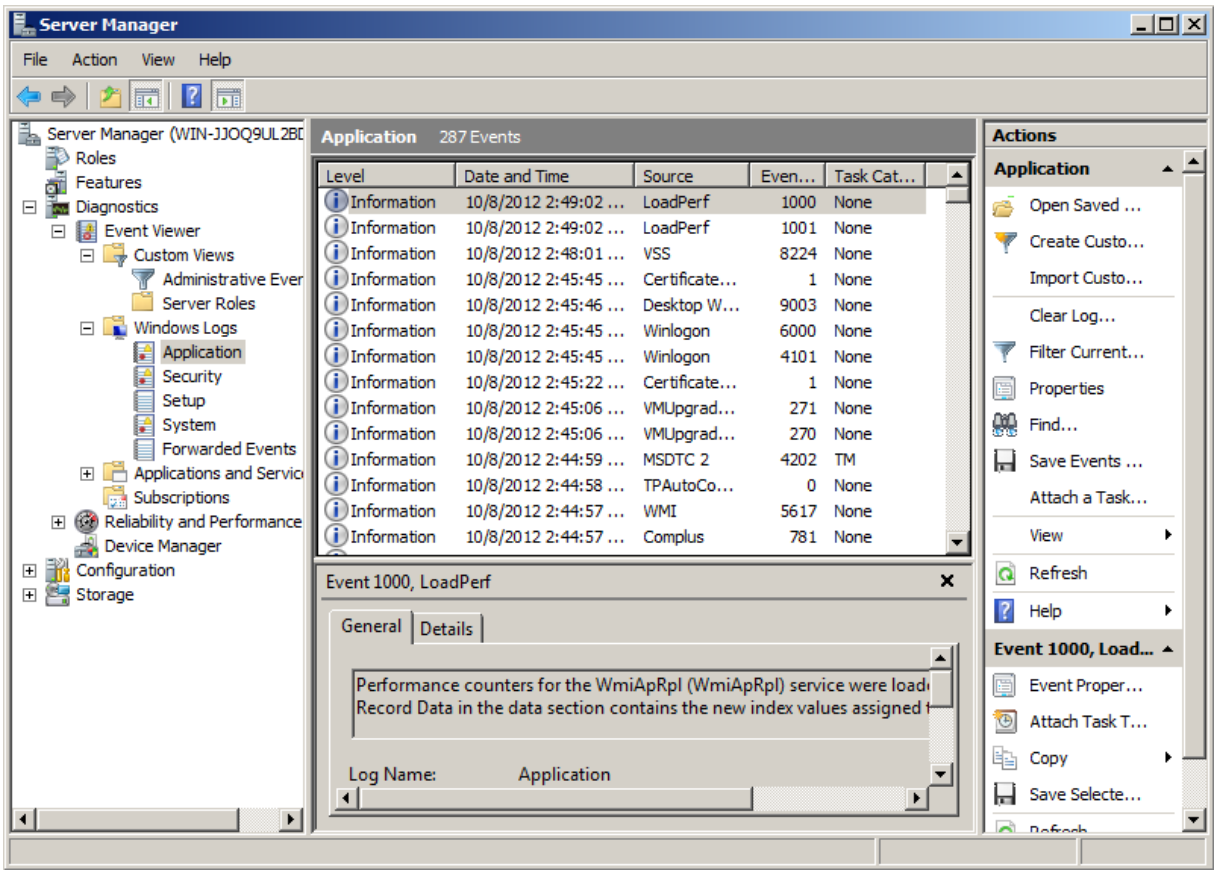
Để mở Event Viewer, mở công cụ Server Manager bằng cách nhắp phải chuột vào biểu tượng Computer chọn Manage rồi truy cập vào Event Viewer.



Hình 2.8 – Event viewer chia các vùng log riêng biệt cho các ứng dụng

3.1. Application log

Application log ghi lại sự kiện của các ứng dụng khác từ các nhà sản xuất khác như symantec hay các ứng dụng mail… Thường thiết lập trong application là mặc định của các ứng dụng nên chúng ta chỉ có thể đọc nó mà không thiết lập được.

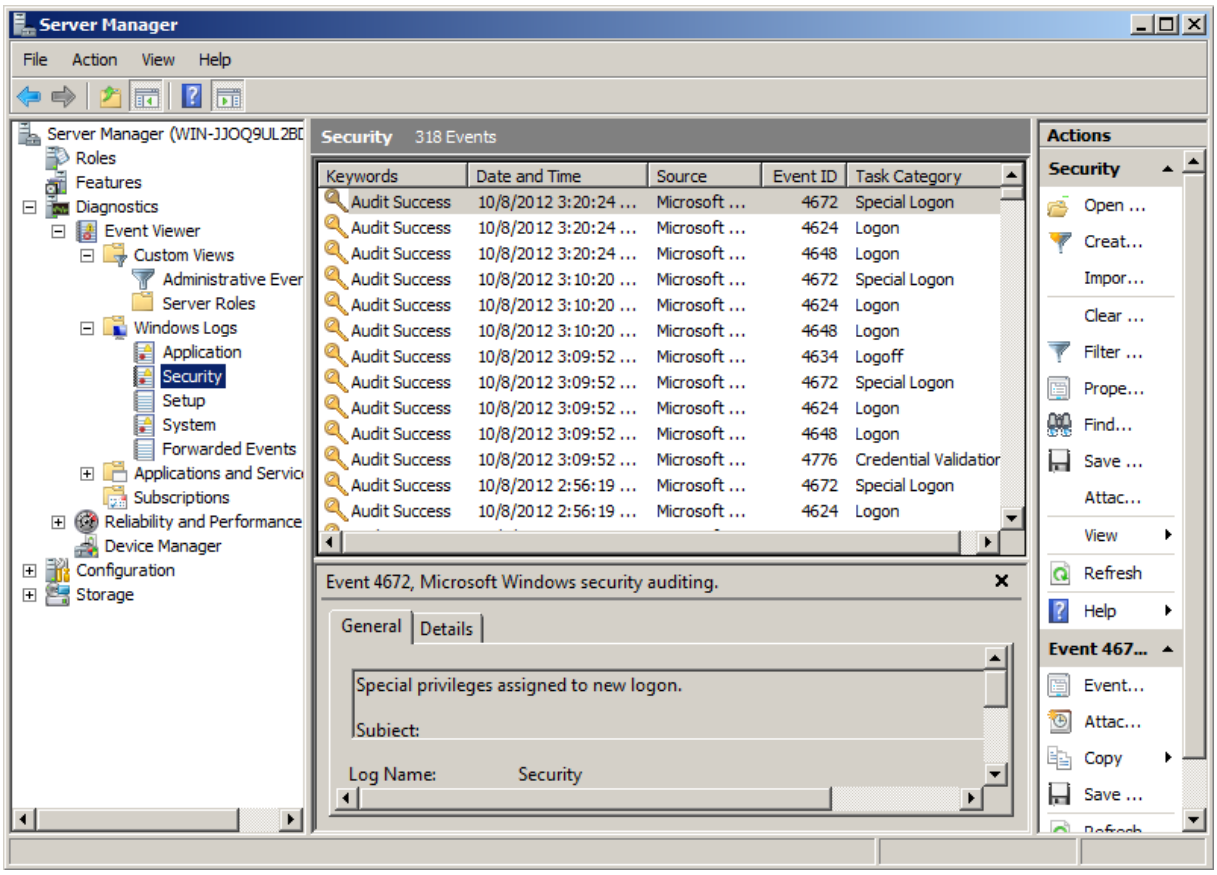


Hình 2.9 – các sự kiện được lưu lại trong application log

Trong ví dụ trên application log chỉ được phần mềm symantec sử dụng.

3.2. Security log

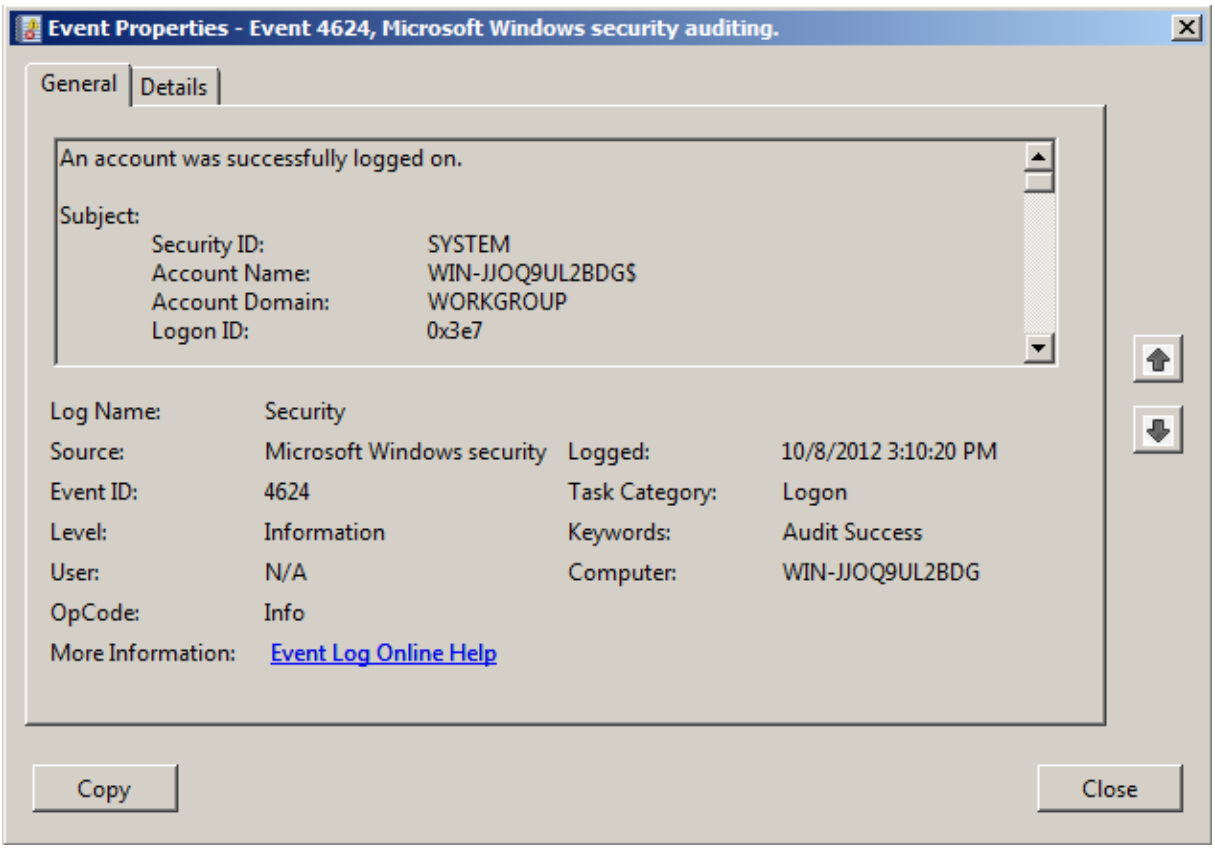
Đây là một trong những log quan trọng nhất trong hệ thống, nó ghi lại toàn bộ các thiết lập audit trong group policy. Nhưng trong các thiết lập group policy quan trọng nhất là thiết lập giám sát quá trình login vào hệ thống, truy cập dữ liệu.



Hình 2.10 – Thiết lập audit trong group policy

Trong thiết lập này chỉ thiết lập giám sát quá trình truy cập login - logoff hệ thống. Nếu với thiết lập như trên toàn bộ người dùng logon hay logoff vào hệ thống đều được ghi lại sau khi thiết lập trong group policy, chúng ta nên logoff hoặc restart lại máy bởi các thông tin chỉnh trong group policy bản chất là tùy chỉnh các thông số trong registry.

Sau khi logoff ra và login vào sẽ thấy ghi lại trong security log (hình 2.11).



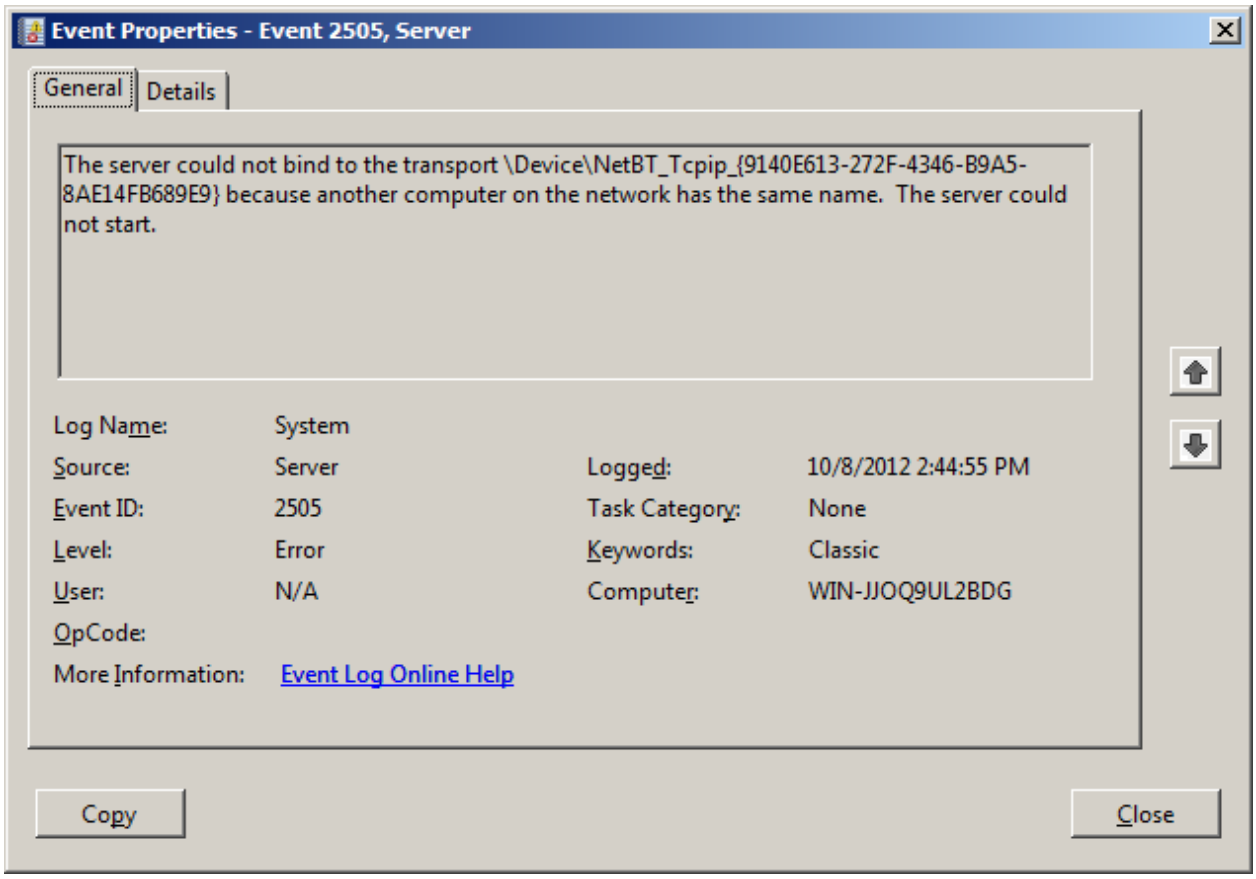
Hình 2.11 – Xem lại event logon vào hệ thống của các user

Sau khi logon vào máy tính mở event viewer ra xem, chúng ta có thể phát hiện ra hệ thống đã lưu lại username: vangtrang computer: vnexperts, event: success audit, time: 8:10:06 PM

3.3. System Log

System log được thiết lập mặc định của hệ thống giúp chúng ta xem lại các sự kiện: Bật, tắt, pause, disable, enable các services của hệ thống.

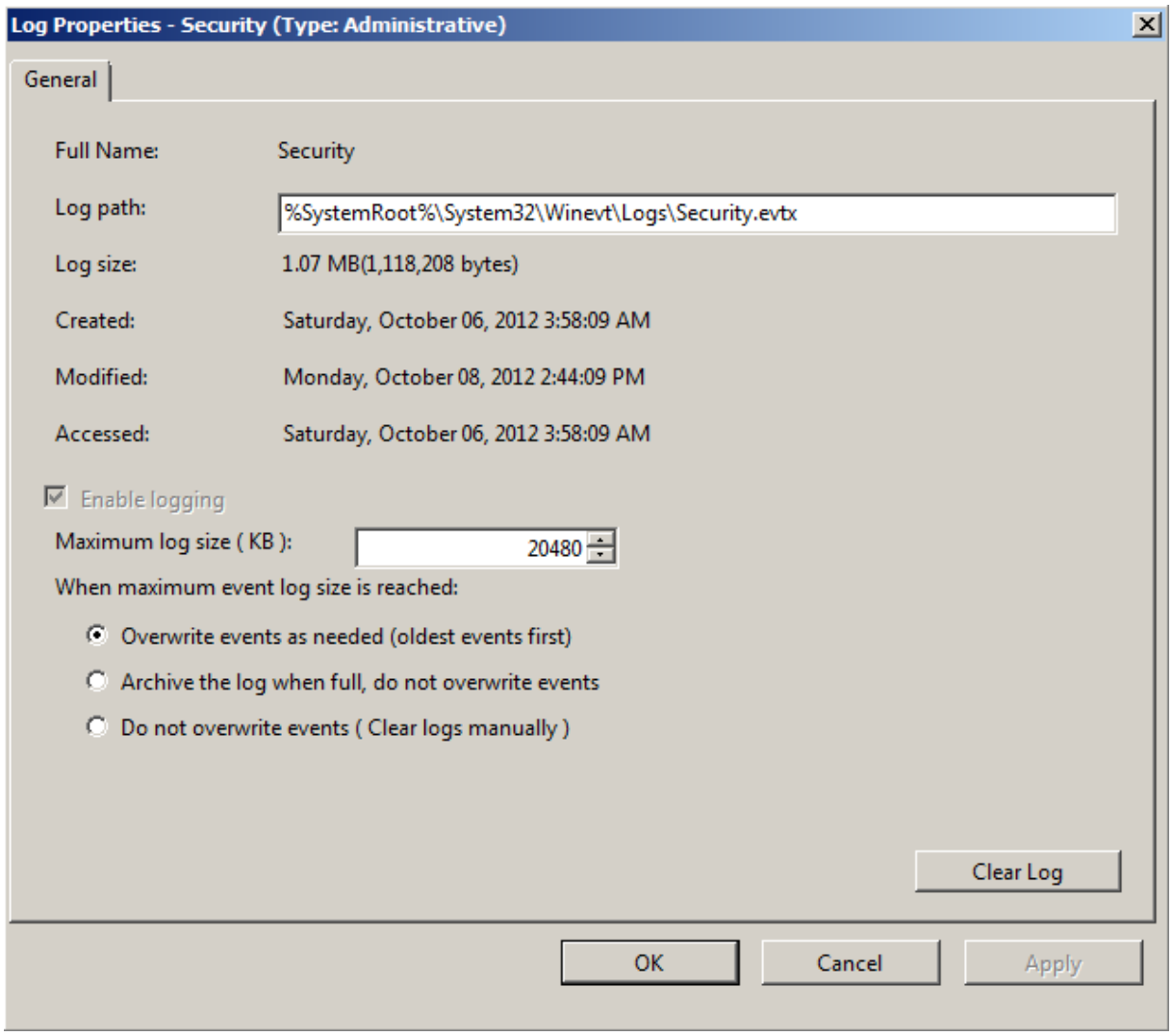
Chẳng hạn, một service bật bị lỗi trong thời điểm nào nó sẽ ghi lại trong system log của event viewer.



Hình 2.12 – Xem một event trong system log (với thông tin là Server đã bị lỗi do trong mạng LAN có máy tính trùng tên hoặc trùng địa chỉ IP)

Log Properties

Log properties giúp chúng ta cấu hình dung lượng file log, cách xoá các event cũ đi như thế nào, và những tính năng lọc các sự kiện.



Hình 2.13 – Tab General của Security Properties

Đây là thiết lập cho security properties: Với file log tên là gì và ở đâu: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Dung lượng tối đa cho file log này là 20480 KB; tuy nhiên,chúng ta có thể cấu hình lại lớn hơn hoặc nhỏ hơn, nếu dung lượng file log lớn hơn 20480 KB hệ thống sẽ tự xoá các sự kiện cũ theo thuật toán First in First out (vào trước - ra trước).

4. Sử dụng Task Manager

Mục tiêu: Windows Task Manager cho phép người dùng kiểm tra các ứng dụng, quá trình (process) và dịch vụ (service) đang chạy trên máy tính. Người dùng có thể sử dụng Task Manager để khởi chạy, dừng các chương trình và dừng quá trình; Ngoài ra Task Manager còn cung cấp các thống kê hữu ích về hiệu suất máy tính và mạng.

Để sử dụng, mở Task Manager bằng một trong các cách sau:

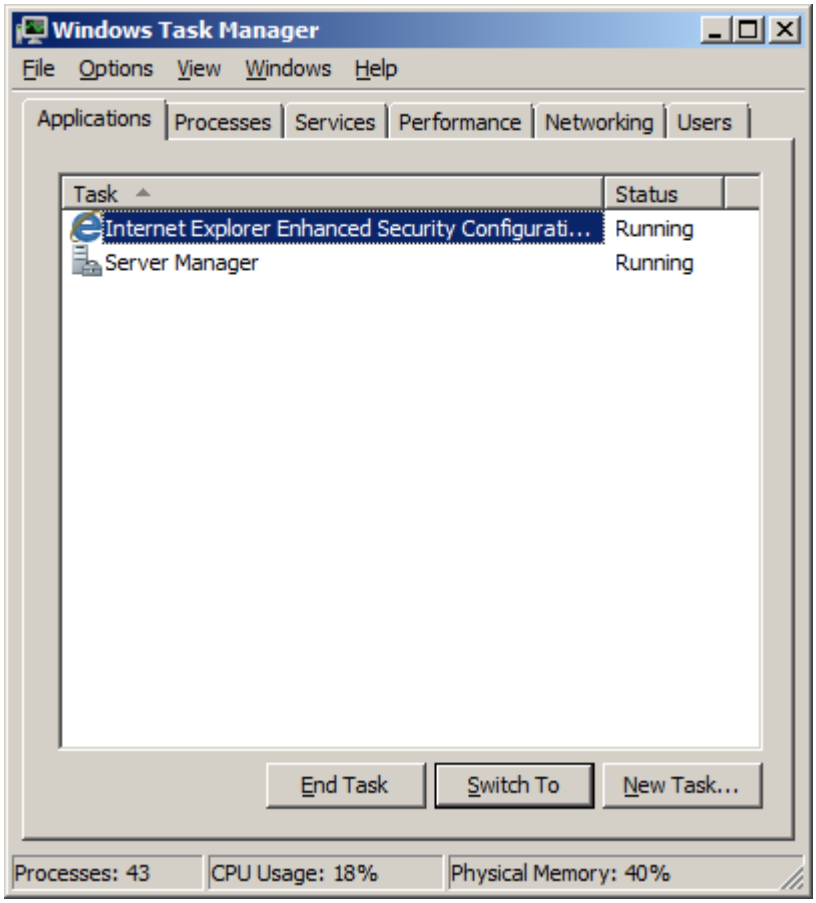
• Nhấn **Ctrl-Shift-Esc**.

• Nhắp phải vào vùng trống trong taskbar và chọn *Task Manager*.

• Nhấn **Ctrl-Alt-Delete**, sau đó nhắp *Task Manager*.

Các tab trong Task Manager sau khi được mở:

4.1. Applications



Tab Applications liệt kê danh sách các chương trình đang chạy trên máy tính. Các ứng dụng chạy trong System Tray sẽ không xuất hiện trong danh sách này. Chúng ta có thể sử dụng tab này để thoát các chương trình bị treo mà không thể thoát theo cách thông thường.

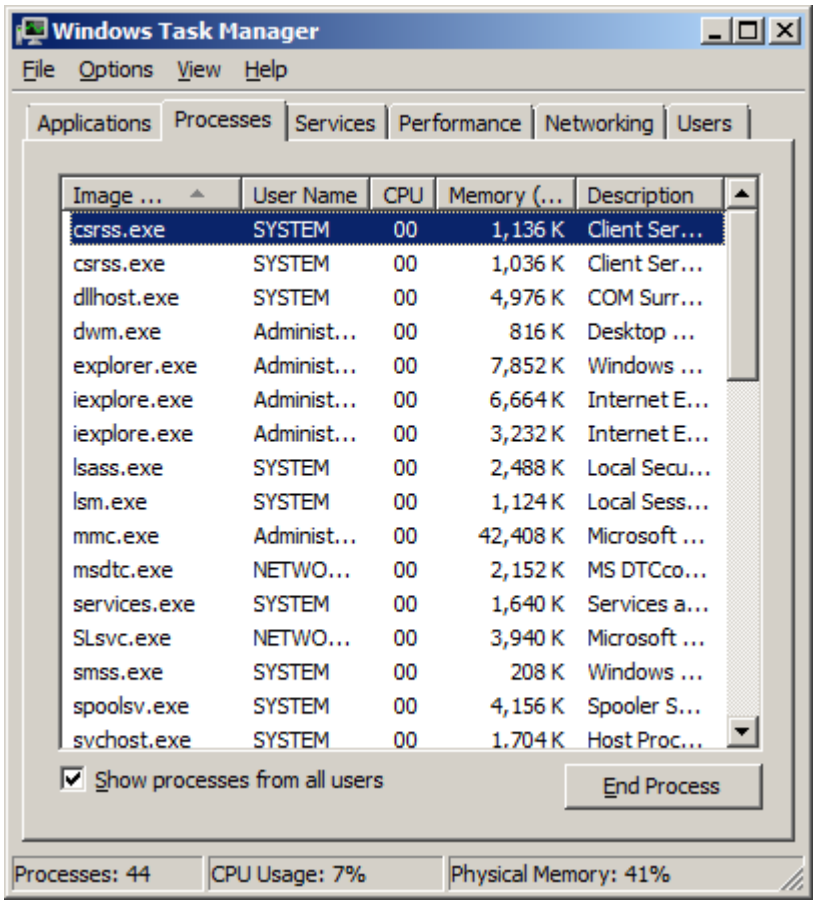
1. Nếu muốn thoát một chương trình, chọn chương trình và chọn nút *End Task*. Tính năng này rất hữu dụng khi có một chương trình nào đó đang được mở nhưng không đáp trả các lệnh đầu vào. Task Manager có thể giúp thoát các chương trình như vậy; Tuy nhiên, cách thoát này có thể làm mất những thông tin chưa được lưu.

2. Để mở một chương trình, chọn chương trình và chọn nút *Switch To*.

3. Để khởi chạy một chương trình mới, nhắp *New Task*... Sau đó đánh vào lệnh hoặc nhắp *Browse* để duyệt đến ứng dụng. Chức năng này làm việc tương tự như *Run* trong menu Start.

4.2. Processes

Tab Processes liệt kê danh sách các quá trình (process) đang chạy. Việc kết thúc một quá trình sẽ làm cho dữ liệu chưa lưu bị mất. Mặc dù vậy, việc kết thúc quá trình của ứng dụng không đáp trả là cách duy nhất để thoát khỏi chương trình đó. Cần phải hiểu mục đích của quá trình muốn kết thúc; việc kết thúc các quá trình của hệ thống có thể gây ra trục trặc cho hệ thống.



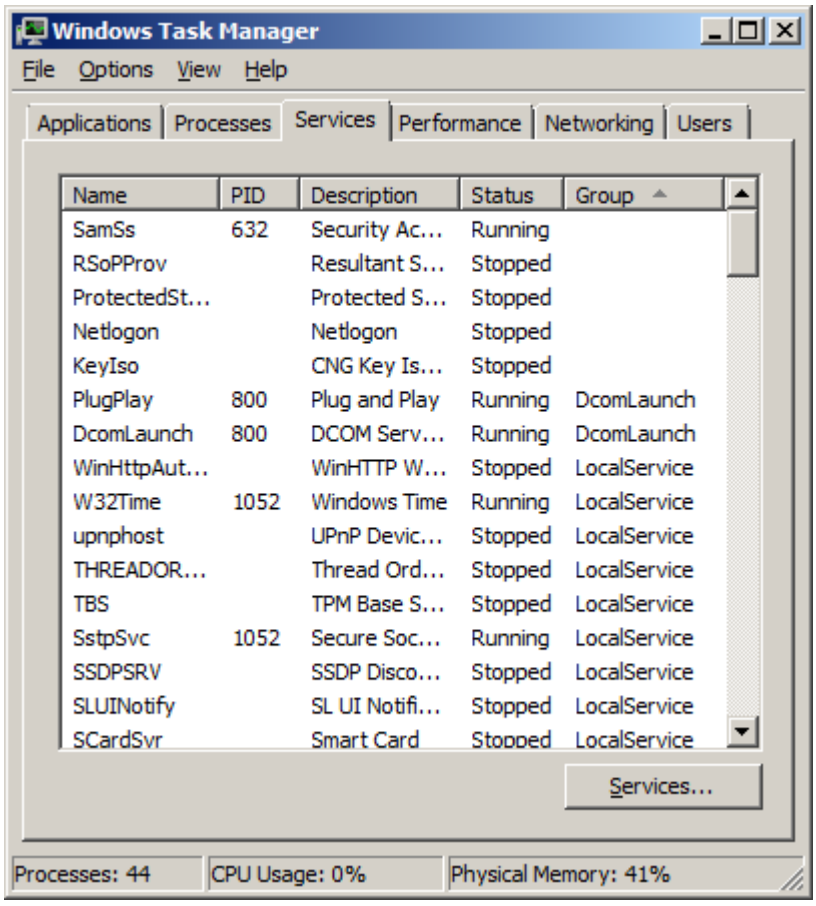
1. Để kết thúc một quá trình của một ứng dụng đang chạy, nhắp phải vào entry ứng dụng trong tab Applications và nhắp *Go To Process*. Quá trình ứng dụng sẽ được đánh dấu trong tab Processes.

2. Để kết thúc một quá trình đã được đánh dấu, nhắp *End Process*. Có thể kết thúc một ứng dụng theo cách này khi việc nhắp *End Task* trong tab Applications không có tác dụng.

3. Nhắp phải vào quá trình và sau đó nhắp *End Process Tree* để kết thúc quá trình đó cũng như các quá trình có liên quan.

4.3. Services

Services là các chương trình hỗ trợ chạy ở chế độ background. Hầu hết các chương trình này sẽ khởi chạy tự động ở thời điểm khởi động máy tính.



1. Để khởi chạy một dịch vụ, nhấp phải vào dịch vụ đã bị dừng và chọn *Start Service*.

2. Để dừng một dịch vụ, nhấp phải vào dịch vụ đang chạy và chọn *Stop Service*.

3. Để xem quá trình có liên quan với dịch vụ, nhấp phải vào dịch vụ đang chạy và chọn *Go To Process*. Thao tác này sẽ cho phép phát hiện ra dịch vụ có ngốn nhiều tài nguyên hay không.

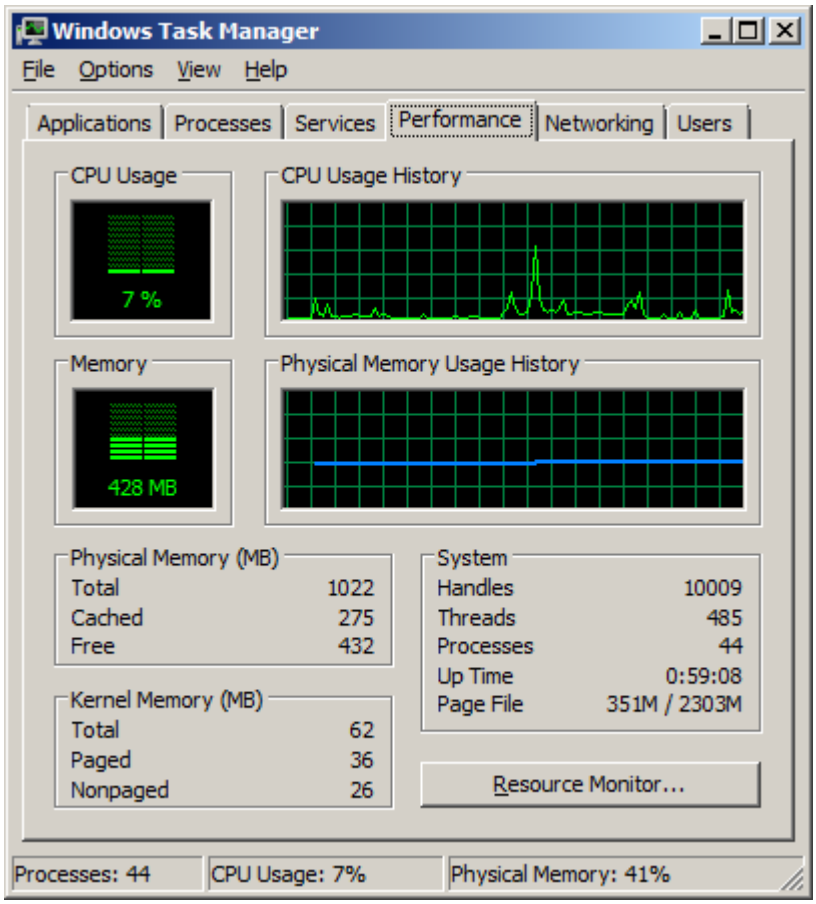
4.4. Performance

Tab này hiển thị thông tin về hiệu suất hệ thống

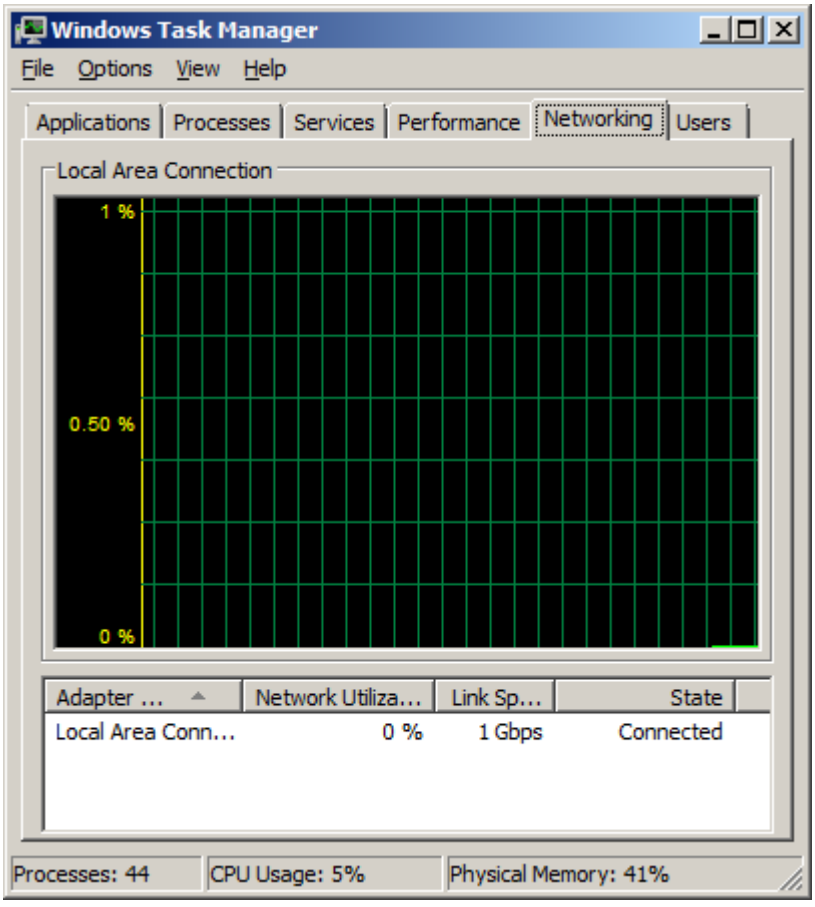
1. Trong CPU Usage hiển thị tham số hiệu suất CPU và đồ thị sử dụng CPU. CPU đa lõi sẽ có nhiều đường đồ thị hiển thị.

2. Memory hiển thị tham số hiệu suất CPU và đồ thị hiệu suất.

3. Phía dưới là các thống kê khác nhau về số *handle*, *thread* và *process* đang chạy cũng như hiệu suất sử dụng bộ nhớ.

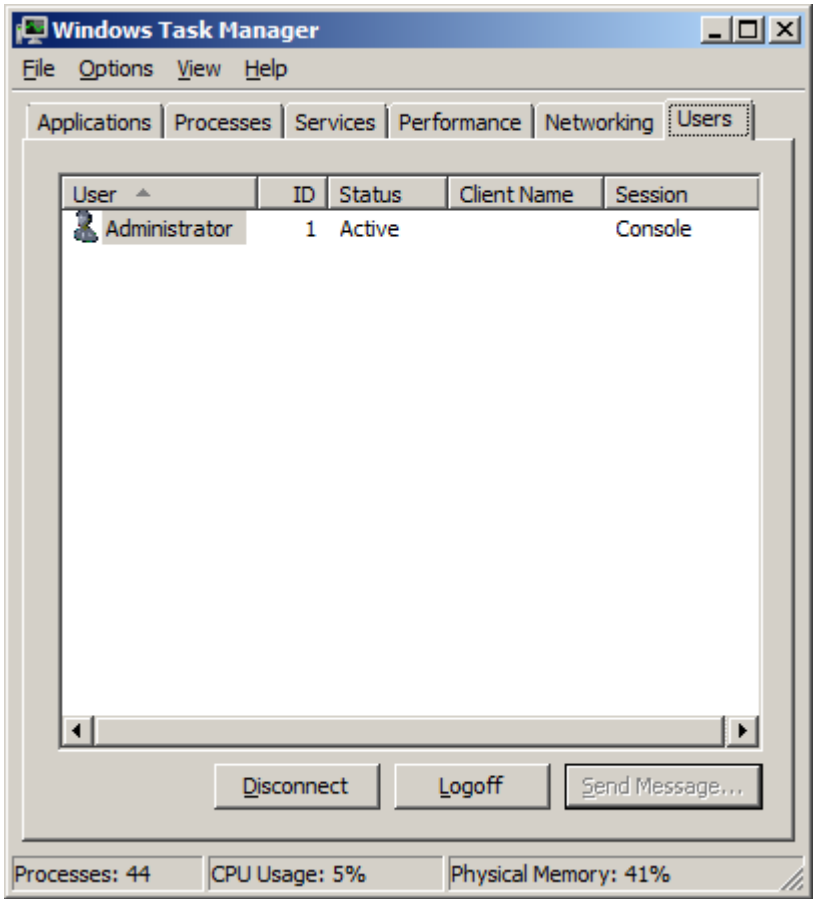


4.5. Networking



Tab Networking chứa các đồ thị dùng hiển thị hiệu suất sử dụng mạng. Bên dưới các đồ thị sẽ có những thống kê bổ sung.

4.6. Users



Trong tab Users hiển thị danh sách tất cả user có trạng thái tích cực (active) trong hệ thống.

1. Đánh dấu user và nhắp *Logoff* để kết thúc phiên làm việc của người dùng đó.

2. Đánh dấu user và nhắp *Disconnect* để kết thúc phiên làm việc của người dùng nhưng vẫn dự trữ trong bộ nhớ, sau đó người dùng có thể đăng nhập trở lại và tiếp tục công việc của họ.

Kết luận

Event Viewer là một công cụ quan trọng trong việc giám sát hệ thống. Dựa vào công cụ này người quản trị sẽ phát hiện ra các truy cập bất hợp pháp vào những thời điểm cụ thể, với tính năng lọc giúp người quản trị giới hạn những sự kiện cần thiết giám sát.

Câu hỏi

1. Trình bày chức năng các công cụ: Counter Log, Trace log, Alert log trong System Monitor.

2. Cho biết ý nghĩa của các phân vùng trong event viewer: Application, Security, System.

Bài tập thực hành

Thiết lập giám sát một folder dữ liệu: giám sát toàn bộ các quá trình truy cập các action cụ thể với folder. Trong ổ E có thư mục quan trọng (VNEDATA) việc cần thiết là đưa ra các thiết lập giám sát toàn bộ truy cập vào folder này.

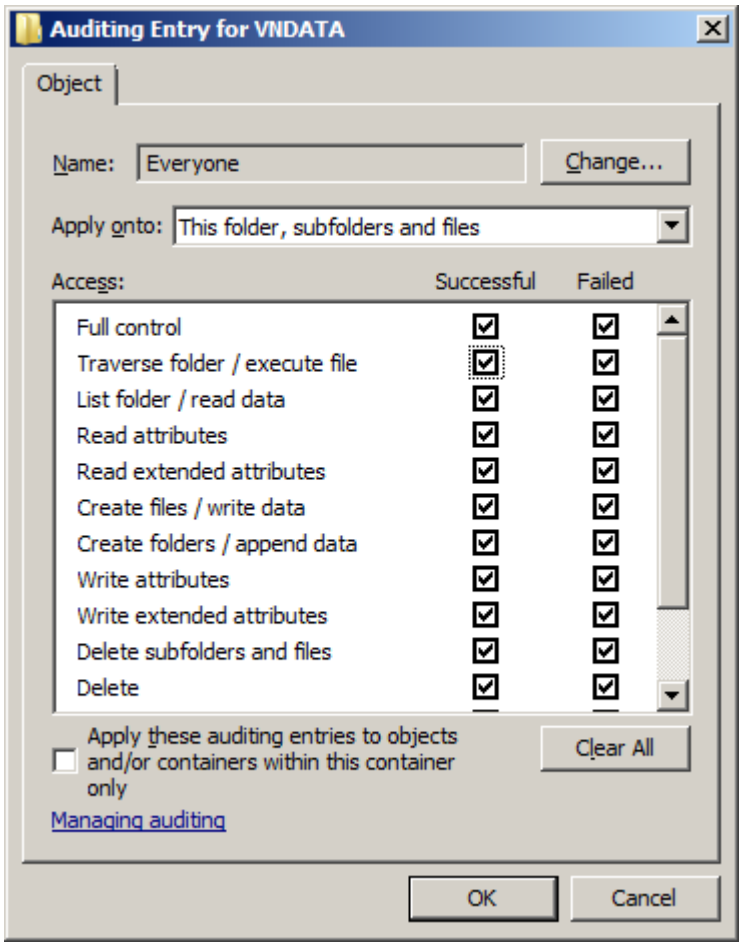
Khi cần lưu lại quá trình truy nhập trên một folder dữ liệu, cần phải thiết lập auditing trên folder đó. Các thiết lập được thực hiện như sau:

- Nhắp phải chuột lên folder cần thiết lập auditing (chẳng hạn folder VNDATA), chọn Property;

- Từ cửa sổ (VNDATA) Properties, chọn tab Security, chọn Advanced;

- Trong cửa sổ Advanced Security Settings for (VNDATA), chọn nút Edit…;

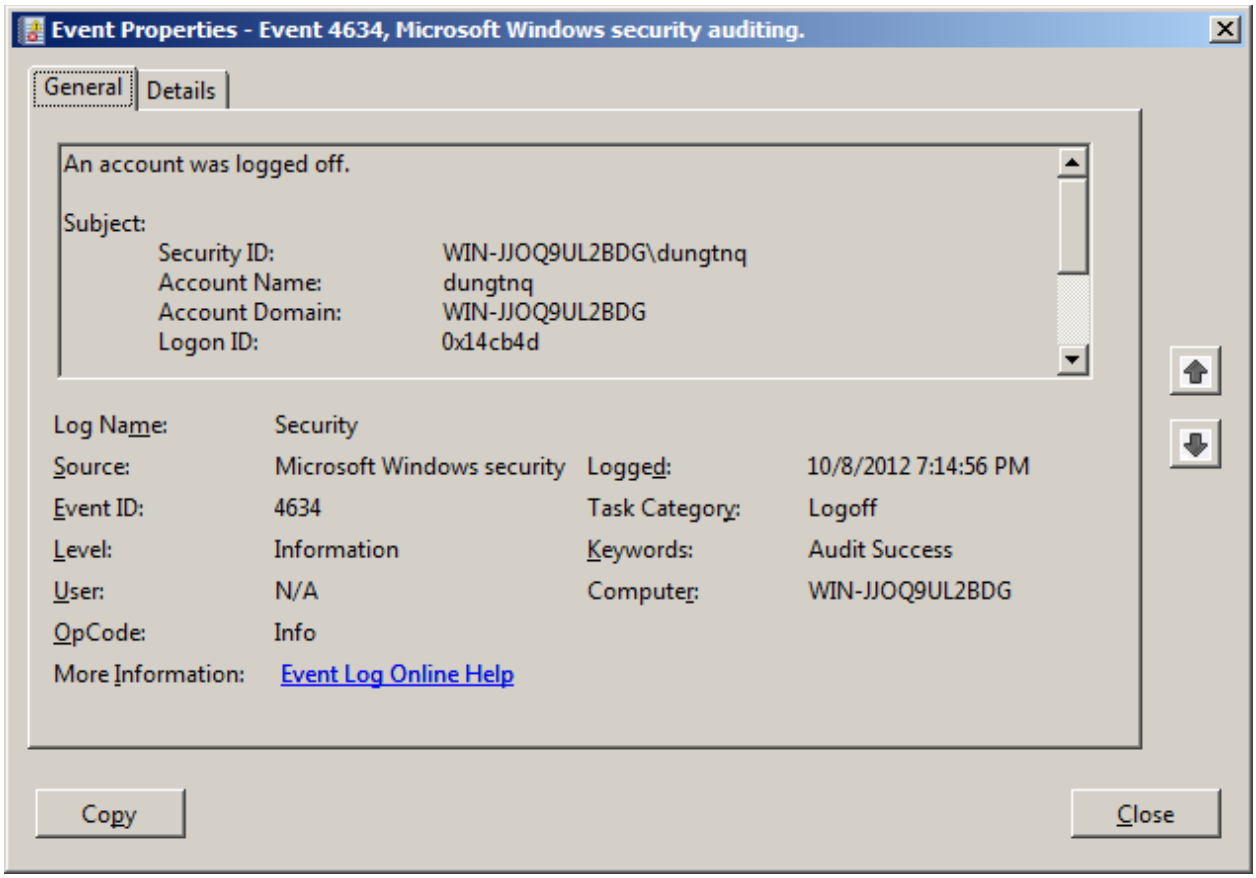
- Khi xuất hiện hộp thoại mới, chọn nút Add…



- Đánh dấu chọn các đối tượng cần thiết lập, chọn OK.

Sau khi thiết lập, restart lại máy và thử dùng một user khác để đăng nhập và truy xuất vào folder VNDATA.

Sau đó, trở lại user quản trị, nhắp đúp chuột vào sự kiện. Khi hộp thoại Event Properties xuất hiện, sẽ thấy được các thông tin liên qua đến quá trình truy nhập.



Hình 2.17 – Xem lại audit object access

Nhìn vào event ta nhận thấy vào lúc 7:14:56 PM ngày 08/10/2012, user với tên là dungtnq từ máy tính có tên WWIN-JJOQ9UL2BDG đã đăng nhập vào. Ứng dụng của tính năng audit và xem lại các event cho ta phát hiện những kẻ truy cập bất hợp pháp và quy trách nhiệm cụ thể cho những kẻ phá hoại.

BÀI 3: KHÔI PHỤC SERVER KHI BỊ HỎNG

Mã bài: MĐ 36-03

Mục tiêu của bài:

Bài học cung cấp kiến thức về các biện pháp giữ cho server an toàn, phương pháp lưu dự phòng cơ bản hay với các tùy chọn chuyên sâu; khi có sự cố người quản trị có thể khôi phục hệ thống bằng các phương án phù hợp.

1. Các biện pháp phòng ngừa

Mục tiêu: Trình bày một số biện pháp phòng ngừa đối với server tránh các rủi ro đối với hệ thống.

Để giữ cho server an toàn, cần thực hiện các yêu cầu sau:

- Duy trì nhiều bản sao đối với dữ liệu quan trọng, các server có vai trò quan trọng (chẳng hạn Domain Controller).

- Bảo vệ mạng về mặt vật lý.

- Bảo vệ dữ liệu hệ thống và dữ liệu người dùng bằng chiến lược lưu dự phòng hợp lý.

- Chuẩn bị kế hoạch khôi phục từng thời điểm.

- Tìm hiểu cách server hoạt động để có thể giải quyết trục trặc và có thể ngăn ngừa phát sinh về sau.

- Cài đặt các hotfix, patch, và service pack do nhà cung cấp phát hành.

1.1. Có dự phòng

Trên server, bảo vệ dữ liệu quan trọng bằng các volume đĩa có tính chịu lỗi, bằng phần mềm, hoặc bằng phần cứng. Để bảo vệ dữ liệu khỏi tổn hại do các hỏng hóc của server – không chỉ hỏng hóc về đĩa – có thể sao chép ra nhiều nơi trên mạng.

Nguyên tắc dự phòng cũng có thể áp dụng cho mạng; cụ thể, khi có nhiều Domain Controller có thể sẽ đơn giản quá trình khôi phục mà người quản trị sẽ tiến hành nếu một máy bị hỏng. Thay vì khôi phục cấu trúc miền từ các bản dự phòng hoặc xây dựng lại hoàn toàn, có thể để quy trình sao chép đảm trách việc khôi phục.

1.2. Bảo vệ điện năng cho server

Sử dụng UPS bất kỳ khi nào để bảo vệ điện năng cho các server và các thiết bị phần cứng của mạng. Đây là cách bảo vệ mạng khỏi các tổn hại do sự thay đổi điện áp một cách đột ngột. Bảo vệ điện năng cũng là cách bảo vệ dữ liệu khỏi sự mất mát.

1.3. Quan tâm về môi trường

Làm giảm các hỏng hóc do môi trường sinh ra bằng cách tránh xa môi trường "có vấn đề". Đảm bảo rằng, phòng chứa server phải được điều hòa không khí, tránh ánh nắng trực tiếp. Tránh xa mọi thứ có thể gây ô nhiễm, có thể gây hại cho server.

1.4. Hạn chế tiếp cận server

Những người đang sử dụng mạng, hoặc không có phận sự thì không được phép tiếp cận server. Điều đó nghĩa là, một người dùng thông thường thì không được thực hiện các thao tác sau tại server:

- Reboot hoặc tắt các server.

- Lấy đĩa cứng có chứa dữ liệu ra khỏi server khi chưa được phép.

- Cài đặt lại hệ điều hành máy.

- Hạn chế quyền truy cập vào server.

1.5. Sử dụng hiệu quả password

- Không cho mạo danh lẫn nhau để sử dụng tài khoản và mật khẩu trên tài khoản.

- Sử dụng mật khẩu có độ phức tạp cao - nếu phải crack thì cần phải có nhiều thời gian để thực hiện.

- Ngăn ngừa việc tiếp cận tài khoản của người khác.

2. Các phương pháp sao lưu dự phòng và khôi phục dữ liệu

Mục tiêu: Trình bày các phương pháp phòng chống sự mất mát dữ liệu một cách có hiệu quả bằng cách sử dụng công cụ Backup và Restore. Đây là cách thức để khắc phục các hỏng hóc của server.

Windows Server Backup cho phép tạo bản sao lưu để khôi phục lại ứng dụng và dữ liệu nhằm khôi phục lại hệ thống khi có sự cố đối với server.

Để thực hiện sao lưu, cần phải:

- Xác định vị trí để lưu trữ bản sao; bản sao phải được lưu trữ trên đĩa đính kèm hoặc thư mục được chia sẻ từ xa. Đảm bảo rằng bất kỳ đĩa cứng để lưu trữ bản sao lưu của bạn có kèm theo và trực tuyến. Đĩa nên có dung lượng lớn hơn ít nhất là 2,5 lần dung lượng cần lưu trữ. Mặc định, nếu lưu trữ bản sao trong một thư mục được chia sẻ từ xa, sao lưu sẽ được ghi đè mỗi khi tạo bản sao lưu mới. Nếu muốn lưu trữ nhiều bản sao lưu, không nên chọn tuỳ chọn này.

- Cài đặt công cụ Backup, bằng cách:

+ Mở Server Manager, nhắp phải vào Features, chọn Add Features;

+ Trong cửa sổ Add Features Wizard, đánh dấu chọn mục Windows Server Backup Features; chọn Next; chọn Install.

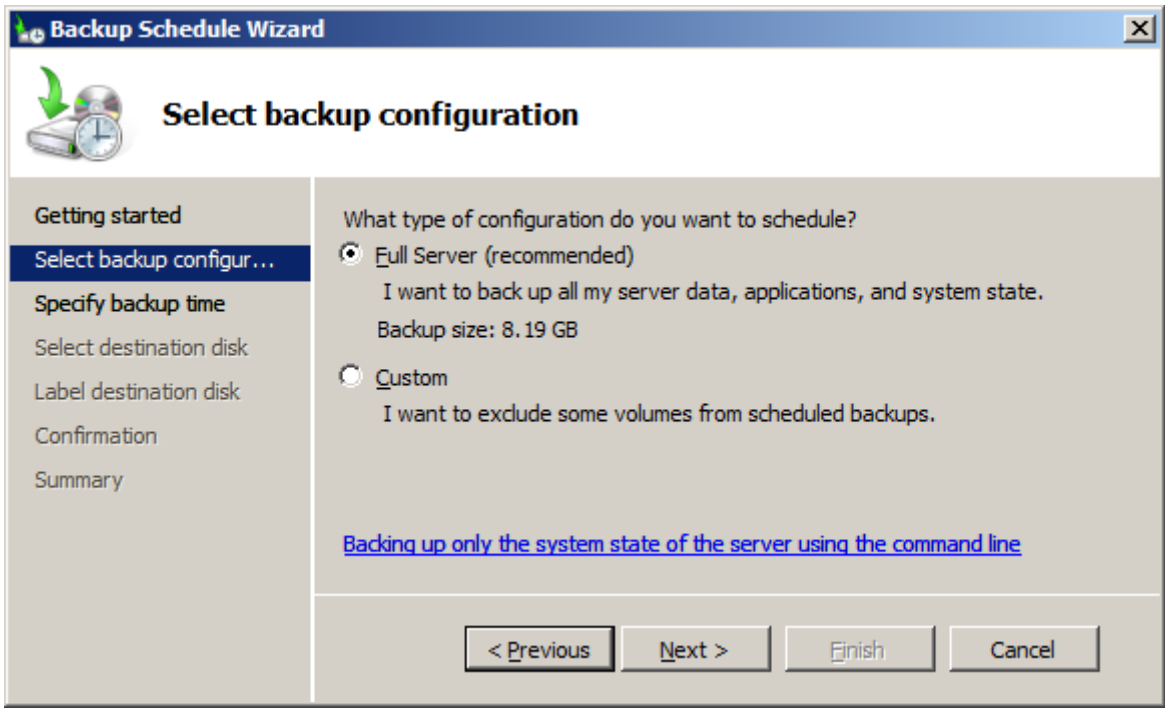
2.1. Cách lưu dự phòng

1. Mở công cụ Backup: Start -> Administrative Tools -> Windows Server Backup; hoặc từ cửa sổ Server Manager, chọn Storage, chọn Windows Server Backup

2. Tại khung Actions, chọn Backup Schedule…

3. Khi hộp thoại Backup Schedule Wizard – Getting started xuất hiện, chọn Next;

4. Trong trang Select backup configuration, chọn kiểu backup, chọn Next

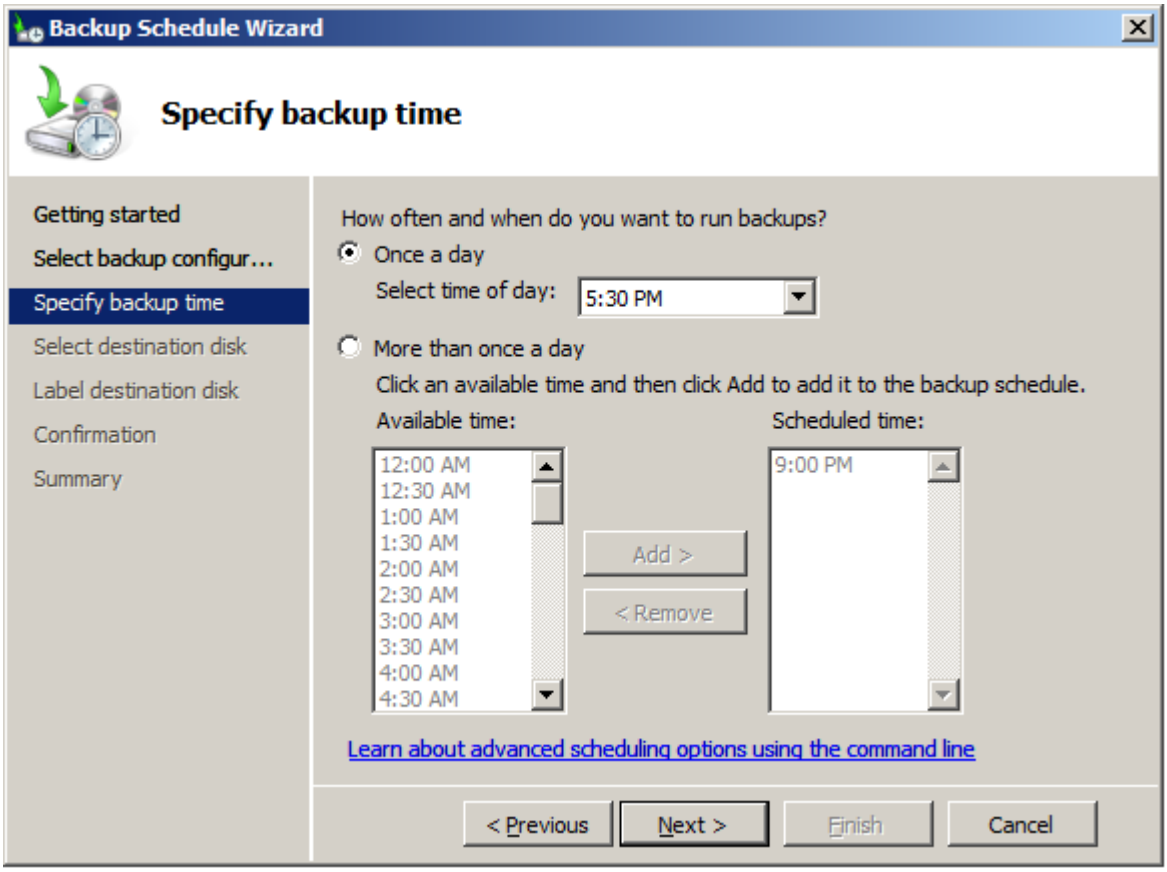


Trong đó:

+ Full server: sao lưu tất cả các volume trên server. Đây là tùy chọn được khuyến cáo nên chọn.

+ Custom: sao lưu volume được chỉ định. Khi chọn tùy chọn này, cần chỉ định: Trên trang Select Items for Backup, chọn Add Items. Trong Select Items chọn volume cần sao lưu; chọn OK.

5. Trong hộp thoại Specify Backup Time, chọn tần suất và thời điểm thực hiện backup rồi chọn Next;



6. Trên trang Specify Destination Type, chỉ định vị trí lưu trữ bản sao:

- Back up to a hard disk that is dedicated for backups: Chỉ định lưu bản sao trên một đĩa cứng dành riêng;

- Back up to a shared network folder: Chỉ định lưu bản sao trên một thư mục được chia xẻ.

7. Trên trang Confirmation, xem các thông tin chi tiết rồi chọn nút Finish để hoàn tất.

2.2. Khôi phục dữ liệu

a. Khôi phục file và Folder

Có thể sử dụng Recovery Wizard trong Windows Server Backupđể khôi phục các file và Folder từ bản sao lưu. Trước khi bạn bắt đầu, cần phải:

- Đảm bảo tồn tại ít nhất một sao lưu trên một đĩa ngoài hoặc trong Folder được chia xẻ từ xa.

- Hãy chắc chắn rằng đĩa ngoài hoặc Folder được chia xẻ từ xa đang lưu trữ bản sao lưu là trực tuyến và có sẵn cho máy chủ.

Xác định các file hoặc Folder muốn khôi phục.

Để khôi phục file hoặc Folder, sử dụng giao diện Windows Server Backup:

1. Từ **Start** menu, chọn **Administrative Tools**, chọn **Windows Server Backup**.

2. Trong khung **Actions** chọn **Recover** để mở Recovery Wizard. Trên trang **Getting Started** chọn một trong các tùy chọn **This server** hoặc **Another server** để chỉ định vị trí nguồn, sau đó chọn **Next**.

3. Trên trang **Select Backup Date** , chọn thời điểm khôi phục, rồi chọn **Next**.

4. Trên trang **Select Recovery Type** , chọn **Files and folders**, chọn **Next**.

5. Chọn thư mục với các nội dung cần khôi phục trong trang **Select Items to Recover**, chọn **Next**.

6. Trên trang **Specify Recovery Options**, chọn vị trí để chứa các đối tượng khôi phục.

7. Chọn phương thức khôi phục (tạo bản sao / Ghi đè …) rồi chọn **Next**:

8. Lựa chọn các thiết lập liên quan đến file hay Folder được khôi phục, chọn **Next**.

9. Chọn **Recover** trên trang **Confirmation** để khôi phục các đối tượng được chỉ định.

b. Khôi phục ứng dụng và dữ liệu

Có thể sử dụng Recovery Wizard trong Windows Server Backup để khôi phục ứng dụng và dữ liệu liên quan đến từ bản sao lưu.

Trước khi bắt đầu, cần chắc chắn rằng, có ít nhất một bản sao lưu của các ứng dụng tồn tại trên máy cục bộ hoặc trong một thư mục được chia sẻ từ xa, và đĩa chứa file backup là trực tuyến hoặc thư mục được chia xẻ từ xa là có sẵn.

Cách thực hiện:

1. Từ **Start** menu, chọn **Administrative Tools**, chọn **Windows Server Backup**.

2. Trong khung **Actions** chọn **Recover** để mở Recovery Wizard. Trên trang **Getting Started** chọn một trong các tùy chọn **This server** hoặc **Another server** để chỉ định vị trí nguồn, sau đó chọn **Next**.

3. Trên trang **Select Backup Date** , chọn thời điểm khôi phục, rồi chọn **Next**.

4. Trên trang **Select Recovery Type** , chọn **Applications**, chọn **Next**.

5. Lựa chọn các thiết lập liên quan đến ứng dụng cần khôi phục, chọn **Next**.

6. Trên trang **Specify Recovery Options**, chọn vị trí để chứa các đối tượng khôi phục.

7. Chọn phương thức khôi phục (tạo bản sao / Ghi đè …) rồi chọn **Next**:

8. Lựa chọn các thiết lập liên quan đến file hay Folder được khôi phục, chọn **Next**.

9. Chọn **Recover** trên trang **Confirmation** để khôi phục các đối tượng được chỉ định.

c. Khôi phục đĩa

Có thể sử dụng Recovery Wizard trong Windows Server Backup để khôi phục lại đĩa. Khi bạn khôi phục đầy đủ một đĩa, tất cả nội dung của đĩa sẽ được khôi phục

Cách thực hiện:

1. Từ **Start** menu, chọn **Administrative Tools**, chọn **Windows Server Backup**.

2. Trong khung **Actions** chọn **Recover** để mở Recovery Wizard. Trên trang **Getting Started** chọn một trong các tùy chọn **This server** hoặc **Another server** để chỉ định vị trí nguồn, sau đó chọn **Next**.

3. Trên trang **Select Backup Date** , chọn thời điểm khôi phục, rồi chọn **Next**.

4. Trên trang **Select Recovery Type** , chọn **Volumes**, chọn **Next**.

5. Lựa chọn các thiết lập liên quan đến đĩa cần khôi phục, chọn **Next**.

6. Chọn **Recover** trên trang **Confirmation** để khôi phục các đối tượng được chỉ định.

d. Khôi phục hệ điều hành và server

Có thể khôi phục Hệ thống điều hành máy chủ hoặc máy chủ bằng cách sử dụng Windows Recovery Environment và một bản sao lưu đã tạo ra trước đó với Windows Server Backup.

Có thể truy cập công cụ phục hồi và xử lý sự cố trong Windows Recovery Environment thông qua hộp thoại **System Recovery Options** trong Install Windows Wizard. Trong Windows Server 2008 R2, để khởi động công cụ này, sử dụng đĩa cài đặt Windows hoặc khởi động lại máy tính, nhấn F8, và sau đó chọn **Repair Your Computer** từ danh sách các tùy chọn khởi động.

Cách thực hiện:

1. Đặt đĩa cài đặt Windows vào khay đĩa, khởi động lại máy, chờ xuất hiện cửa sổ Install Windows Wizard

2. Trong **Install Windows**, chọn ngôn ngữ cài đặt rồi chọn **Next**.

3. Chọn **Repair your computer**.

4. Trên trang **System Recovery Options** , chọn **System Image Recovery** sẽ mở trang **Re-image your computer**.

5. Lựa chọn phương thức khôi phục rồi chọn **Next**.

6. Chọn nút **Finish** để hoàn tất.

3. Công cụ System Information

Mục tiêu: Sử dụng công cụ System Information cho phép xem các thông tin hệ thống bao gồm:

- Tóm tắt thông tin hệ thống.

- Tài nguyên về phần cứng hệ thống.

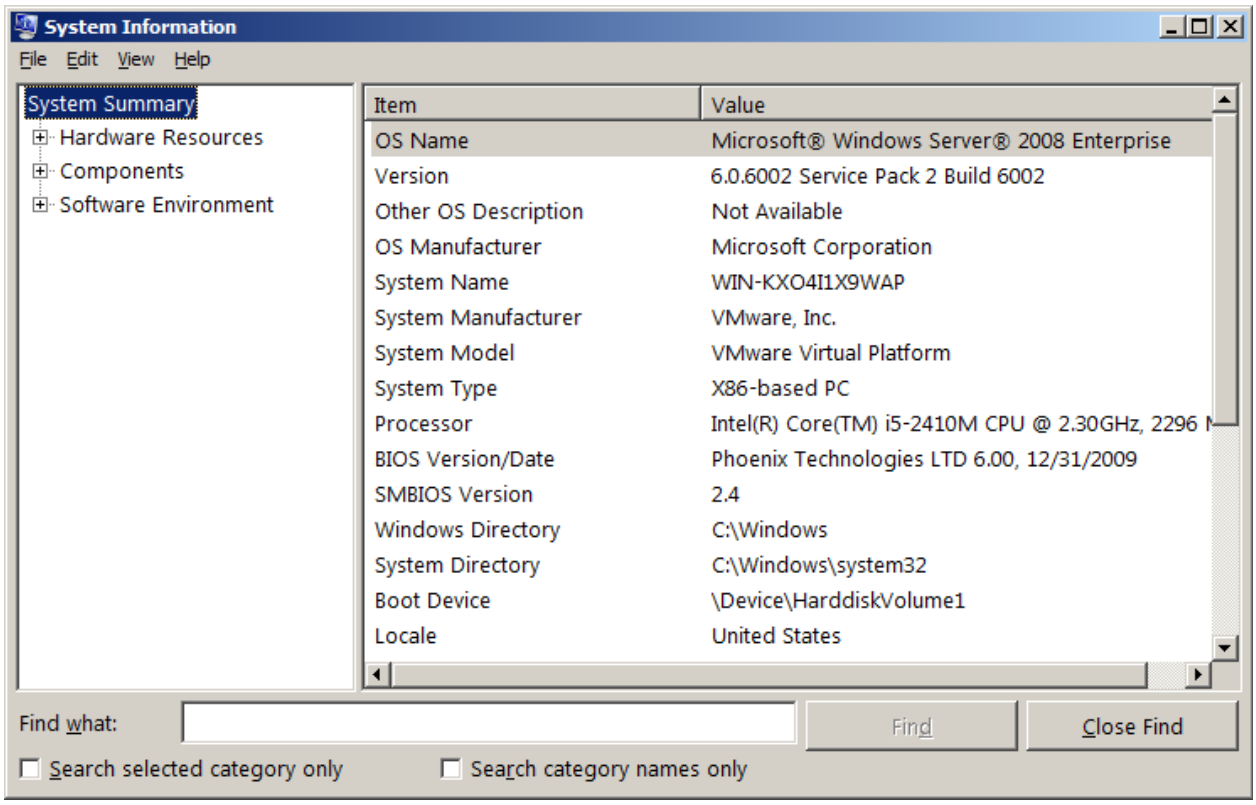
- Thông tin cấu hình dành cho phần cứng của Server đối với thiết bị đang được sử dụng.

- Phần mềm đang được thực thi trên hệ thống.

Để sử dụng System Information, mở menu Start -> Run, gõ msinfo32.exe

3.1. Trang System Summary

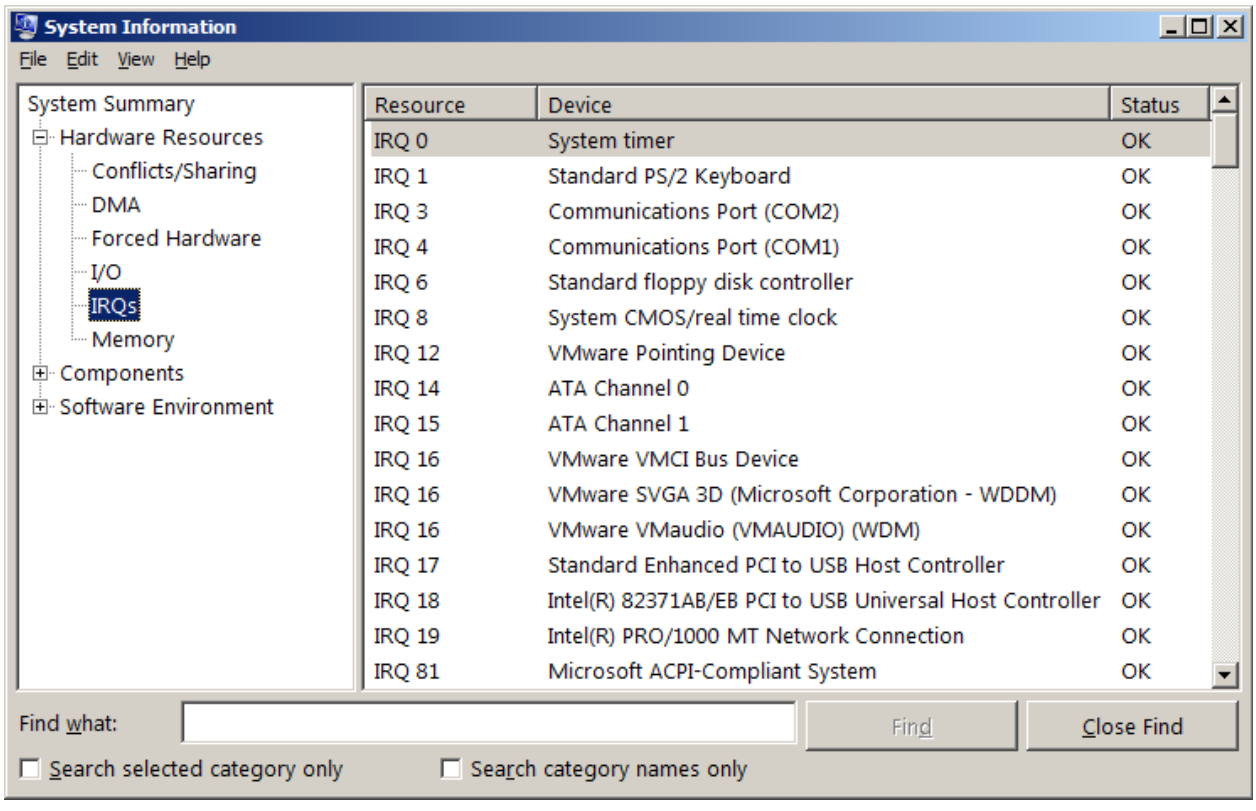
System Summary hiển thị thông tin về hệ thống một cách tóm lược.



Hình 3.15 – Thông tin từ System Summary

3.2. Folder Hardware Resources

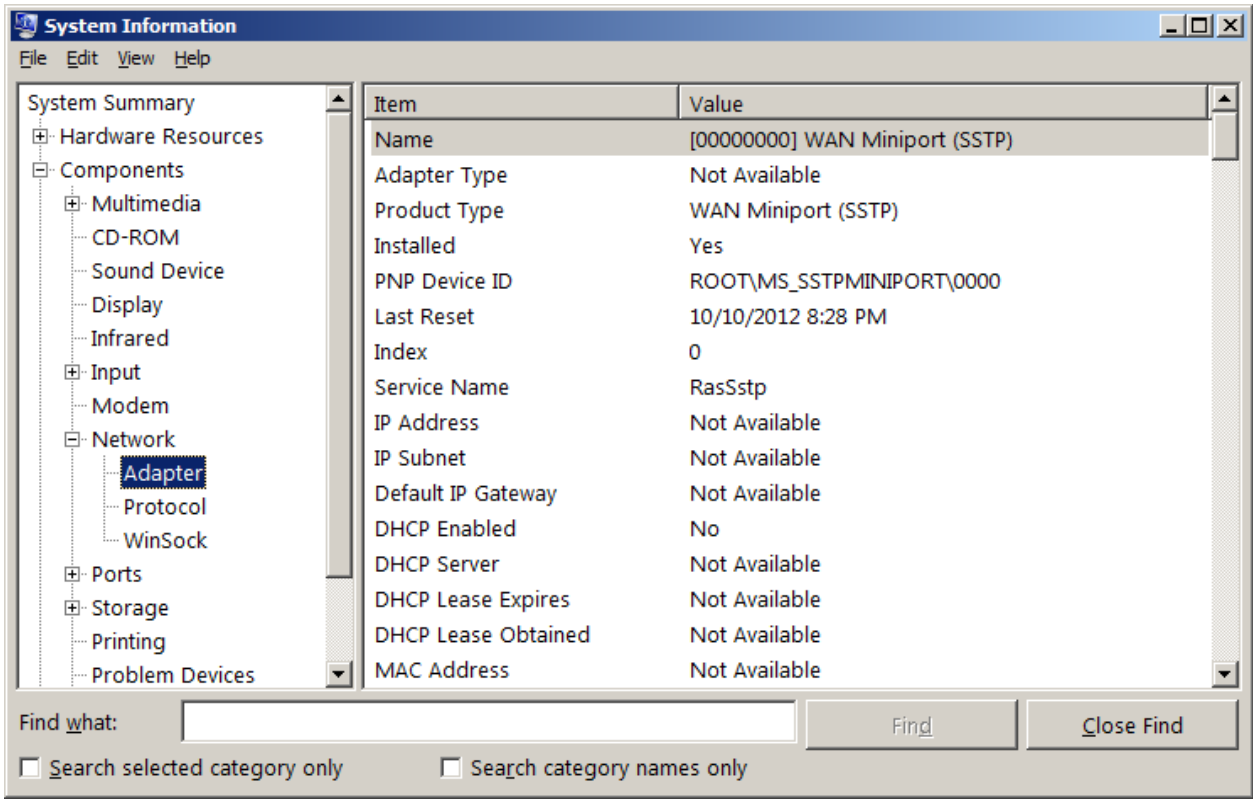
Folder Hardware Resources hiển thị thông tin về tài nguyên của hệ thống.



Hình 3.16 – Thông tin từ Folder Hardware Resources

3.3. Folder Components

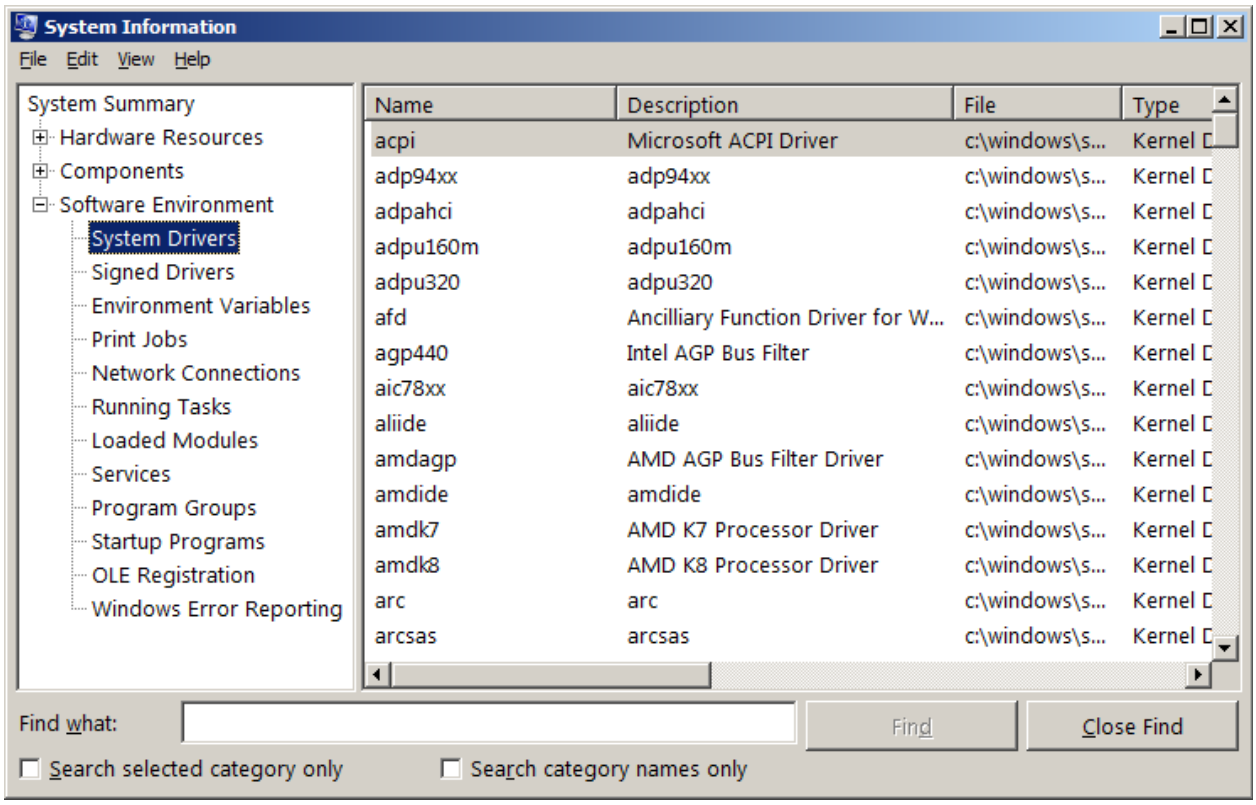
Folder Components hiển thị thông tin về tài nguyên của hệ thống cùng với các thiết bị đang được sử dụng.



Hình 3.17 – Thông tin từ Folder Components

3.4. Folder Software Environment

Folder Software Environment hiển thị thông tin về các phần mềm đang được thực thi trên hệ thống.



Hình 3.18 – Thông tin từ Folder Software Environment

Câu hỏi

1. Trình bày sơ lược các biện pháp phòng ngừa đối với Server.

2. Cho biết các phương pháp sao lưu dự phòng Server.

Bài tập thực hành

1. Lưu dự phòng dữ liệu đĩa C: gồm các thư mục: Documents and Settings, Program Files, Windows (tên file dự phòng: BACKUP, lưu vào đĩa D:\LUUTRU)

Các bước thực hiện:

- Mở công cụ Backup, chọn Back up files and settings
- Chọn đối tượng cần lưu dự phòng (các thư mục: Documents and Settings, Program Files, Windows)
- Chỉ định vị trí và tên file lưu trữ.

2. Khôi phục dữ liệu từ file dự phòng BACKUP

Các bước thực hiện:

- Mở công cụ backup, chọn Restore files and settings
- Lựa chọn đối tượng để khôi phục dữ liệu (Documents and Settings, Program Files, Windows)

3. Thực hiện lưu dự phòng và khôi phục Active Directory trên server đang quản trị.

Các bước thực hiện:

- Mở công cụ Backup, chọn Back up files and settings
- Trong cửa sổ Items to Back Up đánh dấu vào mục System State

4. Xem thông tin về hệ thống bằng công cụ System bao gồm:

- Tóm tắt thông tin hệ thống.

- Tài nguyên về phần cứng hệ thống.

- Thông tin cấu hình dành cho phần cứng của Server đối với thiết bị đang được sử dụng.

- Phần mềm đang được thực thi trên hệ thống.

BÀI 4: CÀI ĐẶT VÀ QUẢN LÝ REMOTE ACCESS SERVICES (RAS) TRONG WINDOWS SERVER

Mã bài: MĐ 36-04

Mục tiêu của bài:

Cung cấp cho học viên kiến thức về dịch vụ truy cập từ xa, cho phép máy trạm ở xa có thể quay số kết nối vào công ty thông qua đường dây điện thoại, chia xẻ Internet đơn giản…

1. Các khái niệm và các giao thức

Mục tiêu: Cung cấp cách nhìn tổng quan về dịch vụ truy cập từ xa, phương thức kết nối và các giao thức sử dụng trong truy cập từ xa.

1.1. Tổng quan về dịch vụ truy cập từ xa

Dịch vụ truy nhập từ xa (Remote Access Service) cho phép người dùng từ xa có thể truy cập từ một máy tính qua một môi trường mạng truyền dẫn (ví dụ mạng điện thoại công cộng) đến một mạng dùng riêng như thể máy tính đó được kết nối trực tiếp trong mạng đó. Người dùng từ xa kết nối tới mạng đó thô ng qua một máy chủ dịch vụ gọi là máy chủ truy cập (Access server). Khi đó người dùng từ xa có thể sử dụng tài nguyên trên trên mạng như là một máy tính kết nối trực tiếp trong mạng đó. Dịch vụ truy nhập từ xa cũng cung cấp khả năng tạo lập một kết nối WAN thông qua các mạng phương tiện truyền dẫn giá thành thấp như mạng thoại công cộng. Dịch vụ truy cập từ xa cũng là cầu nối để một máy tính hay một mạng máy tính thông qua nó được nối đến Internet theo cách được coi là hợp lý với chi phí không cao, phù hợp với các doanh nghiệp, tổ chức qui mô vừa và nhỏ. Khi lựa chọn và thiết kế giải pháp truy cập từ xa, chúng ta cần thiết phải quan tâm đến các yêu cầu sau:

– Số lượng kết nối tối đa có thể để phục vụ người dùng từ xa.

– Các nguồn tài nguyên mà người dùng từ xa muốn muốn truy cập.

– Công nghệ, phương thức và thông lượng kết nối. Ví dụ, các kết nối có thể sử dụng modem thông qua mạng điện thoại công cộng PSTN, mạng số hoá tích hợp các dịch vụ ISDN…

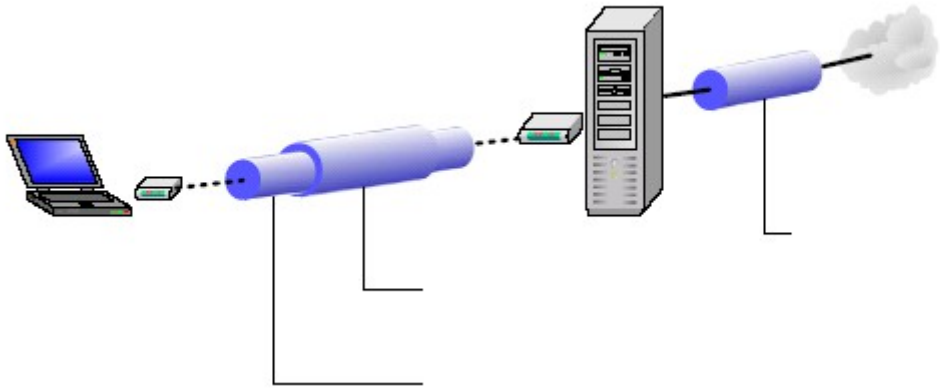
– Các phương thức an toàn cho truy cập từ xa, phương thức xác thực người dùng, phương thức mã hoá dữ liệu

– Các giao thức mạng sử dụng để kết nối.

1.2. Kết nối truy cập từ xa và các giao thức sử dụng trong truy cập từ xa

a. Kết nối truy cập từ xa

Tiến trình truy cập từ xa được mô tả như sau: người dùng từ xa khởi tạo một kết nối tới máy chủ truy cập. Kết nối này được tạo lập bằng việc sử dụng một giao thức truy cập từ xa (ví dụ giao thức PPP- Point to Point Protocol). Máy chủ truy cập xác thực người dùng và chấp nhận kết nối cho tới khi kết thúc bởi người dùng hoặc người quản trị hệ thống. Máy chủ truy cập đóng vai trò như một gateway bằng việc trao đổi dữ liệu giữa người dùng từ xa và mạng nội bộ. Bằng việc sử dụng kết nối này, người dùng từ xa gửi và nhận dữ liệu từ máy chủ truy cập. Dữ liệu được truyền trong các khuôn dạng được định nghĩa bởi các giao thức mạng (ví dụ giao thức TCP/IP) và sau đó được đóng gói bởi các giao thức truy cập từ xa. Tất cả các dịch vụ và các nguồn tài nguyên trong mạng người dùng từ xa đều có thể sử dụng thông qua kết nối truy cập từ xa này.



Hình 4.1 – Kết nối truy cập từ xa

b. Các giao thức mạng sử dụng trong truy cập từ xa

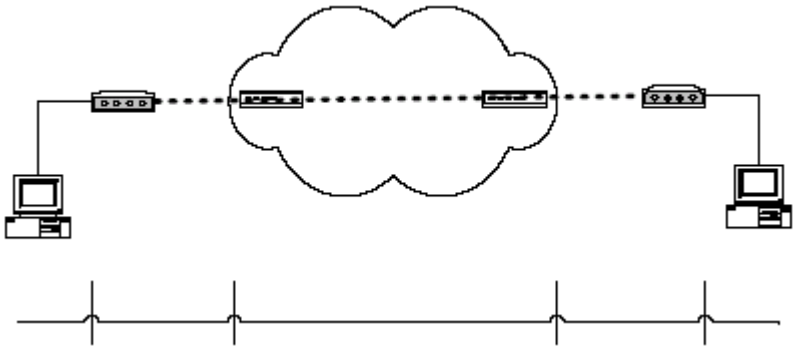
Khi triển khai dịch vụ truy cập từ xa, các giao thức mạng thường được sử dụng là giao thức TCP/IP, IPX, NETBEUI. TCP/IP là một bộ giao thức gồm có giao thức TCP và giao thức IP cùng làm việc với nhau để cung cấp phương tiện truyền thông trên mạng. TCP/IP là một bộ giao thức cơ bản, làm nền tảng cho truyền thông liên mạng là bộ giao thức mạng được sử dụng phổ biến nhất hiện nay. Với khả năng định tuyến và mở rộng, TCP/IP hỗ trợ một cách linh hoạt và phù hợp cho các tất cả các mạng. IPX (Internet Packet Exchange) là giao thức được sử dụng cho các mạng Novell NetWare. IPX là một giao thức có khả năng định tuyến và thường được sử dụng với các hệ thống mạng trước đây. NetBEUI là giao thức dùng cho mạng cục bộ LAN của Microsoft. NetBEUI cho ta nhiều tiện ích và hầu như không phải làm gì nhiều với NetBEUI. Thông qua NetBEUI ta có thể truy cập tất cả các tài

nguyên trên mạng. NETBEUI là một giao thức không có khả năng định tuyến và chỉ thích hợp với mô hình mạng nhỏ, đơn giản.

1.3. Modem và các phương thức kết nối vật lý

a. Modem

Máy tính làm việc với dữ liệu dạng số, khi truyền thông trên môi trường truyền dẫn với các dạng tín hiệu khác (ví dụ như với mạng điện thoại công cộng làm việc với các tín hiệu tương tự) ta cần một thiết bị để chuyển đổi tín hiệu số thành tín hiệu thích nghi với môi trường truyền dẫn, thiết bị đó là gọi là Modem (Modulator/demodulator). Như vậy Modem là một thiết bị chuyển đổi tín hiệu số sang dạng tín hiệu phù hợp với môi trường truyền dẫn và ngược lại. Hình 4.2 mô tả kết nối sử dụng modem qua mạng điện thoại.



Hình 4.2 – Kết nối sử dụng modem qua mạng điện thoại

Các modem sử dụng các phương pháp nén dữ liệu nhằm mục đích tăng tốc độ truyền dữ liệu. Hiệu suất nén dữ liệu phụ thuộc vào dữ liệu, có hai giao thức nén thường được sử dụng là V.42bis và MNP 5. hiệu suất nén của V.42bis và MNP 5 có thể thay đổi từ 0 đến 400 % hay cao hơn phụ thuộc vào dữ liệu tự nhiên Chuẩn modem V.90 cho phép các modem nhận dữ liệu với tốc độ 56 Kbps qua mạng điện thoại công cộng (PSTN). V.90 xem mạng PSTN như là một mạng số và chúng sẽ mã hóa dòng dữ liệu xuống theo kỹ thuật số thay vì điều chế để gửi đi như các chuẩn điều chế trước đây.

Trong khi đó theo hướng ngược lại từ khách hàng đến nhà cung cấp dịch vụ dòng dữ liệu lên vẫn được điều chế theo các nguyên tắc thông thường và tốc độ tối ta đạt được là 33.6 Kbps, giao thức hướng lên này dựa trên chuẩn V.34. Sự khác nhau giữa tín hiệu số ban đầu với tín hiệu số được phục hồi tại đầu nhận gọi là tạp âm lượng tử hóa (nhiễu lượng tử), chính tạp âm này đã hạn chế tốc độ truyền dữ liệu. Giữa các modem đầu cuối có một cấu trúc hạ tầng cho việc kết nối đó là mạng thoại công cộng. Các chuẩn modem trước đây đều giả sử cả hai đầu của kết nối giống nhau là có một kết nối tương tự vào mạng điện thoại công cộng, công

nghệ V.90 đã lợi dụng ưu điểm của tổ chức mạng mà một đầu kết nối giữa hệ thống truy cập từ xa và mạng thoại công cộng là dạng số hoàn toàn còn đầu kia vẫn được kết nối vào mạng PSTN theo dạng tương tự nhờ đó tận dụng được các ưu điểm của liên kết số tốc độ cao, vì chỉ có quá trình biến đổi A/D mới gây ra tạp âm với các kết nối số thì không có lượng tử hóa do đó nhiễu lượng tử rất ít trong cấu trúc mạng này.

b. Các phương thức kết nối vật lý cơ bản

Một phương thức phổ biến và sẽ được dùng nhiều đó là kết nối qua mạng điện thoại công cộng (PSTN). Máy tính được nối qua một modem lắp đặt bên trong (Internal modem) hoặc qua cổng truyền số liệu nối tiếp COM port. Tốc độ truyền tối đa hiện nay có thể có được bằng phương thức này có thể lên đến 56 Kbps cho chiều lấy dữ liệu xuống và 33,6Kbps cho chiều truyền dữ liệu hướng lên với các chuẩn điều chế tín hiệu phổ biến V90, K56Flex, X2. Ta cũng có thể sử dụng modem có yêu cầu về hạ tầng cơ sở thấp hơn với chuẩn điều chế V.24, V.32Bis, V.32…

Phương thức thứ hai là sử dụng mạng truyền số liệu số đa dịch vụ ISDN. Phương thức này đòi hỏi chi phí cao hơn và ngày càng được phổ biến rộng rãi. Ta có được khá nhiều các lợi ích từ việc sử dụng mạng ISDN mà một trong số đó là tốc độ. Ta có thể sử dụng các lựa chọn ISDN 2B+D BRI (2x64Kbps dữ liệu + 16Kbps dùng cho điều khiển) hoặc 23B+D PRI (23x64Kbps + 64Kbps) thông qua thiết bị TA (Terminal Adapter) hay các card ISDN. Một phương thức khác nhưng ít được sử dụng là qua mạng truyền số liệu X.25, tốc độ không cao nhưng an toàn và bảo mật cao hơn. Yêu cầu cho người sử dụng trong trường hợp này là phải có sử dụng card truyền số liệu X.25 hoặc một thiết bị được gọi là PAD (Packet Asssembled Disassembled). Ta cũng có thể sử dụng các kết nối trực tiếp qua cáp modem, phương thức này cho ta các kết nối tốc độ cao nhưng phải thông qua các modem truyền số liệu có giá thành cao.

2. An toàn trong truy cập từ xa

Mục tiêu: An toàn trong truy cập từ xa phụ thuộc vào quá trình nhận thực và xác thực khi có yêu cầu kết nối; Bên cạnh đó, việc mã hóa dữ liệu với các phương thức sẽ cung cấp cơ chế an toàn trong truy cập từ xa.

2.1. Các phương thức xác thực kết nối

a. Quá trình nhận thực

Tiến trình nhận thực với các giao thức xác thực được thực hiện khi người dùng từ xa có các yêu cầu xác thực tới máy chủ truy cập, một thỏa thuận giữa

người dùng từ xa và máy chủ truy cập để xác định phương thức xác thực sẽ sử dụng. Nếu không có phương thức nhận thực nào được sử dụng, tiến trình PPP sẽ khởi tạo kết nối giữa hai điểm ngay lập tức. Phương thức xác thực có thể được sử dụng với các hình thức kiểm tra cơ sở dữ liệu địa phương (lưu trữ các thông tin về username và password ngay trên máy chủ truy cập) xem các thông tin về username và password được gửi đến có trùng với trong cơ sở dữ liệu hay không. Hoặc là gửi các yêu cầu xác thực tới một server khác để xác thực thường sử dụng là các RADIUS server (sẽ được trình bày ở phần sau)

Sau khi kiểm tra các thông tin gửi trả lại từ cơ sở dữ liệu địa phương hoặc từ RADIUS server. Nếu hợp lệ, tiến trình PPP sẽ khởi tạo một kết nối, nếu không yêu cầu kết nối của người dùng sẽ bị từ chối.

b.Giao thức xác thực PAP

PAP là một phương thức xác thực kết nối không an toàn, nếu sử dụng một chương trình phân tích gói tin trên đường kết nối ta có thể nhìn thấy các thông tin về username và password dưới dạng đọc được. Điều này có nghĩa là các thông tin gửi đi từ người dùng từ xa tới máy chủ truy cập không được mã hóa mà được gửi đi dưới dạng đọc được đó chính là lý do PAP không an toàn. Hình dưới mô tả quá trình xác thực PAP, sau khi thỏa thuận giao thức xác thực PAP trên liên kết PPP giữa các đầu cuối, người dùng từ xa gửi thông tin (username:nntrong, password:ras123) tới máy chủ truy cập từ xa, sau khi kiểm tra các thông tin này trong cơ sở dữ liệu của mình, máy chủ truy cập từ ra sẽ quyết định xem liệu yêu cầu kết nối có được thực hiện hay không.

c.Giao thức xác thực CHAP

Sau khi thỏa thuận giao thức xác thực CHAP trên liên kết PPP giữa các đầu cuối, máy chủ truy cập gửi một "challenge" tới người dùng từ xa. Người dùng từ xa phúc đáp lại một giá trị được tính toán sử dụng tiến trình xử lý một chiều (hash). máy chủ truy cập kiểm tra và so sánh thông tin phúc đáp với giá trị hash mà tự nó tính được. Nếu các giá trị này bằng nhau việc xác thực là thành công, ngược lại kết nối sẽ bị hủy bỏ. Như vậy CHAP cung cấp cơ chế an toàn thông qua việc sử dụng giá trị challenge thay đổi, duy nhất và không thể đoán được. Các thông tin về username và password không được gửi đi dưới dạng đọc được trên mạng và do đó chống lại các truy cập trái phép bằng hình thức lấy trộm password trên đường kết nối.

d.Giao thức xác thực mở rộng EAP

Ngoài các giao thức kiểm tra tính xác thực cơ bản PAP, CHAP, trong Microsoft Windows hỗ trợ thêm một số giao thức nhằm nâng cao độ an toàn, bảo

mật và đa truy nhập, đó là giao thức xác thực mở rộng EAP (Extensible Authentication Protocol). EAP cho phép có được một cơ cấu xác thực tuỳ ý để công nhận một kết nối gọi vào. Người sử dụng và máy chủ truy nhập từ xa sẽ trao đổi để tìm ra giao thức chính xác được sử dụng.

EAP hỗ trợ các hình thức sau:

– Sử dụng các card vật lý dùng để cung cấp mật khẩu. Các card này dùng một số các phương thức xác thực khác nhau như sử dụng các đoạn mã thay đổi theo mỗi lượt sử dụng.

– Hỗ trợ MD5-CHAP, giao thức mã hoá tên người sử dụng, mật khẩu sử dụng thuật toán mã hoá MD5 (Message Digest 5).

– Hỗ trợ sử dụng cho các thẻ thông minh. Thẻ thông minh bao gồm thẻ và thiết bị đọc thẻ. Các thông tin xác thực về cá nhân người dùng được ghi lại trong các thẻ này.

– Các nhà phát triển phần mềm độc lập sử dụng giao diện chương trình ứng dụng EAP có thể phát triển các module chương trình cho các công nghệ áp dụng cho thẻ nhận dạng, thẻ thông minh, các phần cứng sinh học như nhận dạng võng mạc, các hệ thống sử dụng mật khẩu một lần.

2.2. Các phương thức mã hóa dữ liệu

Dịch vụ truy cập từ xa cung cấp cơ chế an toàn bằng việc mã hóa và giải mã dữ liệu truyền giữa người dùng truy cập từ xa và máy chủ truy cập. Có hai phương thức mã hóa dữ liệu thường được sử dụng đó là mã hóa đối xứng và mã hóa phi đối xứng.

Phương thức mã hoá đối xứng: thông tin ở dạng đọc được, được mã hoá sử dụng khóa bí mật (khoá mà chỉ có người mã hoá mới biết được) tạo thành thông tin đã được mã hoá. ở phía nhận, thông tin mã hoá được giải mã cùng với khóa bí mật thành dạng gốc ban đầu. Điểm chú ý của phương pháp mã hoá này là việc sử dụng khoá bí mật cho cả quá trình mã hoá và quá trình giải mã. Do đó, nhược điểm chính của phương thức này là cần có quá trình trao đổi khoá bí mật, dẫn đến tình trạng dễ bị lộ khoá bí mật.

Phương pháp mã hoá phi đối xứng, để khắc phục điể m hạn chế của phương pháp mã hoá đối xứng là quá trình trao đổi khoá bí mật, người ta đã sử dụng phương pháp mã hoá phi đối xứng sử dụng một cặp khoá tương ứng với nhau gọi là phương thức mã hoá phi đối xứng dùng khoá công khai. Phương thức mã hóa này sử dụng hai khóa là khóa công khai và khóa bí mật có các quan hệ toán học với nhau.

Trong đó khóa bí mật được giữ bí mật và không có khả năng bị lộ do không cần phải trao đổi trên mạng. Khóa công khai không phải giữ bí mật và mọi người đều có thể nhận được khoá này. Do phương thức mã hóa này sử dụng 2 khóa khác nhau, nên người ta gọi nó là phương thức mã hóa phi đối xứng. Mặc dù khóa bí mật được giữ bí mật, nhưng không giống với "secret Key" được sử dụng trong phương thức mã hóa đối xứng sử dụng khoá bí mật do khóa bí mật không được trao đổi trên mạng. Khóa công khai và khóa bí mật tương ứng của nó có quan hệ toán học với nhau và được sinh ra sau khi thực hiện các hàm toàn học; nhưng các hàm toán học này luôn thỏa mãn điều kiện là sao cho không thể tìm được khóa bí mật từ khóa công cộng và ngược lại.

Do có mối quan hệ toán học với nhau, thông tin được mã hóa bằng khóa công khai chỉ có thể giải mã được bằng khóa bí mật tương ứng. Giao thức thường được sử dụng để mã hóa dữ liệu hiện nay là giao thức IPsec. Hầu hết các máy chủ truy cập dựa trên phần cứng hay mềm hiện nay đều hỗ trợ IPSec. IPSec là một giao thức bao gồm các chuẩn mở bảo đảm các vấn đề bảo mật, an toàn và toàn vẹn dữ liệu cho các kết nối qua mạng sử dụng giao thức IP bằng các biện pháp mã hoá. IPSec bảo vệ chống lại các hành động phá hoại từ bên ngoài. Các client khởi tạo một mối liên quan bảo mật hoạt động tương tự như khoá công khai để mã hoá dữ liệu. Ta có thể sử dụng các chính sách áp dụng cho IPSec để cấu hình nó. Các chính sách cung cấp nhiều mức độ và khả năng để bảo đảm an toàn cho từng loại dữ liệu. Các chính sách cho IPSec sẽ được thiết lập cho phù hợp với từng người dùng, từng nhóm người dùng, cho một ứng dụng, một nhóm miền hay toàn bộ hệ thống mạng.

3. Triển khai dịch vụ truy cập từ xa

Mục tiêu: Trình bày các phương thức kết nối, các điều kiện và các thiết đặt cho phép người quản trị gán các quyền truy cập và mức độ sử dụng các nguồn tài nguyên trên mạng đối với người dùng từ xa.Việc kết nối sử dụng dịch vụ truy cập từ xa với Mạng riêng ảo (VPN) là giải pháp cho phép người dùng thực hiện một kết nối tới trụ sở chính bằng việc sử dụng hạ tầng mạng là một mạng công cộng như Internet.

3.1. Kết nối gọi vào và kết nối gọi ra

Cấu hình máy chủ truy cập để tạo lập các kết nối gọi vào cho phép người dùng từ xa truy cập vào mạng. Các thông số cơ bản thường được cấu hình khi tạo lập các kết nối gọi vào bao gồm xác định các phương thức xác thực người dùng, mã hóa hay không mã hóa dữ liệu, các phương thức mã hóa dữ liệu nếu yêu cầu, các giao thức mạng sẽ được sử dụng cho truy nhập từ xa, các thiết đặt về chính sách và

các quyền truy nhập của người dùng từ xa, mức độ được phép truy nhập như thế nào, xác định phương thức cấp phát địa chỉ IP cho máy truy nhập từ xa, các yêu cầu cấu hình để tạo lập các kết nối VPN… Kết nối gọi ra có thể được thiết lập để gọi ra tới một mạng dùng riêng hoặc tới một ISP.

Windows server hỗ trợ các hình thức kết nối sau:

- Nối tới mạng dùng riêng, ta sẽ phải cung cấp số điện thoại nơi sẽ nối đến. Có thể là số điện thoại của ISP, của mạng dùng riêng hay của máy tính phía xa. Xác định quyền sử dụng kết nối này.

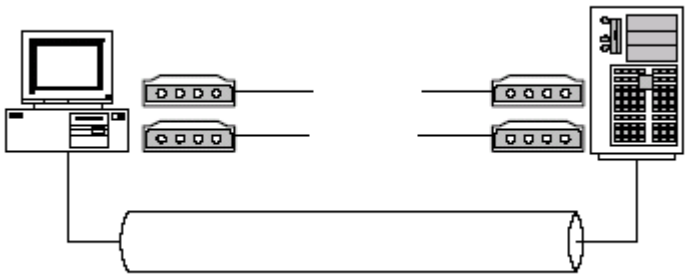
- Nối tới Internet, hai lựa chọn có thể là sử dụng truy cập qua đường thoại và sử dụng truy cập qua mạng LAN. Sử dụng đường thoại, các vấn đề ta cần quan tâm là số điện thoại truy nhập, tên và mật khẩu được cung cấp bởi ISP. Sử dụng LAN, ta sẽ phải quan tâm đến proxy server và một số thiết đặt khác.

- Tạo lập kết nối VPN, VPN là một mạng sử dụng các kết nối dùng giao thức tạo đường hầm (PPTP, L2TP, IPSEC,…) để tạo được các kết nối an toàn, bảo đảm thông tin không bị xâm phạm khi truyền tải qua các mạng công cộng. Tương tự như khi tạo lập một kết nối gọi ra, Nếu cần thiết phải thông qua một ISP trung gian trước khi nối tới mạng dùng riêng, lựa chọn một kết nối gọi ra. Cung cấp địa chỉ máy chủ, địa chỉ mạng nơi mà ta đang muốn nối tới. Các thiết lập khác là thiết đặt các quyền sử dụng kết nối.

- Tạo lập kết nối trực tiếp với máy tính khác, lựa chọn này được sử dụng để kết nối trực tiếp hai máy tính với nhau thông qua một cáp được thiết kế cho nối trực tiếp hai máy tính. Một trong hai máy tính được lựa chọn là chủ và máy tính kia được lựa chọn là tớ. Lựa chọn thiết bị cổng nơi hai máy tính nối với nhau.

3.2. Kết nối sử dụng đa luồng (Multilink)

Multilink là sự kết hợp nhiều liên kết vật lý trong một liên kết logic duy nhất nhằm gia tăng băng thông cho kết nối. Multilink cho phép sử dụng hai hoặc nhiều hơn các cổng truyền thông như là một cổng duy nhất có tốc độ cao. Điều này có nghĩa là ta có thể sử dụng hai modem để kết nối Internet với tốc độ cao gấp đôi so với việc sử dụng một modem. Multilink gia tăng băng thông và giảm độ trễ giữa các hệ thống bằng cơ chế chia các gói dữ liệu và gửi đi trên các mạch song song. Multilink sử dụng giao thức MPPP cho việc quản lý các kết nối của mình. Để sử dụng, MPPP cần phải được hỗ trợ ở cả hai phía của kết nối.



Hình 4.3 – Kết nối sử dụng đa luồng

Hình 4.3 mô tả kết nối sử dụng Multilink, khi người dùng từ xa sử dụng hai modem và hai đường thoại kết nối với máy chủ truy cập, mỗi kết nối là việc theo chuẩn V.90 có tốc độ 56 kbps sử dụng kỹ thuật Multilink cho phép đạt tốc độ 112 Kbps giữa máy truy cập từ xa và máy chủ truy cập.

3.3. Các chính sách thiết lập cho dịch vụ truy nhập từ xa

Chính sách truy nhập từ xa là tập hợp các điều kiện và các thiết đặt cho phép người quản trị mạng gán cho mỗi người dùng từ xa các quyền truy cập và mức độ sử dụng các nguồn tài nguyên trên mạng. Ta có thể dùng các chính sách để có được nhiều các lựa chọn phù hợp với từng mức độ người dùng, tăng tính mềm dẻo, tính năng động khi cấp quyền truy nhập cho người dùng.

Một chính sách truy nhập từ xa thông thường bao gồm ba thành phần nhằm cung cấp các truy nhập an toàn có kiểm soát đến máy chủ truy cập. Các điều kiện (Conditions): là một danh sách các tham số như ngày tháng, nhóm người dùng, mã người gọi, địa chỉ IP phù hợp với máy trạm đang nối đến máy chủ truy cập. Bộ chính sách điều kiện đầu tiên này tương ứng với các thông số của yêu cầu kết nối gọi đến được xử lý đối với sự cho phép truy cập và cấu hình.

Sự cho phép (Permission): Các kết nối truy nhập từ xa được cho phép và gán trực tiếp tới mỗi người dùng bởi các thiết đặt trong các chính sách truy nhập từ xa. Ví dụ một chính sách có thể gán tất cả người dùng trong một nhóm nào đấy quyền truy cập chỉ trong giờ làm việc hành chính từ 8:00 A.M đến 5:00 P.M, hay đồng thời gán cho một nhóm người dùng khác quyền truy cập liên tục 24/24. Profile: Mỗi chính sách đều bao gồm một thiết đặt của profile áp dụng cho kết nối như là các thủ tục xác thực hay mã hóa. Các thiết đặt trong profile được thi hành ngay tới các kết nối. Ví dụ: nếu một profile thiết đặt cho một kết nối mà người dùng chỉ được phép sử dụng trong 30 phút mỗi lần thì người dùng sẽ bị ngắt kết nối tới máy chủ truy cập trong sau 30 phút.

Các điều kiện được gửi tới để tạo một kết nối, nếu các điều kiện gửi tới này không thích hợp truy cập bị từ chối, nếu thích hợp các điều kiện này được sử dụng để xác định sự truy cập. Tiếp theo máy chủ truy cập kiểm tra các cho phép quay số vào người dùng sẽ bị từ chối nếu thiết đặt này là Deny và được phép truy cập nếu là Allow, nếu thiết đặt là sử dụng các chính sách truy cập để xác định quyền truy cập thì sự cho phép của các chính sách sẽ quyết định quyền truy cập của người dùng. Nếu các chính sách này từ chối truy cập người dùng sẽ bị ngắt kết nối, nếu là cho phép sẽ chuyển tới để kiểm tra các chính sách trong profile là bước cuối cùng để xác định quyền truy cập của người dùng.

3.4. Sử dụng dịch vụ gán địa chỉ động DHCP cho truy cập từ xa

Khi thiết lập một máy chủ truy cập để cho phép người dùng từ xa truy cập vào mạng, ta có thể lựa chọn phương thức mà các máy từ xa có thể nhận được địa chỉ IP.

Với phương thức cấu hình địa chỉ IP tĩnh ngay trên các máy trạm, người dùng phải cấu hình bằng tay địa chỉ IP trên mỗi máy truy cập. Sử dụng phương thức này phải đảm bảo rằng các thông tin cấu hình địa chỉ IP là hợp lệ và chưa được sử dụng trên mạng. Đồng thời các thông tin về default gateway, DNS…cũng phải được cấu hình bằng tay một cách chính xác.Vì lí do này khuyến nghị không nên sử dụng phương pháp này cho việc gán IP cho các máy truy cập từ xa. Máy chủ truy cập có thể gán động một địa chỉ IP cho các máy truy cập từ xa.

Địa chỉ IP này thuộc trong khoảng địa chỉ mà ta đã cấu hình trên máy chủ truy cập. Sử dụng phương pháp này ta cần phải đảm bảo rằng khoảng địa chỉ IP này được dành riêng để cấp phát cho các máy truy cập từ xa. Phương thức sử dụng DHCP server, máy chủ truy cập nhận địa chỉ IP từ DHCP server và gán cho các máy truy cập từ xa. Phương thức này rất linh hoạt, không cần phải dành riêng một khoảng địa chỉ IP dự trữ cho máy truy cập từ xa và thường được sử dụng trong một mạng có tổ chức và đa dạng trong các hình thức kết nối. Địa chỉ IP được cấp phát cho các máy truy cập từ xa một cách tự động, các thông tin cấu hình khác (Gateway, DNS server…) cũng được cung cấp tập trung, chính xác tới từng máy truy cập đồng thời các máy truy cập cũng không cần thiết phải cấu hình lại khi có các thay đổi về cấu trúc mạng.

Hoạt động của DHCP được mô tả như sau: Mỗi khi DHCP client khởi động, nó yêu cầu một địa chỉ IP từ DHCP server. Khi DHCP server nhận yêu cầu, nó chọn một địa chỉ IP trong khoảng IP đã được định nghĩa trong cơ sở dữ liệu của nó. DHCP server cấp phát địa chỉ IP tới DHCP client Nếu DHCP client chấp nhận địa

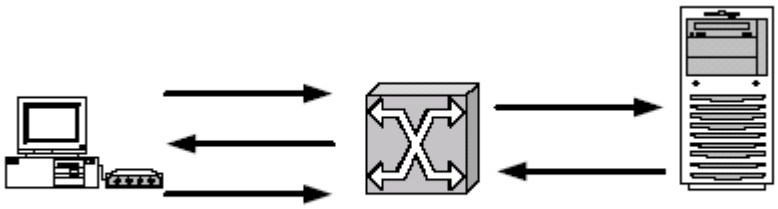
chỉ IP này, DHCP server cho thuê địa chỉ IP này trong một khoảng thời gian cụ thể (tùy theo thiết đặt).

Các thông tin về địa chỉ IP được gửi từ DHCP server tới DHCP client thường bao gồm các thành phần sau: địa chỉ IP, subnet mask, các giá trị lựa chọn khác (default gateway, địa chỉ DNS server).

3.5. Sử dụng Radius server để xác thực kết nối cho truy cập từ xa

a. Hoạt động của Radius server

Radius là một giao thức làm việc theo mô hình client/server. Radius cung cấp dịch vụ xác thực và tính cước cho mạng truy nhập gián tiếp. Radius client là một máy chủ truy cập tiếp nhận các yêu cầu xác thực từ người dùng từ xa và chuyển các yêu cầu này tới Radius server. Radius server nhận các yêu cầu kết nối của người dùng xác thực; sau đó, trả về các thông tin cấu hình cần thiết cho Radius client để chuyển dịch vụ tới người sử dụng.



Hình 4.4 – Quá trình hoạt động của Radius server

Quá trình hoạt động được mô tả như sau:

1. Người sử dụng từ xa khởi tạo quá trình xác thực PPP tới máy chủ truy cập;

2. Máy chủ truy cập yêu cầu người dùng cung cấp thông tin về username và password bằng các giao thức PAP hoặc CHAP;

3. Người dùng từ xa phúc đáp và gửi thông tin username và password tới máy chủ truy cập;

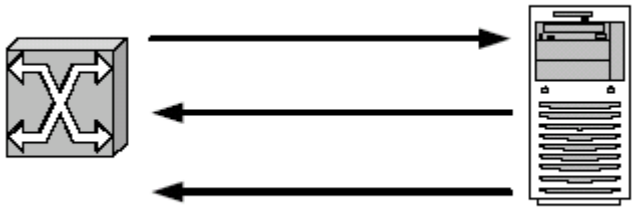
4. Máy chủ truy cập (Radius client) gửi chuyển tiếp các thông tin username và password đã được mã hóa tới Radius server;

5. Radius server trả lời với các thông tin chấp nhận hay từ chối. Radius client thực hiện theo các dịch vụ và các thông số dịch vụ đi cùng với các phúc đáp chấp nhận hay từ chối từ Radius server.

b. Nhận thực và cấp quyền

Khi Radius server nhận yêu cầu truy cập từ Radius client, Radius server tìm kiếm trong cơ sở dữ liệu các thông tin về yêu cầu này. Nếu username không có trong cơ sở dữ liệu này thì hoặc một profile mặc định được chuyển hoặc một thông báo từ chối truy cập được chuyển tới Radius client.

Trong RADIUS nhận thực và cấp quyền đi đôi với nhau, nếu username có trong cơ sở dữ liệu và password được xác nhận là đúng thì Radius server gửi trả về thông báo truy cập được chấp nhận, thông báo này bao gồm một danh sách các cặp đặc tính- giá trị mô tả các thông số được sử dụng cho phiên làm việc. Các thông số điển hình bao gồm: kiểu dịch vụ, kiểu giao thức, địa chỉ gán cho người dùng (động hoặc tĩnh), danh sách truy cập được áp dụng hay một định tuyến tĩnh được cài đặt trong bảng định tuyến của máy chủ truy cập. Thông tin cấu hình trong Radius server sẽ xác định những gì sẽ được cài đặt trên máy chủ truy cập. Hình 4.5 dưới đây mô tả quá trình nhận thực và cấp quyền của Radius server.



Hình 4.5 – Mô tả quá trình nhận thực và cấp quyền của Radius server

c.Tính cước

Các vấn đề về xử lý cước của RADIUS hoạt động độc lập với nhận thực và cấp quyền. Chức năng tính cước cho phép ghi lại dữ liệu được gửi tại thời điểm bắt đầu và kết thúc của một phiên làm việc và đưa ra các con số về mặt sử dụng tài nguyên như (thời gian, số gói, số byte…) được sử dụng trong phiên làm việc đó.

3.6. Mạng riêng ảo và kết nối sử dụng dịch vụ truy cập từ xa

VPN (Virtual Private Network) là một mạng riêng được xây dựng trên nền tảng hạ tầng mạng công cộng (ví dụ mạng Internet), sử dụng mạng công cộng cho việc truyền thông riêng tư.

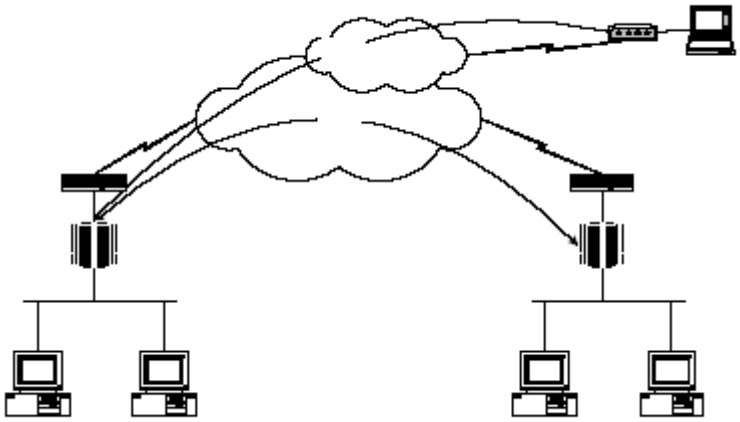
Giải pháp VPN cho phép người dùng làm việc tại nhà hoặc đang đi công tác ở xa có thể thực hiện một kết nối tới trụ sở chính bằng việc sử dụng hạ tầng mạng là một mạng công cộng như là Internet, Như vậy thay vì phải thực hiện một kết nối đường dài tới trụ sở chính người sử dụng chỉ cần tạo lập một kết nối nội hạt tới một ISP khi đó bằng công nghệ VPN một kết nối VPN sẽ được thiết lập

giữa người dùng với mạng trung tâm. Kết nối VPN cũng cho phép các tổ chức kết nối liên mạng giữa các địa điểm ở xa khác nhau thông qua các kết nối trực tiếp (leased line) từ các địa điểm đó tới một ISP.

Như vậy kết nối VPN cho phép một tổ chức giảm chi phí gọi đường dài qua Dialup hay chi phí thuê đường leadline cho khoảng cách xa thay vì như vậy chỉ cần các kết nối nội hạt và điều này là tiết kiệm được chi phí. VPN gửi dữ liệu giữa các đầu cuối, dữ liệu được đóng gói, với các Header cung cấp thông tin định tuyến cho phép chuyển dữ liệu qua một liên kết hoặc một liên mạng công cộng tới đích. Dữ liệu chuyển đi được mã hoá để đảm bảo an toàn, các gói dữ liệu truyền thông trên mạng là không thể đọc mà không có khoá giải mã. Liên kết mà trong đó dữ liệu được đóng gói và mã hoá là một kết nối VPN.

Các hình thức kết nối:

Có hai kiểu kết nối VPN, kết nối VPN truy cập từ xa và kết nối Site-to-site. Một kết nối VPN truy cập từ xa được thiết lập bởi một máy tính PC tới một mạng dùng riêng. VPN gateway cung cấp truy cập tới các tài nguyên của mạng dùng riêng. Các gói dữ liệu gửi qua kết nối VPN được khởi tạo từ các client. VPN client thực hiện việc xác thực tới VPN gateway. Kết nối site-to-site, được thiết lập bởi các VPN gateway và kết nối hai phần của một mạng dùng riêng.



Hình 4.6 – Giải pháp kết nối VPN

Tunnel: là một phần quan trọng trong việc xây dựng một mạng VPN. Các chuẩn truyền thông sử dụng để quản lý các tulnnel và đóng gói dữ liệu của VPN bao gồm các giao thức làm việc ở lớp 2 như PPTP (Point-to-Point Tunlling Protocol) được phát triển bởi Microsoft hỗ trợ trong môi trường mạng Windows, L2TP (Layer 2 Tunnelling Protocol) được phát triển bởi Cisco. IPsec là một giao thức làm việc ở lớp 3, IPsec được phát triển bởi IETF và ngày càng được sử dụng rộng rãi. L2TP và PPTP có mục đích là cung cấp các đường hầm dữ liệu thông qua mạng truyền dữ

liệu công cộng. L2TP khác với PPTP ở chỗ nó tạo lập đường hầm nhưng không mã hoá dữ liệu. L2TP cung cấp các đường hầm bảo mật khi cùng hoạt động với các công nghệ mã hoá khác như IPSec. IPSec không yêu cầu phải có L2TP nhưng các chức năng mã hoá của nó đưa đến cho L2TP khả năng cung cấp các kênh thông tin bảo mật, cung cấp các giải pháp VPN. L2TP và PPTP cùng sử dụng PPP để đóng gói, thêm bớt thông tin tiếp đầu và truyền tải dữ liệu qua mạng. Các kết nối VPN có các đặc trưng sau: đóng gói (Encapsulation), xác thực (Authentication) và mã hoá dữ liệu (Data encryption)

Đóng gói dữ liệu: Công nghệ VPN sử dụng một phương thức đóng gói dữ liệu trong đó cho phép dữ liệu truyền được qua mạng công cộng qua các giao thức tạo đường hầm.

Xác thực: Khi một kết nối VPN được thiết lập,VPN gateway sẽ xác thực VPN client đang yêu cầu kết nối và nếu được được phép kết nối được thực hiện. Nếu sự xác thực kết nối là qua lại được sử dụng, thì VPN client sẽ thực hiện việc xác thực lại VPN gateway, để đảm bảo rằng đấy chính là server mà mình cần gọi. Xác thực dữ liệu và tính toàn vẹn của dữ liệu: để xác nhận rằng dữ liệu đang được gửi từ một đầu của kết nối khác mà không bị thay đổi trong quá trình truyền, dữ liệu phải bao gồm một trường kiểm tra bằng mật mã dự trên một khoá mã hoá đã biết chỉ giữa người gửi và người nhận

Mã hóa dữ liệu: để đảm bảo dữ liệu truyền trên mạng, dữ liệu phải được mã hoá tại đầu gửi và giải mã tại đầu nhận. Việc mã hoá và giải mã dữ liệu phụ thuộc và người gửi và người nhận đang sử dụng phương thức mã hoá và giải mã nào.

3.7. Sử dụng Network and Dial-up Connection

Network and Dial-up Connection (NDC) là một công cụ được Microsoft phát triển để hỗ trợ việc tạo lập các kết nối trong đó bao gồm các kết nối cho truy cập từ xa. Với việc sử dụng NDC ta có thể truy cập tới các tài nguyên dù đang ở trong mạng hay ở một địa điểm ở xa. Các kết nối được khởi tạo, thiết lập cấu hình, lưu giữ và quản lý bởi NDC. Mỗi một kết nối bao gồm một bộ các đặc tính được sử dụng để thiết lập liên kết giữa một máy tính tới máy tính hoặc mạng khác. Các kết nối gọi ra được liên lạc với một máy chủ truy cập ở xa bằng các hình thức truy cập gián tiếp thương là qua các mạng truyền dẫn mạng thoại công cộng, mạng ISDN.

NDC cũng hỗ trợ việc thiết lập các kết nối gọi vào có nghĩa là đóng vai trò như một máy chủ truy cập. Bởi vì tất cả các dịch vụ và các phương thức truyền thông đều được thiết lập trong kết nối nên không cần phải sử dụng các công cụ khác để cấu hình cho kết nối. Ví dụ để thiết lập cho một kết nối dial-up bao gồm

các đặc tính được sử dụng trước, trong và sau khi kết nối. Các thông số này bao gồm: modem sẽ quay số, kiểu mã hóa password được sử dụng và các giao thức mạng sẽ sử dụng sau kết nối. Trạng thái kết nối bao gồm thời gian và tốc độ cũng được chính kết nối hiển thị mà không cần bất cứ một công cụ nào khác.

3.8. Một số vấn đề xử lý sự cố trong truy cập từ xa

Các vấn đề liên quan đến sự cố trong truy cập từ xa, thường bao gồm:

- Giám sát truy cập từ xa: giám sát máy chủ truy cập là phương pháp tốt nhất thường sử dụng để tìm ra nguồn gốc của các vấn đề xảy ra sự cố. Mỗi một chương trình phần mềm hay thiết bị phần cứng máy chủ truy cập bao giờ cũng có các công cụ sử dụng để giám sát và ghi lại các sự kiện xảy ra (trong các file log) đối với mỗi phiên truy cập từ xa.

- Theo dõi các kết nối truy cập từ xa: khả năng theo dõi các kết nối truy cập từ xa của một Máy chủ truy cập cho ta xử lý các vấn đề phức tạp về sự cố mạng. Các thông tin theo dõi một kết nối từ xa thường rất phức tạp và khá chi tiết do đó để phân tích và xử lý cần thiết người quản trị mạng phải có kinh nghiệm và trình độ về hệ thống mạng.

- Xử lý các sự cố về phần cứng: bao gồm các thiết bị truyền thông tại người dùng và tại máy chủ truy cập. Đối với các thiết bị tại người dùng (thường là các modem, cạc mạng…), hãy xem tài liệu về sản phẩm đó hay hỏi nhà cung cấp thiết bị về sản phẩm của họ về các cách kiểm tra và xác định lỗi của sản phẩm này. Nếu kết nối sử dụng modem, hãy kiểm tra rằng modem đã được cài đặt đúng chưa.

Trong Windows server, các bước kiểm tra như sau:

o Trong Control Panel, chọn Phone and Modem Options; Trong trang modem, nhắp tên modem, sau đó chọn Properties

o Chọn Diagnostics, sau đó chọn Query Modem. Nếu modem đã được cài đặt đúng, bộ các thông số về modem sẽ được hiển thị, ngược lại hãy kiểm tra và cài đặt lại modem, trong trường hợp cuối cùng hãy hỏi nhà sản xuất thiết bị này. Để nhận thêm các thông tin về modem trong khi đang cố gắng tạo lập một kết nối, hãy xem thông tin trong log file để tìm ra nguyên nhân gạp sự cố.

Để ghi các thông tin vào log file thực hiện theo các bước sau:

o Trong Control Panel, chọn Phone and Modem Options

o Trong trang modem, chọn tên modem, sau đó chọn Properties

o Chọn Diagnostics, lựa chọn Record a log, sau đó nhắp OK. Đối với thiết bị truyền thông tại máy chủ truy cập: Kiểm tra các thiết bị phần cứng tương tự như

trong trường hợp thiết bị tại người dùng, đồng thời kiểm tra log file về các sự kiện xẩy ra với hệ thống để tìm ra nguyên nhân sự cố. Một cách khác để kiểm tra modem tại máy chủ truy cập là sử dụng một đường điện thoại và gọi tới modem đó sau đó nghe xem modem đó có trả lời và cố gắng tạo một kết nối hay không. Nếu không có tín hiệu tạo kết nối từ modem đó thì có thể kết luận rằng đang có một vấn đề lỗi về modem tại máy chủ truy cập.

Xử lý các sự cố về đường truyền thông: Thường là do cáp được đấu sai hay vì nguyên nhân từ nhà cung cấp dịch vụ điện thoại. Hãy kiểm tra đường điện thoại từ người dùng tới máy chủ truy cập bằng cách gọi điện thoại thông thường, thông qua chất lượng cuộc gọi ta cũng có thể phần nào dự đoán được chất lượng của đường truyền.

Xử lý các thiết đặt về cấu hình: Sau khi xác định rằng các vấn đề về phần cứng cũng như đường truyền thông đều tốt, bước tiếp theo ta kiểm tra các thiết đặt về cấu hình, bao gồm: Các thiết đặt về mạng: lỗi cấu hình về mạng xảy ra khi đã tạo kết nối thành công nhưng vẫn không thể truy cập được các nguồn tài nguyên trên mạng, các lỗi thường xẩy ra như việc phân giải tên chưa hoạt động, các lỗi về định tuyến… khi lỗi về cấu hình mạng xảy ra, trước tiên ta kiểm tra rằng các máy kết nối trực tiếp (không thông qua dịch vụ truy cập từ xa) có thể truy cập được vào các nguồn tài nguyên trên mạng. Sau đó kiểm tra các cấu hình về TCP/IP bằng việc sử dụng lệnh ipconfig /all trên máy client. Kiểm tra rằng các thông số như DNS, địa chỉ IP, các thông số về định tuyến đã được thiết đặt đúng chưa. Sử dụng lệnh ping để kiểm tra kết nối mạng đã làm việc.

Các thiết đặt máy chủ truy cập: Các thiết đặt trên máy chủ truy cập với các thông sô sai khi tạo lập kết nối có thể là nguyên nhân người dùng không thể truy cập vào các nguồn tài nguyên trên mạng. Để hỗ trợ cho việc xác định nguyên nhân gây lỗi, kiểm tra các sự kiện đã ghi log trên máy chủ truy cập và client, trong một số trường hợp cần thiết phải theo dõi (tracing) các kết nối trên máy chủ truy cập. Các thiết đặt trên máy người dùng từ xa: kiểm tra các giao thức mạng làm việc trên client, các giao thức mạng làm việc trên client phải được hỗ trợ bởi máy chủ truy cập. Ví dụ, nếu người dùng từ xa thiết đặt trên client các giao thức NWLink, IPX/SPX và máy chủ truy cập chỉ hỗ trợ sử dụng TCP/IP, thì kết nối sẽ không thành công.

Câu hỏi

1. Trình bày ý nghĩa của dịch vụ truy nhập từ xa.
2. Cho biết các phương thức xác thực kết nối.

3. Mô tả các phương thức mã hóa dữ liệu.

Bài tập thực hành

1. Xây dựng một Remote Access Server.

Các bước thực hiện:
- Cấu hình RAS server
- Cấu hình RAS client

2. Cài đặt và cấu hình dịch vụ truy cập từ xa cho phép người dùng từ xa truy cập vào mạng trên hệ điều hành Windows Server.

Các bước thực hiện:
- Cài đặt máy chủ dịch vụ truy cập từ xa
- Thiết đặt tài khoản cho người dùng từ xa. Thiết lập một tài khoản có tên RemoteUser
- Kiểm tra cấu hình đã thiết lập
- Cấu hình cho phép tài khoản RemoteUser truy cập vào mạng được điều khiển truy cập bởi các chính sách truy cập từ xa (Remote access policy)
- Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.
- Sử dụng RRAS để thiết lập một chính sách mới đối với người dùng từ xa, tên chính sách này là Allow RemoteGroup Access cho phép người dùng trong nhóm RemoteGroup truy cập.
- Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.
- Cấu hình để default policy được thi hành trước
- Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser. Thông báo lỗi xuất hiện, kết nối không được thiết lập.
- Cấu hình cho phép truy cập sử dụng Properties của RemoteUser
- Kiểm tra cấu hình đã thiết lập ở bước trên bằng việc thực hiện một kết nối quay số tới máy chủ truy cập từ xa với tài khoản có tên là RemoteUser, kết nối được thiết lập sau đó đóng kết nối lại.

BÀI 5: GROUP POLICY OBJECT

Mã bài: MĐ 36-05

Mục tiêu của bài:
- Hiểu được chức năng của Group policy;
- Tạo và quản lý các đối tượng trong GPO;
- Thực hiện các thao tác an toàn với máy tính.

1. Giới thiệu Group Policy

Mục tiêu: Trình bày các chức năng chính của Group Policy, phân biệt được sự khác nhau cơ bản giữa System Policy và Group Policy.

1.1. So sánh giữa System Policy và Group Policy

Trong mô đun Quản trị mạng 1, chúng ta đã tìm hiểu về chính sách hệ thống (System Policy), tiếp theo chúng ta sẽ tìm hiểu về chính sách nhóm (Group Policy). Vậy hai chính sách này khác nhau như thế nào.

- Chính sách nhóm chỉ xuất hiện trên miền Active Directory, nó không tồn tại trên miền NT4.

- Chính sách nhóm làm được nhiều điều hơn chính sách hệ thống. Tất nhiên chính sách nhóm chứa tất cả các chức năng của chính sách hệ thống, hơn thế nữa, có thể dùng chính sách nhóm để triển khai một phần mềm cho một hoặc nhiều máy một cách tự động.

- Chính sách nhóm tự động hủy bỏ tác dụng khi được gỡ bỏ, không giống như các chính sách hệ thống.

- Chính sách nhóm được áp dụng thường xuyên hơn chính sách hệ thống. Các chính sách hệ thống chỉ được áp dụng khi máy tính đăng nhập vào mạng. Các chính sách nhóm được áp dụng khi bật máy lên, khi đăng nhập vào một cách tự động vào những thời điểm ngẫu nhiên trong suốt ngày làm việc.

- Có nhiều mức độ để gán chính sách nhóm này cho người từng nhóm người hoặc từng nhóm đối tượng.

- Chính sách nhóm tuy có nhiều ưu điểm nhưng chỉ áp dụng được trên máy Win2K, WinXP và Windows Server 2003.

1.2. Chức năng của Group Policy

- Triển khai phần mềm ứng dụng: có thể gom tất cả các tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (package), đặt nó lên Server, rồi

dùng chính sách nhóm hướng một hoặc nhiều máy trạm đến gói phần mềm đó. Hệ thống sẽ tự động cài đặt phần mềm này đến tất cả các máy trạm mà không cần sự can thiệp nào của người dùng.

- Gán các quyền hệ thống cho người dùng: chức năng này tương tự với chức năng của chính sách hệ thống. Nó có thể cấp cho một hoặc một nhóm người nào đó có quyền tắt server, đổi giờ hệ thống hay backup dữ liệu…

- Giới hạn những ứng dụng mà người dùng được phép thi hành: chúng ta có thể kiểm soát máy trạm của một người dùng nào đó và cho phép người dùng này chỉ chạy được một vài ứng dụng nào đó thôi như: Outlook Express, Word hay Internet Explorer.

- Kiểm soát các thiết lập hệ thống: Người quản trị có thể dùng chính sách nhóm để qui định hạn ngạch đĩa cho một người dùng nào đó. Người dùng này chỉ được phép lưu trữ tối đa bao nhiêu MB trên đĩa cứng theo qui định.

- Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy: trong hệ thống NT4 thì chỉ hỗ trợ kịch bản đăng nhập (logon script), nhưng Windows Server hỗ trợ cả bốn sự kiện này được kích hoạt (trigger) một kịch bản (script). Người quản trị có thể dùng các GPO để kiểm soát những kịch bản nào đang chạy.

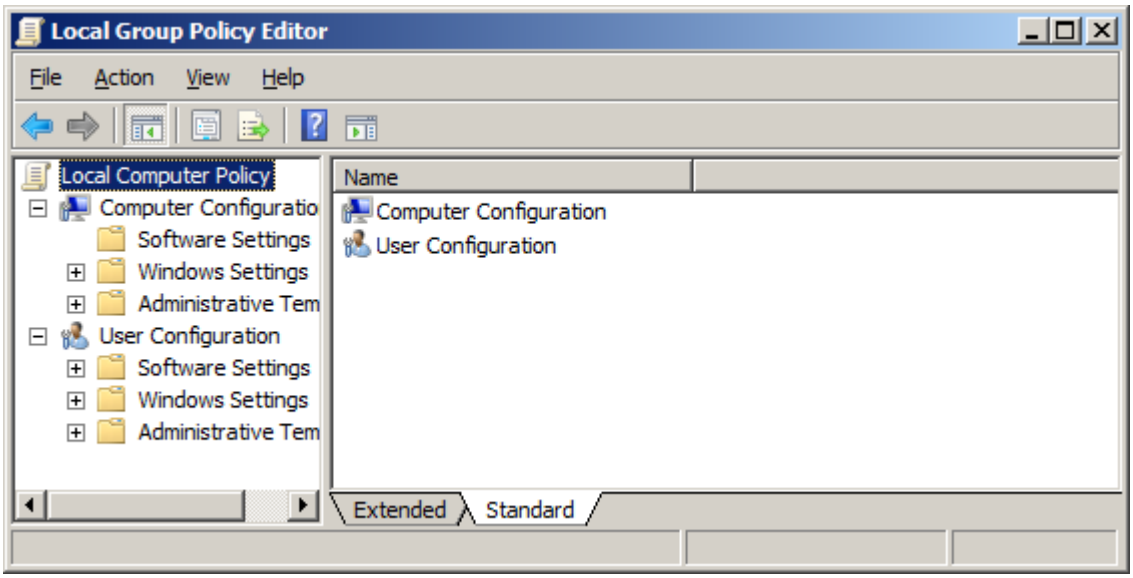
- Đơn giản hóa và hạn chế các chương trình: có thể dùng GPO để gỡ bỏ nhiều tính năng khỏi Internet Explorer, Windows Explorer và những chương trình khác.

- Hạn chế tổng quát màn hình Desktop của người dùng: có thể gỡ bỏ hầu hết các đề mục trên menu Start của một người dùng nào đó, ngăn chặn không cho người dùng cài thêm máy in, sửa đổi thông số cấu hình của máy trạm…

2. Tạo và tổ chức các đối tượng trong Group policy

Mục tiêu: Trình bày cách thức để xem chính sách cục bộ của một máy tính ở xa, tạo và áp dụng các chính sách trên miền.

Chúng ta cấu hình và triển khai Group Policy bằng cách xây dựng các đối tượng chính sách (GPO). Các GPO là một vật chứa (container) có thể chứa nhiều chính sách áp dụng cho nhiều người, nhiều máy tính hay toàn bộ hệ thống mạng. Người quản trị có thể dùng Group Policy Object Editor để tạo ra các đối tượng chính sách. Trong cửa sổ chính của Group Policy Object Editor (hình 5.1) có hai mục chính: cấu hình máy tính (computer configuration) và cấu hình người dùng (user configuration).



Hình 5.1 – Cửa sổ chính của Group Policy Object Editor

Điều kế tiếp cần chú ý khi triển khai Group Policy là các cấu hình chính sách của Group Policy được tích lũy và kề thừa từ các vật chứa (container) bên trên của Active Directory. Ví dụ các người dùng và máy tính vừa ở trong miền vừa ở trong OU nên sẽ nhận được các cấu hình từ cả hai chính sách cấp miền lẫn chính sách cấp OU. Các chính sách nhóm sau 90 phút sẽ được "làm tươi" và áp dụng một lần, nhưng các chính nhóm trên các Domain Controller được "làm tươi" 5 phút một lần. Các GPO hoạt động được không chỉ nhờ chỉnh sửa các thông tin trong Registry mà còn nhờ các thư viện liên kết động (DLL) làm phần mở rộng đặt tại các máy trạm. Chú ý nếu dùng chính sách nhóm thì chính sách nhóm tại chỗ trên máy cục bộ sẽ xử lý trước các chính sách dành cho site, miền hoặc OU.

2.1. Xem chính sách cục bộ của một máy tính ở xa

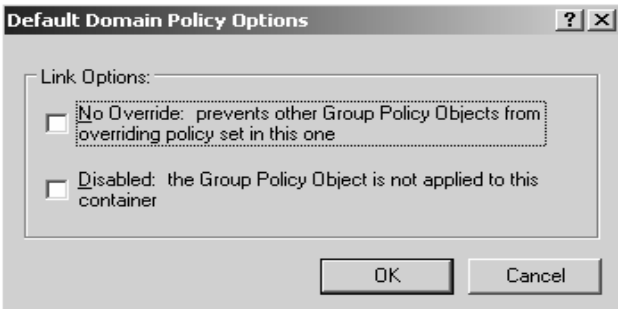
Để xem một chính sách cục bộ trên các máy tính khác trong miền, người xem phải có quyền quản trị trên máy đó hoặc quản trị miền. Lúc đó, có thể dùng lệnh GPEDIT.MSC /gpcomputer:machinename; ví dụ khi muốn xem chính sách trên máy PC01, gõ lệnh GPEDIT.MSC /gpcomputer: PC01. Chú ý: không thể dùng cách này để thiết lập các chính sách nhóm ở máy tính ở xa (do tính chất bảo mật Microsoft không cho phép người dùng ở xa thiết lập các chính sách nhóm).

2.2. Tạo các chính sách trên miền

Chúng ta dùng snap-in Group Policy trong Active Directory User and Computer hoặc gọi trực tiếp tiện ích Group Policy Object Editor từ dòng lệnh trên máy Domain Controller để tạo ra các chính sách nhóm cho miền. Nếu mở Group Policy từ Active Directory User and Computer, trong khung cửa sổ chính của chương trình, nhấp chuột phải vào biểu tượng tên miền (ví dụ: danavtc.edu), chọn Properties. Trong hộp thoại xuất hiện, chọn Tab Group Policy.

Hình 5.2 – Cửa sổ thuộc tính với chính sách mặc định

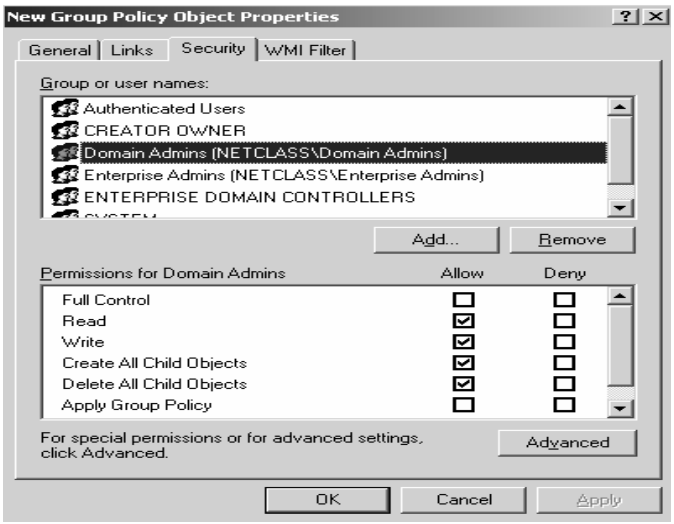
Nếu chưa tạo ra một chính sách nào thì cửa sổ chỉ hiển thị một chính sách tên Default Domain Policy (xem hình 5.2). Cuối hộp thoại có một checkbox tên Block Policy inheritance, chức năng của mục này là ngăn chặn các thiết định của mọi chính sách bất kỳ ở cấp cao hơn lan truyền xuống đến cấp đang xét. Chú ý rằng chính sách được áp dụng đầu tiên ở cấp site, sau đó đến cấp miền và cuối cùng là cấp OU. Chọn chính sách Default Domain Policy và nhấp chuột vào nút Option để cấu hình các lựa chọn việc áp dụng chính sách. Trong hộp thoại Options (hình 5.3), nếu đánh dấu vào mục No Override thì các chính sách khác được áp dụng ở dòng dưới sẽ không phủ quyết được những thiết định của chính sách này, cho dù chính sách đó không đánh dấu vào mục Block Policy inheritance. Tiếp theo, nếu đánh dấu vào mục Disabled thì chính sách này sẽ không hoạt động ở cấp này; việc disabled chính sách ở một cấp không làm disabled bản thân đối tượng chính sách.



Hình 5.3 – Hộp thoại cấu hình các lựa chọn việc áp dụng chính sách

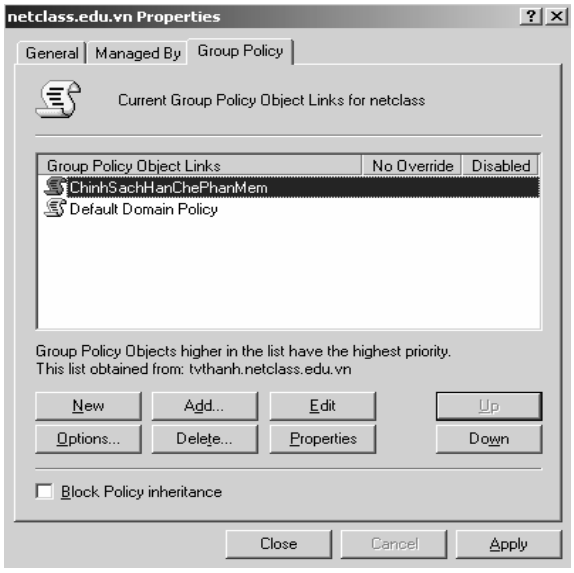
Để tạo ra một chính sách mới, nhấp chuột vào nút New, sau đó nhập tên của chính sách mới. Để khai báo thêm thông tin cho chính sách này, nhấp chuột vào nút Properties, hộp thoại xuất hiện có nhiều Tab, vào Tab Links để chỉ ra các site,

domain hoặc OU nào liên kết với chính sách. Tab Security như hình 5.4 cho phép cấp quyền cho người dùng hoặc nhóm người dùng trên chính sách này.



Hình 5.4 – Cấp quyền cho người dùng hoặc nhóm người dùng

Trong hộp thoại chính của Group Policy thì các chính sách được áp dụng từ dưới lên trên, cho nên chính sách nằm trên cùng sẽ được áp dụng cuối cùng. Do đó, các GPO càng nằm trên cao trong danh sách thì càng có độ ưu tiên cao hơn, nếu chúng có những thiết định mâu thuẫn nhau thì chính sách nào nằm trên sẽ thắng. Nút Up và Down giúp thay đổi thứ tự các chính sách.



Hình 5.5 – Thứ tự các chính sách

Nút Edit cho phép thiết lập các thiết định cho chính sách này; Dựa trên các khả năng của Group Policy, có thể thiết lập các thiết định theo yêu cầu.

3. Thiết lập các chính sách trên Domain Controller

Mục tiêu: Trình bày cách thiết lập các chính sách nhóm chặn người dùng cài đặt phần mềm ứng dụng, hay chặn người dùng sử dụng các chương trình được chỉ định.

3.1. Thiết lập chính sách nhóm "chặn người dùng cài đặt phần mềm ứng dụng"

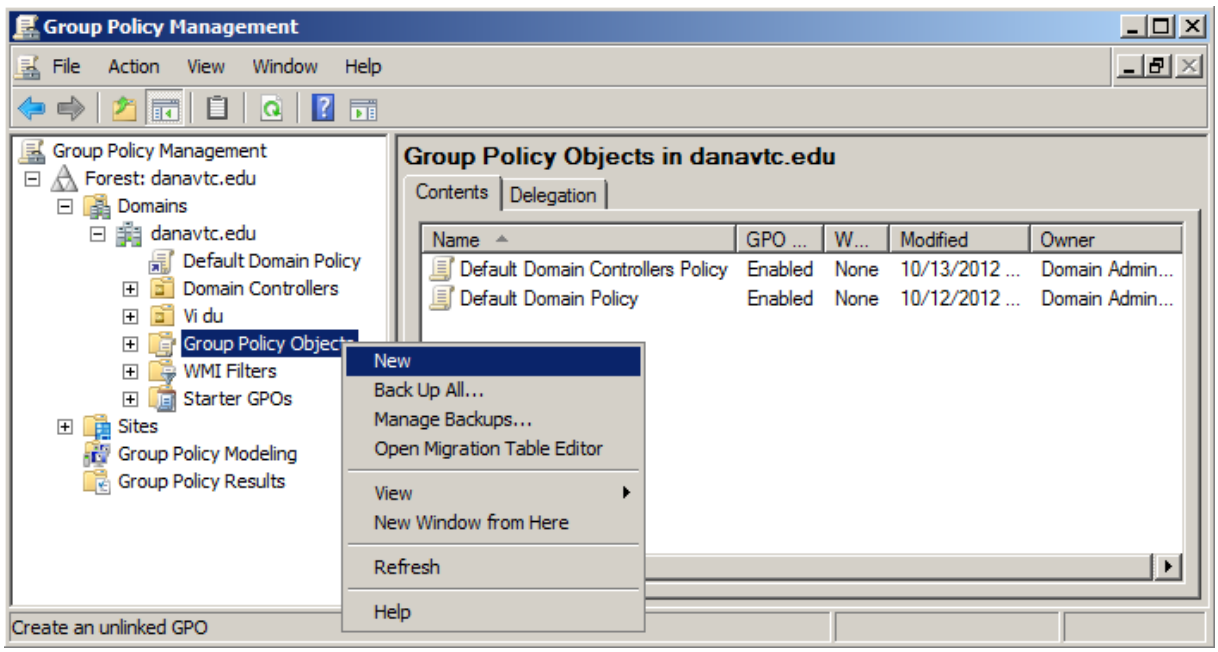
Công cụ này cho phép hạn chế người dùng cài đặt các phần mềm ứng dụng.

Thực hiện:

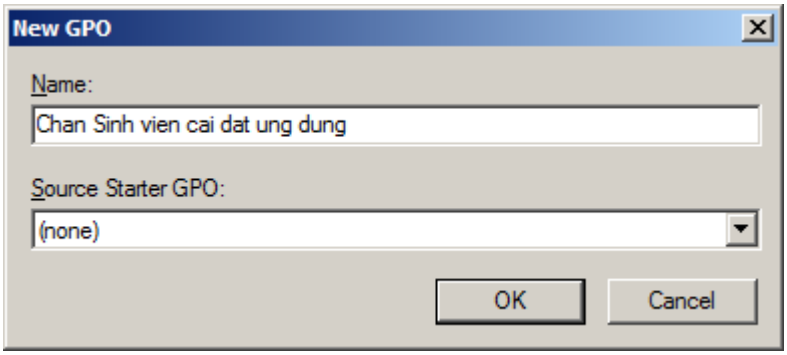
- Tạo một Group Policy Object (GPO) độc lập:

+ Start → Administrative Tools → Group Policy Management

+ Tại cửa sổ Group Policy Management, nhấp chuột phải lên mục Group Policy Objects và chọn New



+ Tại hộp thoại Name GPO nhập tên GPO (Chặn Sinh viên cài đặt ứng dụng), chọn OK

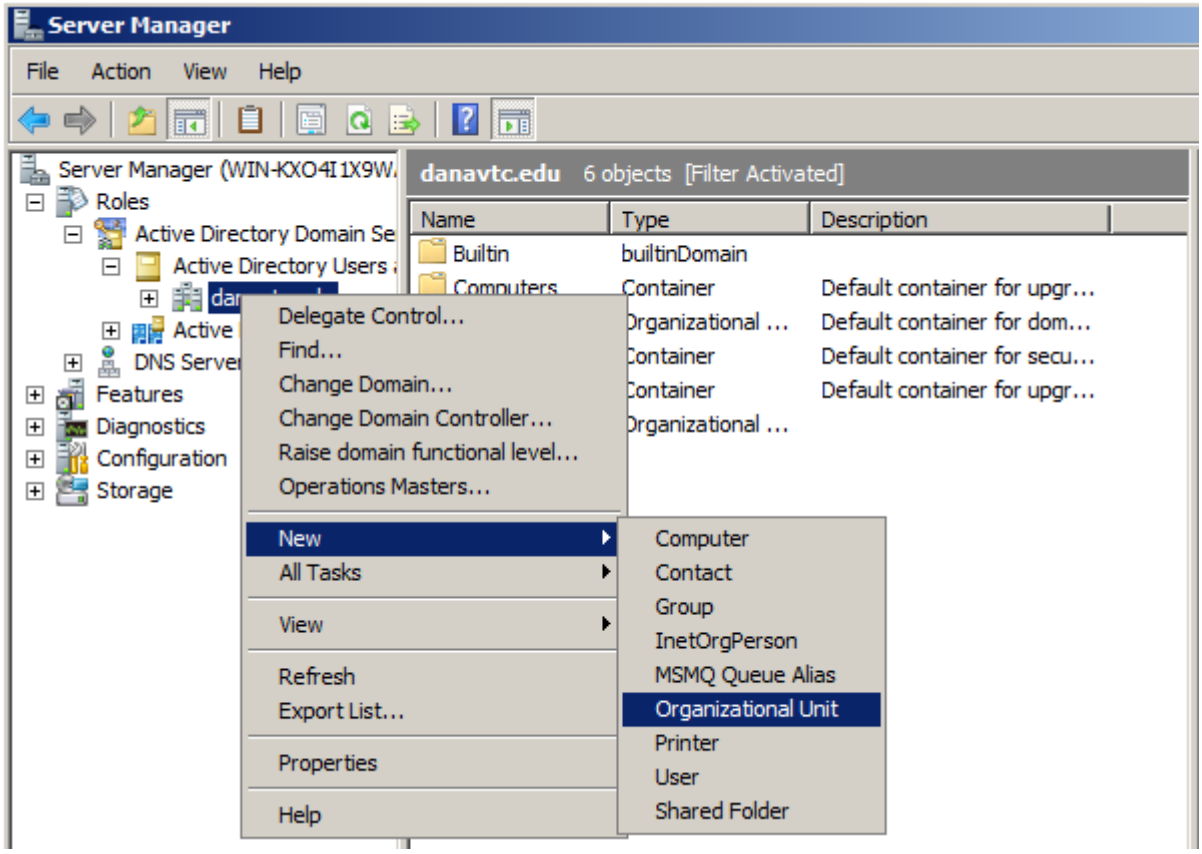


+ Trở lại cửa sổ Group Policy Management, nhắp phải chuột lên GPO vừa tạo, chọn Edit. Khi xuất hiện cửa sổ Group Policy Management Editor, chỉ định Polices cần cấu hình của Computer hoặc user (chọn Computer Configuration / Policies / Administrative Templates / Windows Components / Windows Installer).

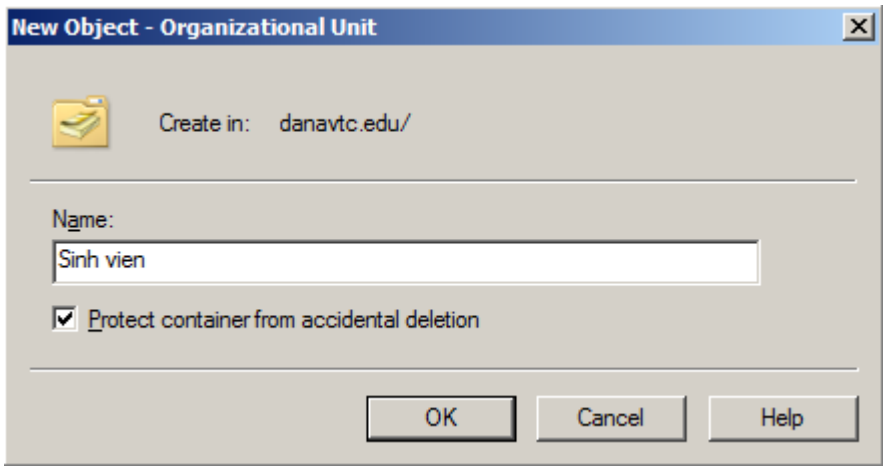
+ Sử dụng thiết lập Prohibit User Installs: Nhắp phải chuột vào Prohibit User Installs (ở khung phải), chọn Properties rồi thực hiện các thiết lập: Chọn Enabled và lựa chọn hành vi tương ứng là Hide User Installs. Chọn Apply, OK để đóng cửa sổ Prohibit User Installs Properties.

- Liên kết GPO vào các loại đối tượng trên Active Directory (Lưu ý: mỗi GPO có thể liên kết đến nhiều đối tượng trên Active Directory):

+ Tạo các đối tượng trên Active Directory: Server Manager → Roles → Active Directory Domain Services → Active Directory Users and Computers. Nhấp chuột phải vào tên domain và chọn New → Organization Unit.

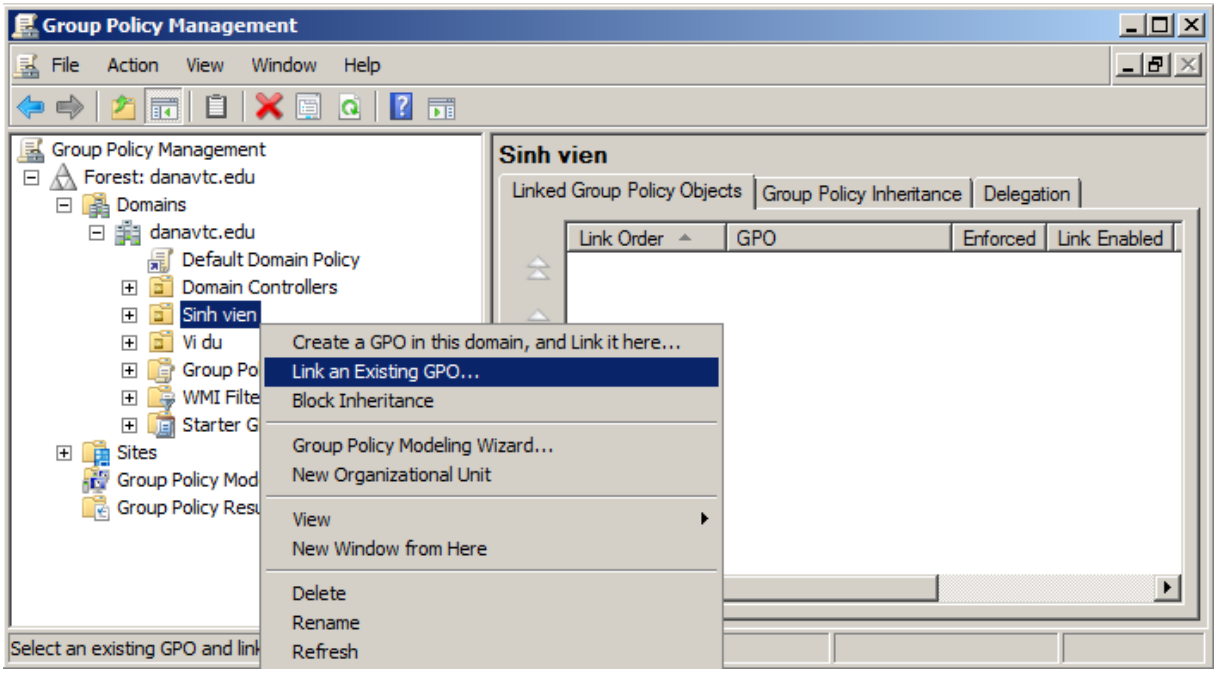


+ Khi xuất hiện cửa sổ New Object, gõ tên đối tượng vào (Sinh vien)

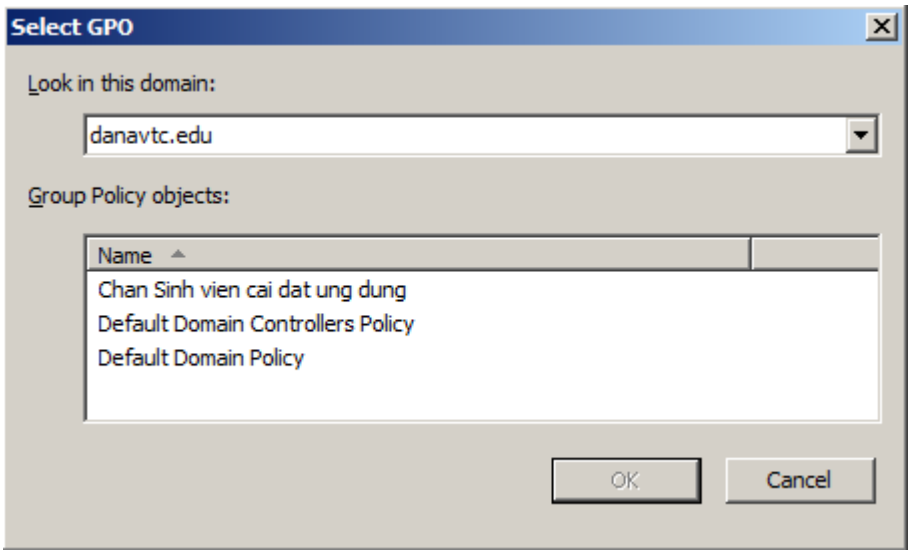


+ Tạo user và computer trong OU này (user SV1, V2)

+ Liên kết GPO vào OU: Vào Start → Adminitrative Tools → Group Policy Management; Nhấp chuột phải vào OU và chọn Link an Existing GPO



+ Trong hộp thoại Select GPO chọn tên domain ở mục Look in this domain; Đồng thời chọn GPO tương ứng (Chan Sinh vien cai dat ung dung) ở mục Group Policy objects.



+ Chọn OK để hoàn tất.

3.2. Thiết lập chính sách nhóm "chặn người dùng sử dụng Internet Explorer"

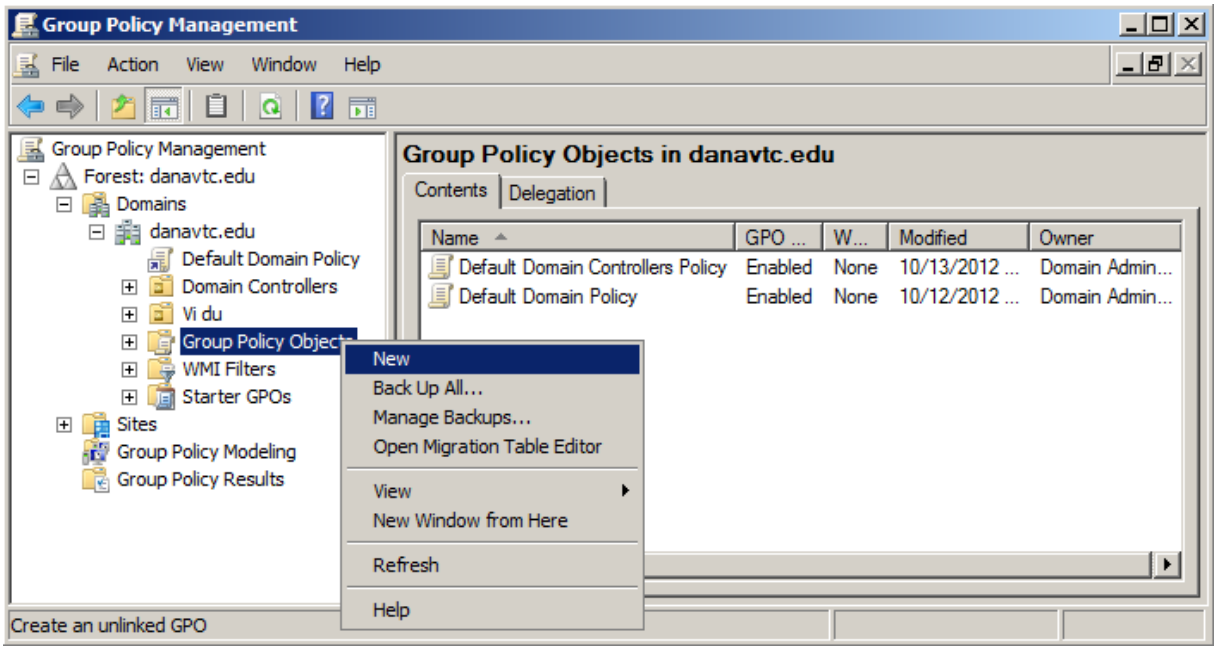
Công cụ này cho phép hạn chế người dùng sử dụng các chương trình được chỉ định.

Thực hiện:

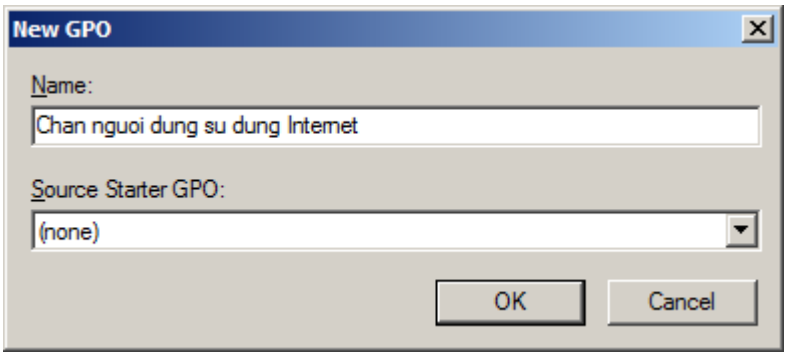
- Tạo một Group Policy Object (GPO) độc lập:

+ Start → Administrative Tools → Group Policy Management

+ Tại cửa sổ Group Policy Management, nhấp chuột phải lên mục Group Policy Objects và chọn New

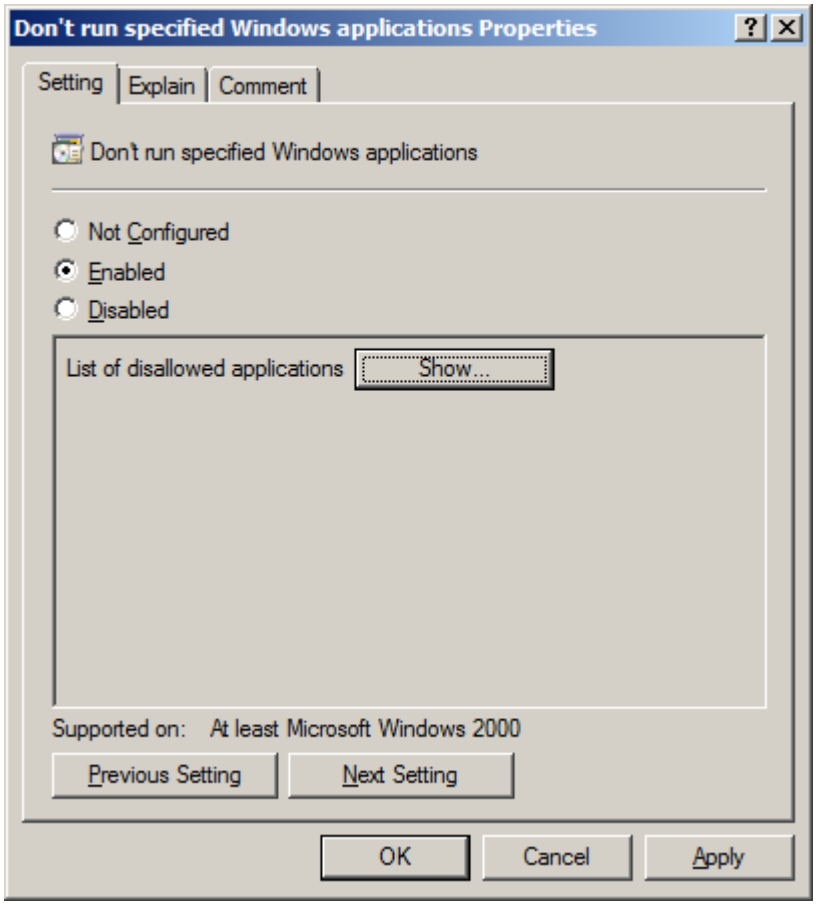


+ Tại hộp thoại Name GPO nhập tên GPO (Chặn người dùng sử dụng Interrnet), chọn OK



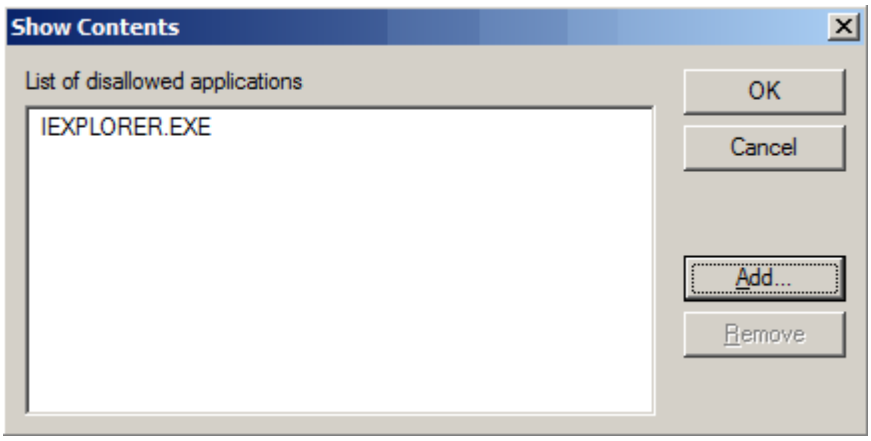
+ Trở lại cửa sổ Group Policy Management, nhắp phải chuột lên GPO vừa tạo, chọn Edit. Khi xuất hiện cửa sổ Group Policy Management Editor, chỉ định Polices cần cấu hình của Computer hoặc user (chọn User Configuration / Policies / Administrative Templates / System).

+ Sử dụng thiết lập Don't run specified Windows applications: Nhắp phải chuột vào Don't run specified Windows applications (ở khung phải), chọn Properties rồi thực hiện các thiết lập:



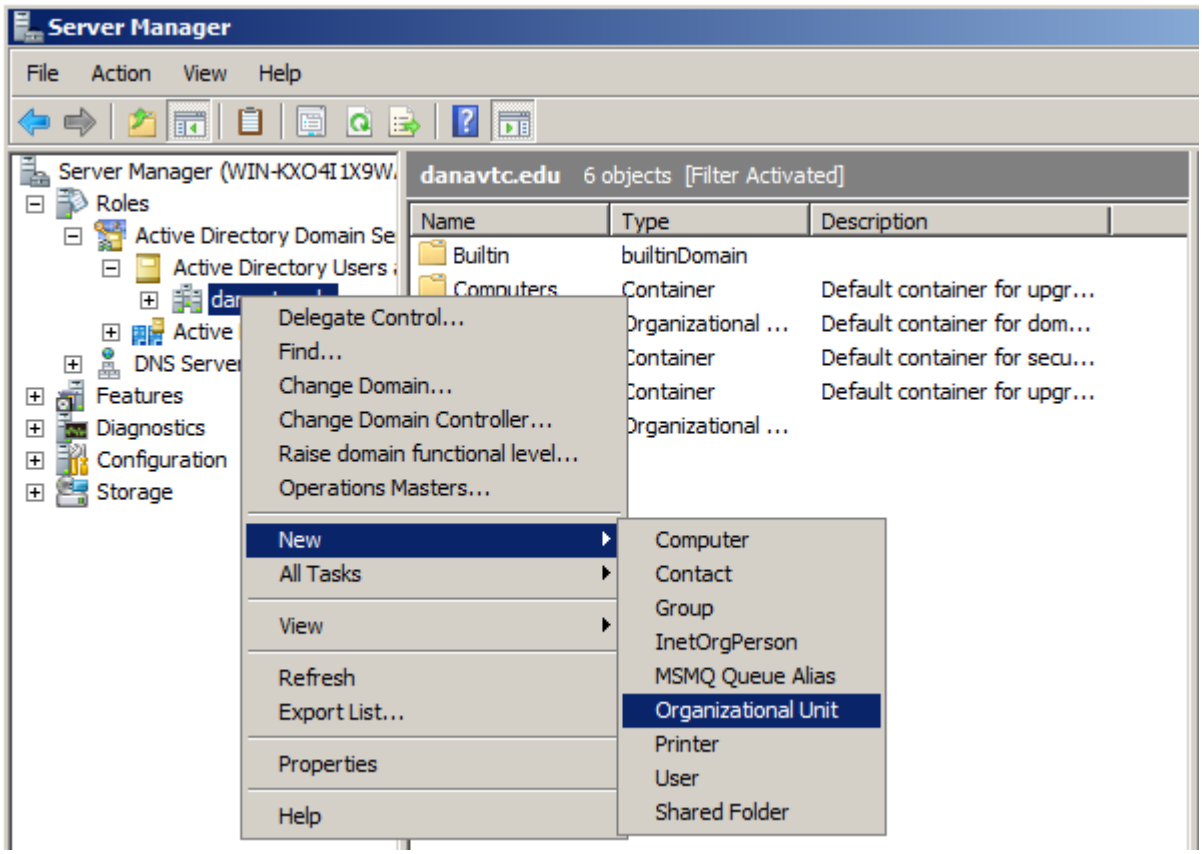
Đánh dấu chọn Enabled; Chọn nút Show…

Khi màn hình xuất hiện hộp thoại Show Contents, chọn nút Add… để chỉ định tập tin chương trình ứng dụng không được phép thi hành.

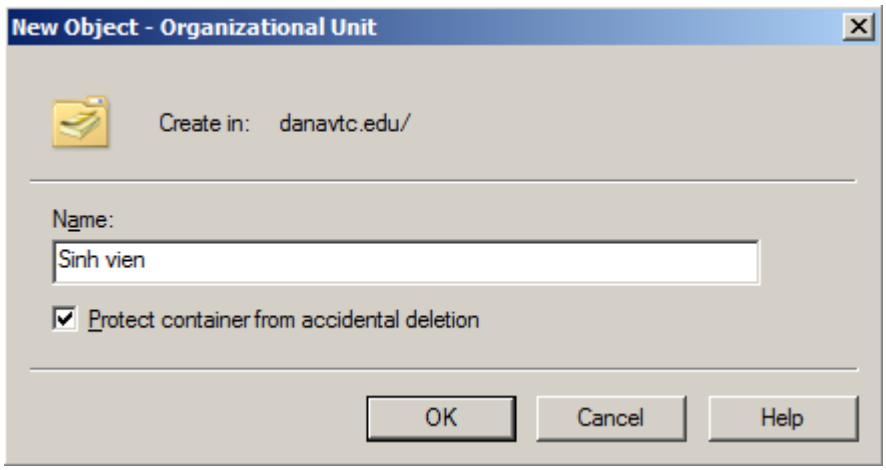


- Liên kết GPO vào các loại đối tượng trên Active Directory (Lưu ý: mỗi GPO có thể liên kết đến nhiều đối tượng trên Active Directory):

+ Tạo các đối tượng trên Active Directory: Server Manager → Roles → Active Directory Domain Services → Active Directory Users and Computers. Nhấp chuột phải vào tên domain và chọn New → Organization Unit.

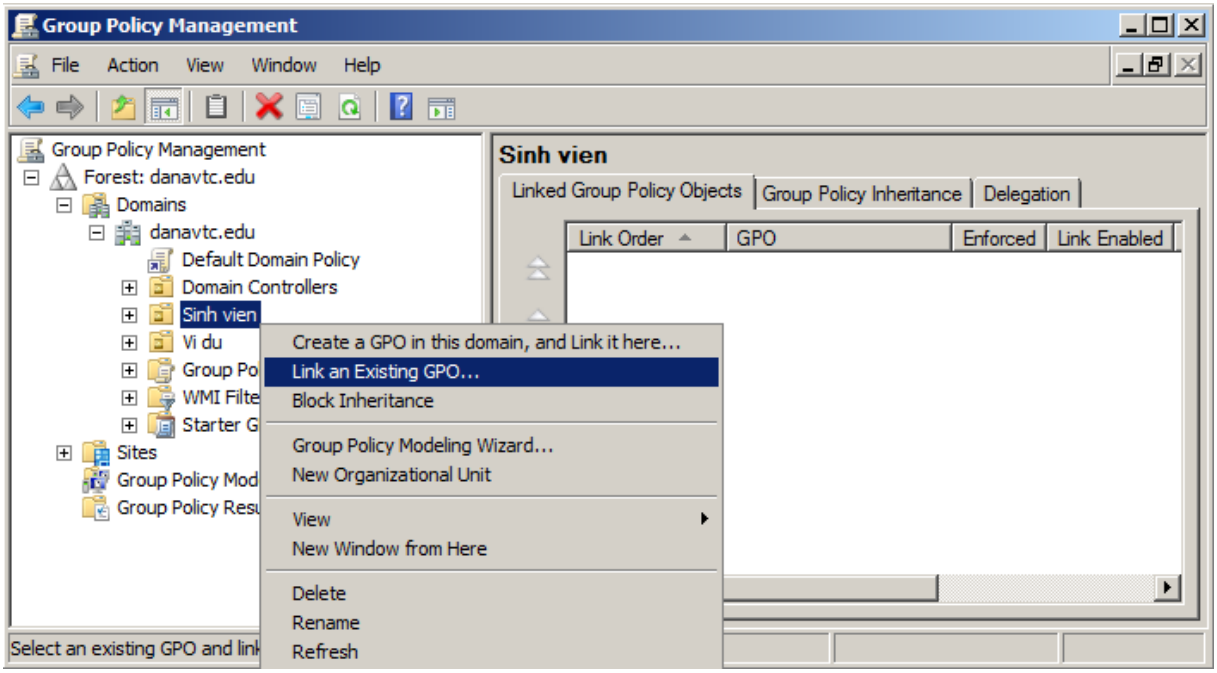


+ Khi xuất hiện cửa sổ New Object, gõ tên đối tượng vào (Sinh vien)

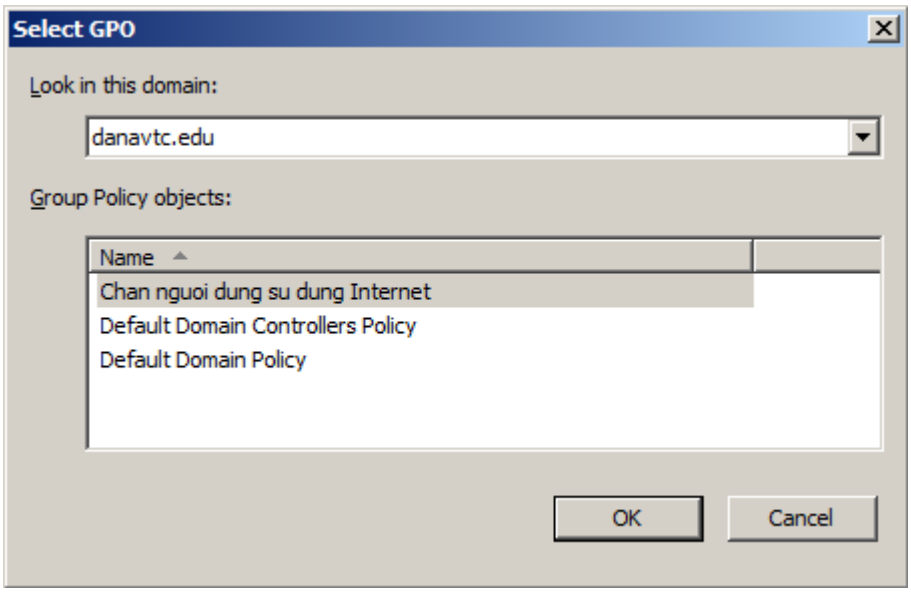


+ Tạo user và computer trong OU này (user SV1, V2)

+ Liên kết GPO vào OU: Vào Start → Adminitrative Tools → Group Policy Management; Nhấp chuột phải vào OU và chọn Link an Existing GPO



+ Trong hộp thoại Select GPO chọn tên domain ở mục Look in this domain; Đồng thời chọn GPO tương ứng (Chan nguoi dung su dung Internet) ở mục Group Policy objects.



+ Chọn OK để hoàn tất.

4. Sử dụng GPO để triển khai MS Office

Mục tiêu: Việc cài đặt các phần mềm (MS Office) trên từng máy lặp đi lặp lại là một công việc hết sức nhàm chán; để tránh điều này, có thể sử dụng GPO để triển khai phần mềm (bao gồm cả Product Key) trên Windows Server.

Cách thực hiện:

Bước 1: Sao chép đĩa cài đặt MS Office (2007) vào server và share (giả sử server là server1.

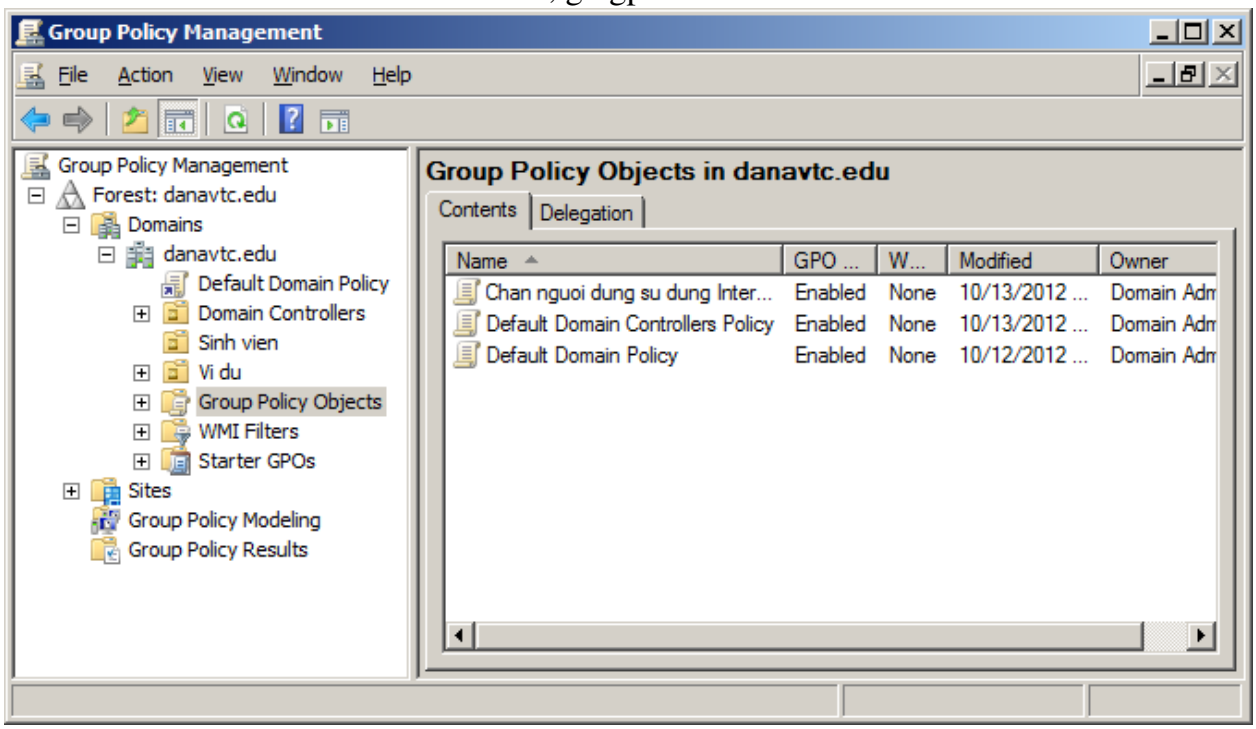
Bước 2: Tạo file Office2007.bat với nội dung (xem hỗ trợ từ http://technet.microsoft.com/en-us/library/cc179134%28v=office.12%29.aspx):

```
setlocal
set ProductName=Enterprise
set DeployServer=\\server1\Office2007
set ConfigFile=\\server1\Office2007\Enterprise.ww\config.xml
set Loglocation=\\server1\share\ Office2007Logs
IF NOT "%ProgramFiles(x86)%"=="" SET WOW6432NODE=WOW6432NODE\
Reg query HKEY_LOCAL_MACHINE\SOFTWARE\%WOW6432NODE%Microsoft\windows\CurentVersion\Uninstall\%ProductName%
If %errorlevel%==1 (goto DeployOffice) else (goto End)
:DeployOffice
start /wait %DeployServer%\setup.exe /config %ConfigFile%
echo %date% %time% Setup ended with error code %error level%. >> %loglocation%\%computername%.txt
:End
Endlocal
```

Bước 3: Mở file config.xml (trong notepad) và sửa các thông tin để cài đặt tự động (xem hỗ trợ từ http://technet.microsoft.com/en-us/library/cc179134%28v=office.12%29.aspx):

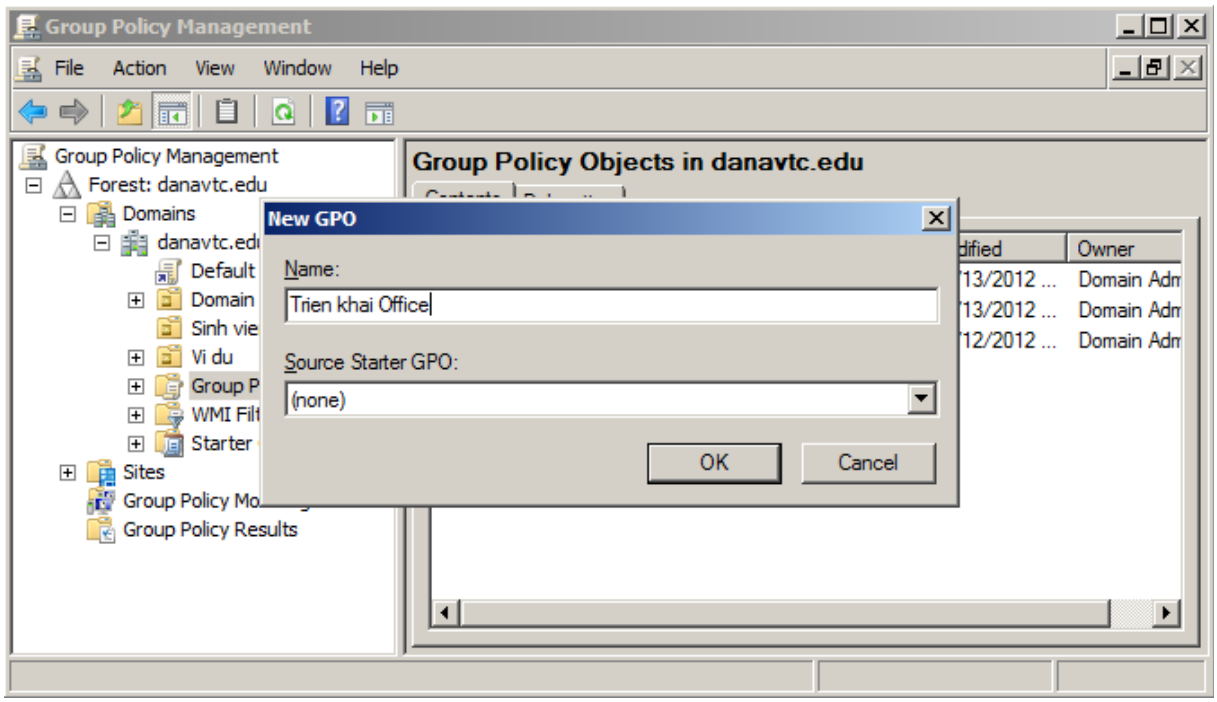
```
<Configuration Product="Enterprise">
<Display Level="none" CompletionNotice="no" SuppressModal="yes" AcceptEula="yes" />
<!-- <logging Type="Standard" Path="%temp%" Template="Microsoft Office Enterprise Setup(*).txt" /> -->
<PIDKEY Value="KGFVY7733B8WCK9KTG64BC7D8" />
<!-- <USERNAME Value="Customer" /> -->
<!-- <COMPANYNAME Value="MyCompany" /> -->
<!-- INSTALLLOCATION Value="%programfile%\Microsoft Office" /> -->
<!-- <LIS CACHEATION="CacheOnly" /> -->
<!-- <SOURCELIST Value="Server1\share\office12;\\server2\share\office12" /> -->
<!-- <DistributionPoint Location="Server\share\office12" /> -->
<!-- <OptionState Id="OptionID" State="absent" Children="force" /> -->
<!-- <Setting Id="Reboot" Value="IfNeeded" /> -->
<!-- <Command Path="msiexec.exe" Args="/i \\server\share\my.msi" QuietArg="/q" ChainPosition="after" Execute="install" /> -->
</Configuration>
```

Bước 4: Triển khai GPO: Start -> Run, gõ gpmc.msc

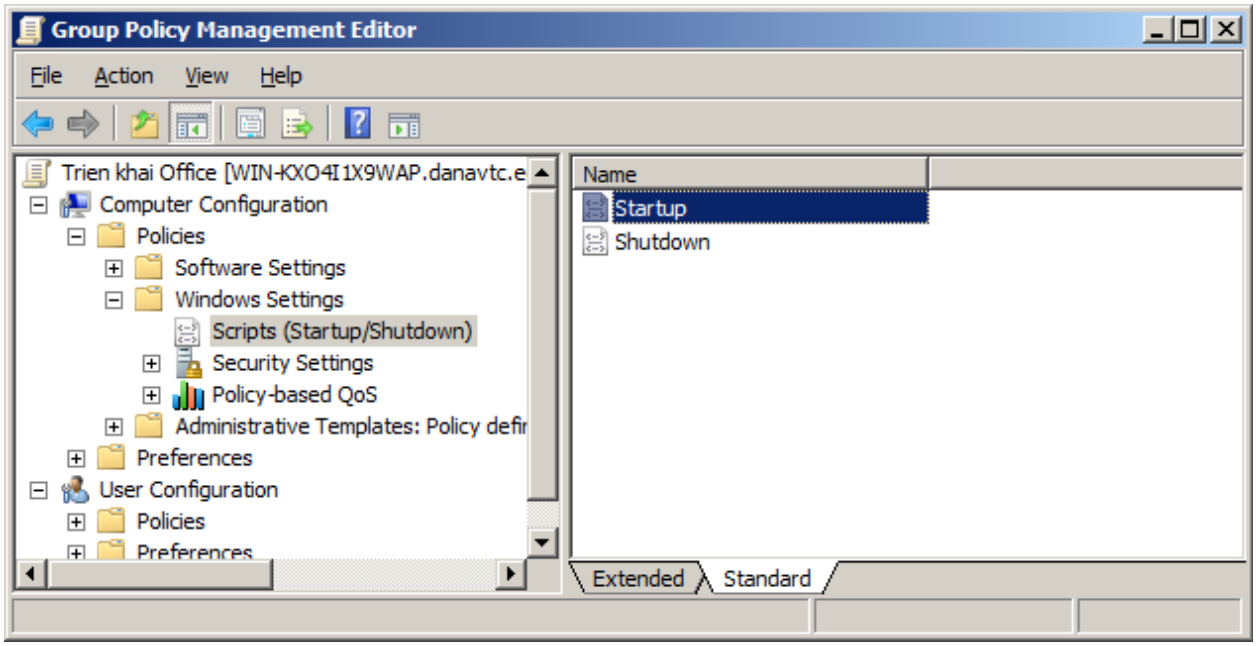


Tại cửa sổ Group Policy Management, nhấp chuột phải lên mục Group Policy Objects và chọn New

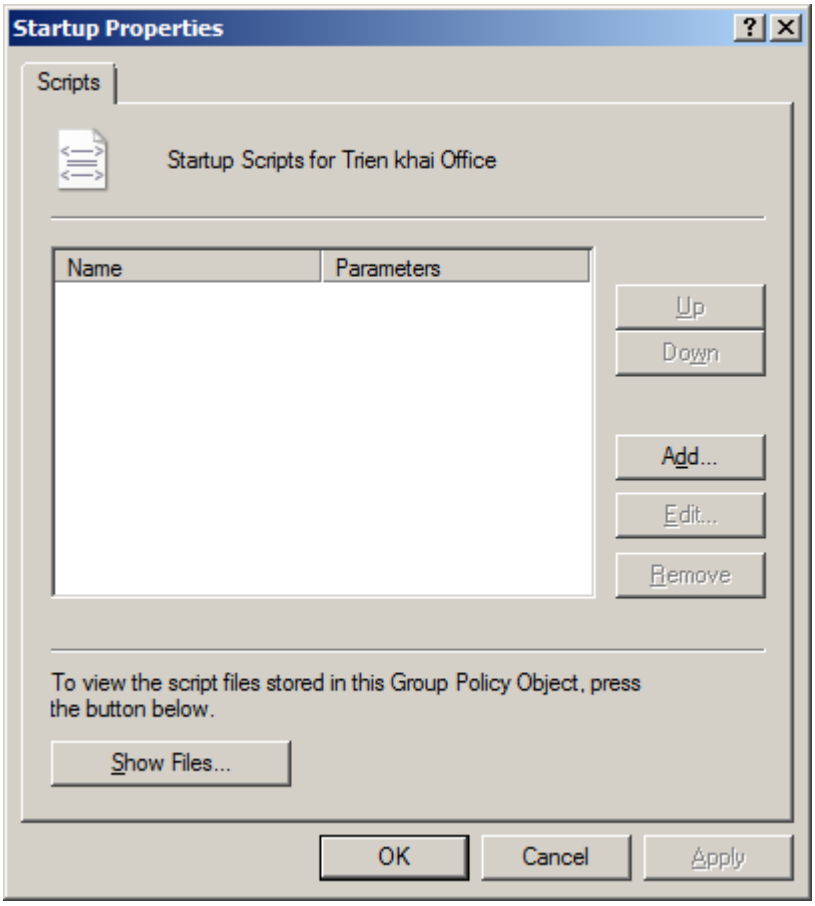
Tại hộp thoại Name GPO nhập tên GPO (Trien khai Office), chọn OK



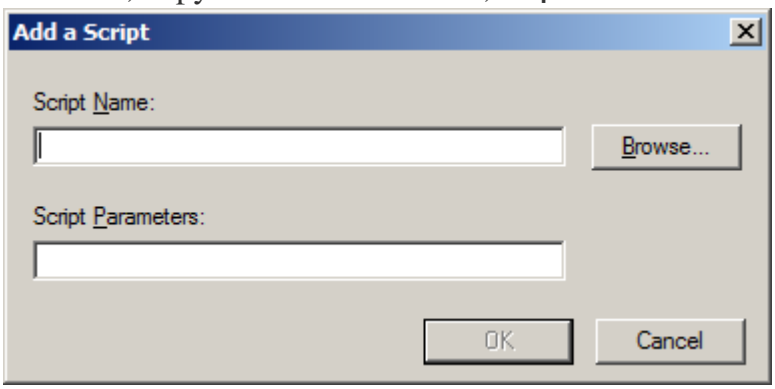
+ Trở lại cửa sổ Group Policy Management, nhắp phải chuột lên GPO vừa tạo, chọn Edit. Khi xuất hiện cửa sổ Group Policy Management Editor, chỉ định Polices cần cấu hình của Computer (chọn Computer Configuration / Policies / Windows Settings / Scripts).



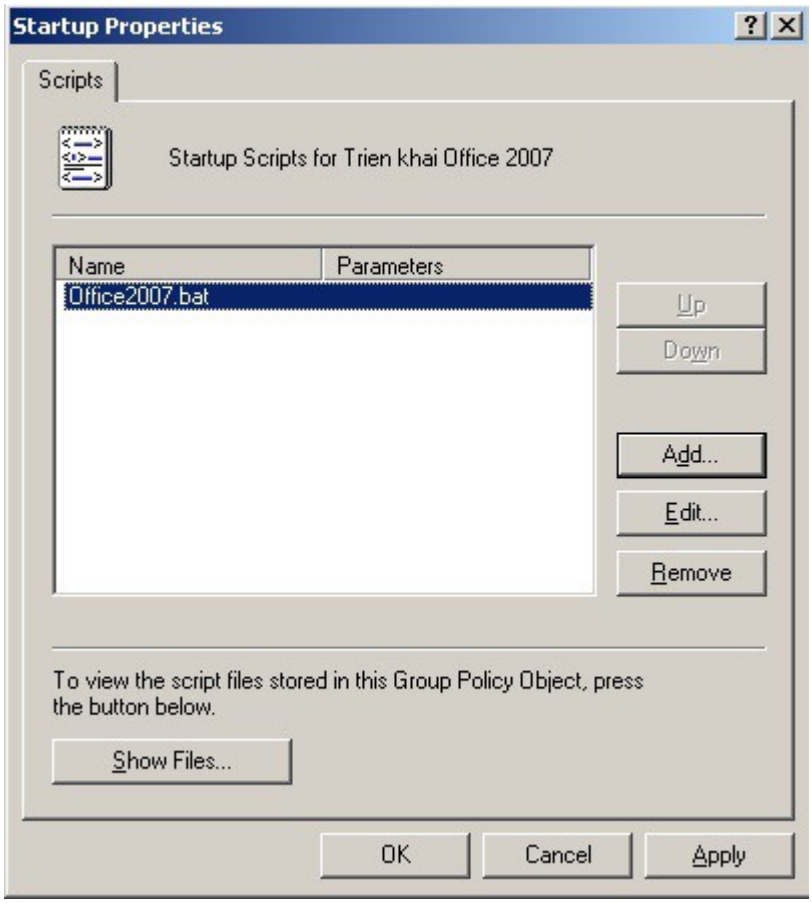
Nhắp phải chuột tại **Startup** (ở khung phải), **Properties**



Chọn **Show Files**, copy file Office2007.bat, chọn **Add**



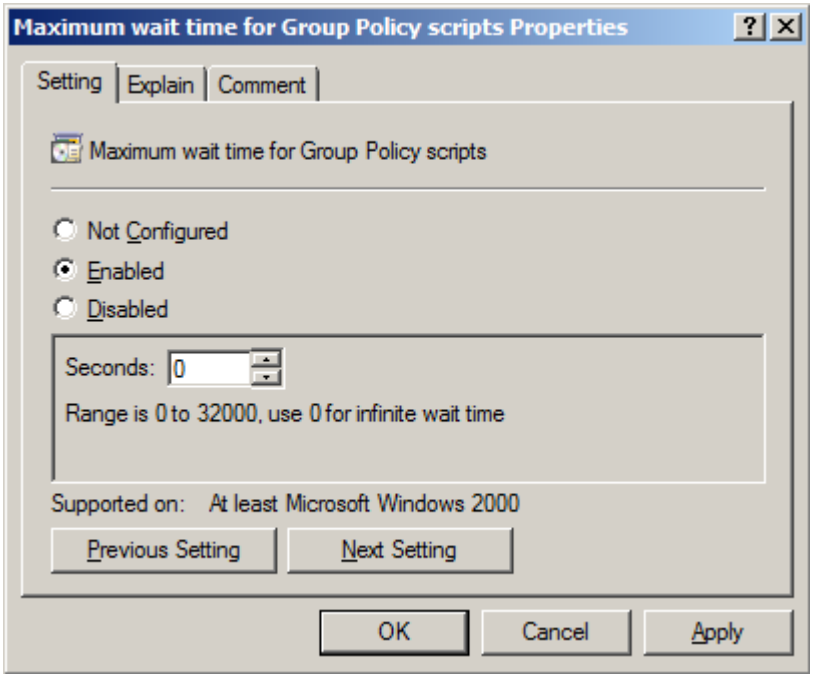
Chọn **Browse**



-> **Apply / OK**

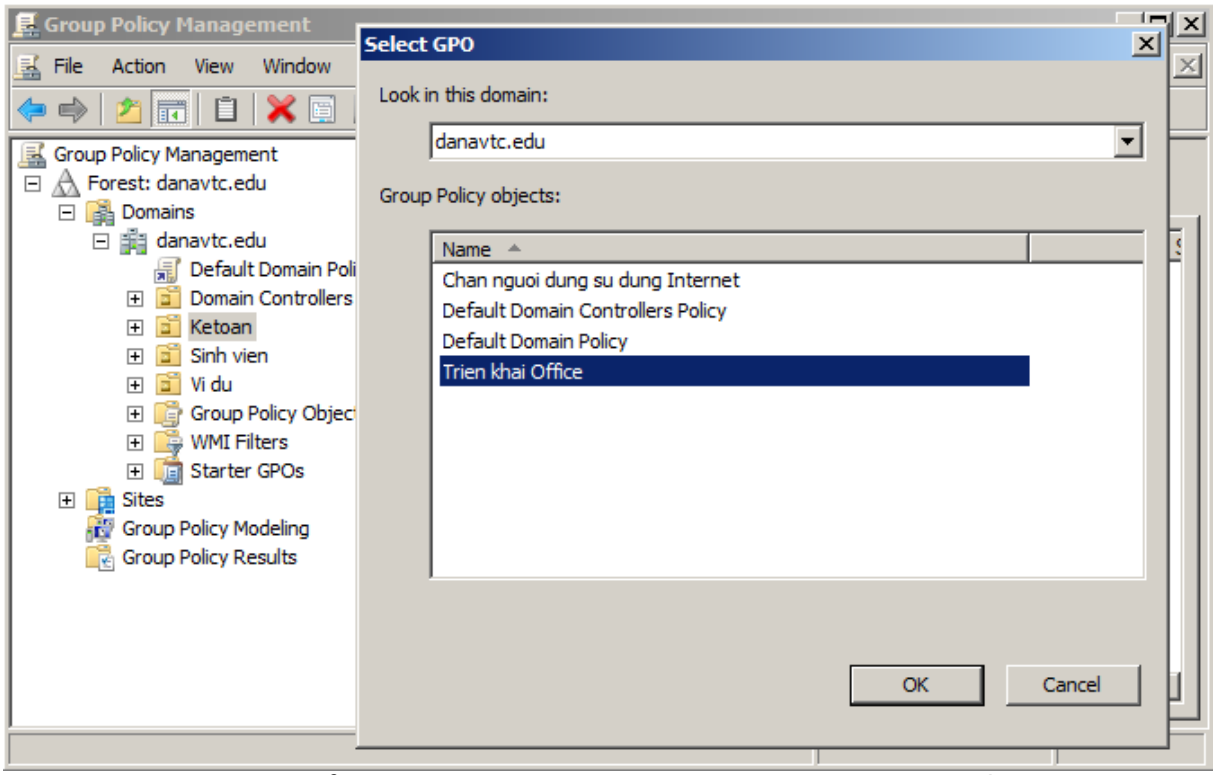
*** Chỉnh thời gian chờ cho group policy scripts**:

Computer Configuration / Administrative Templates / System / Scripts / Maximum wait time for group policy scripts, chọn Enabled và Seconds = 0

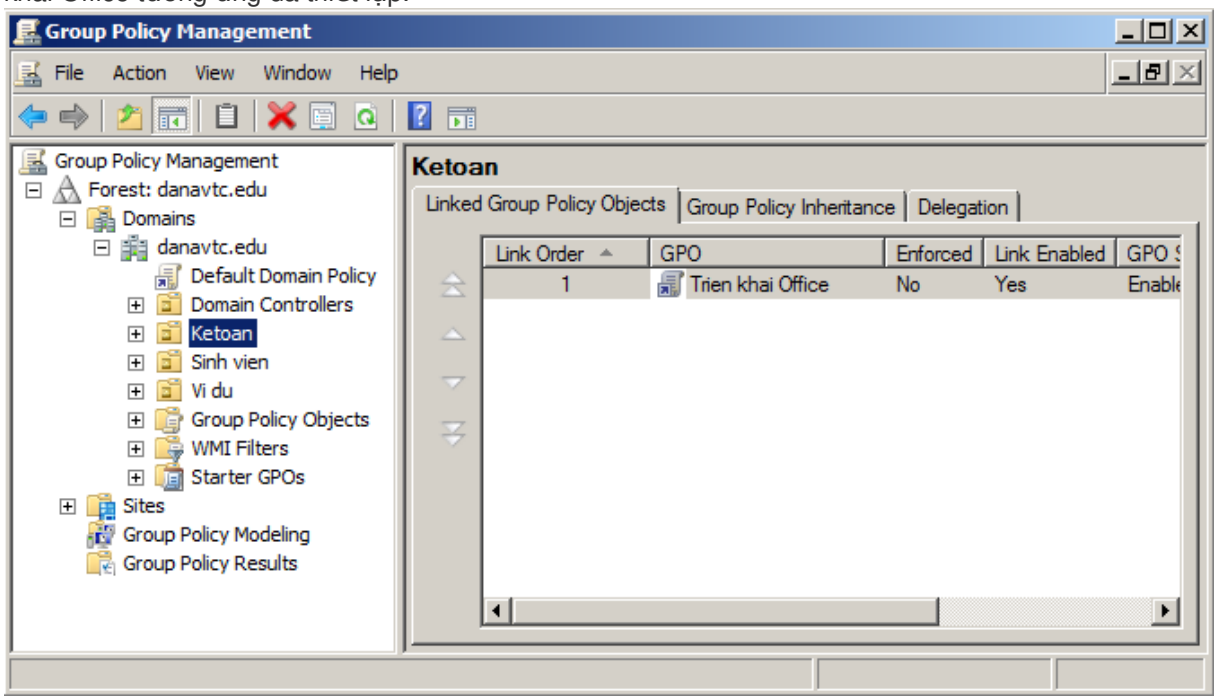


*** Triển khai cài đặt Office cho OU Ketoan:**

- Di chuyển các computer cần cài đặt Office 2007 vào OU Ketoan.
- Chọn OU Ketoan và Link an Existing GPO…



Lúc này, tại cửa sổ Group Policy Management, trong OU Ketoan, sẽ xuất hiện GPO Trien khai Office tương ứng đã thiết lập.



Câu hỏi

1. So sánh System Policy và Group Policy.

2. Trình bày các chức năng chính của Group Policy.

Bài tập thực hành

1. Xem chính sách cục bộ của một máy tính ở xa (PC01)

Để xem một chính sách cục bộ trên các máy tính khác trong miền, người xem phải có quyền quản trị trên máy đó hoặc quản trị miền.

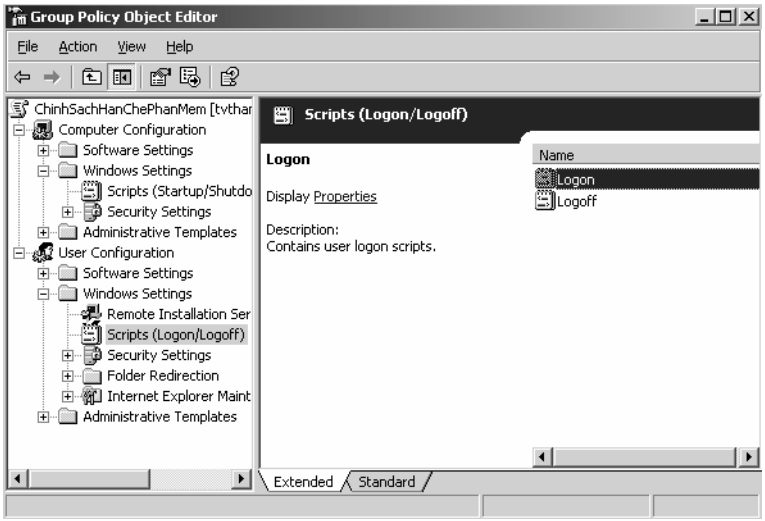
- Xem chính sách trên máy PC01, gõ lệnh GPEDIT.MSC /gpcomputer: PC01.

2. Khai báo logon script dùng chính sách nhóm

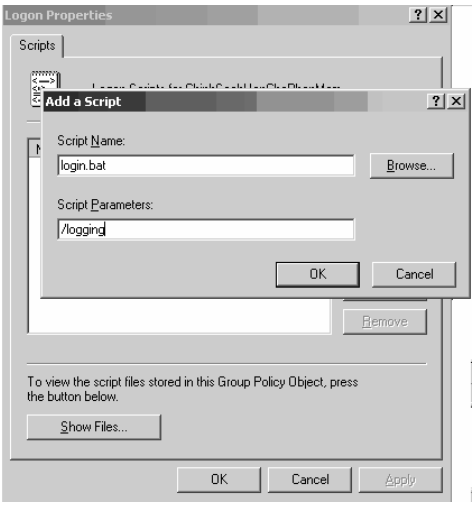
Tạo một logon script

Các bước thực hiện:

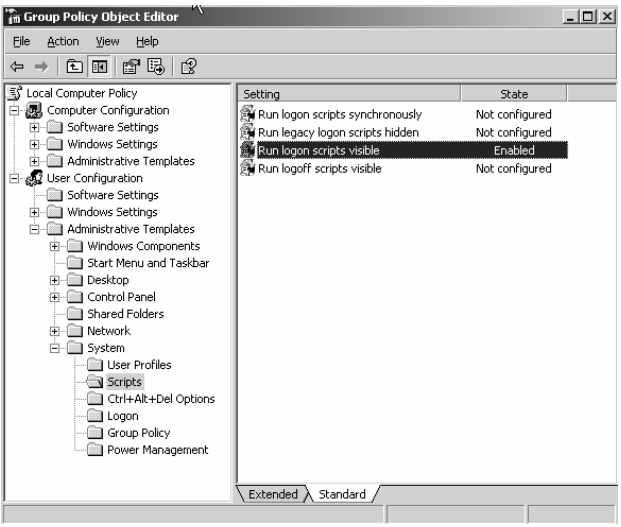
- Mở Group Policy Object Editor, vào User Configuration\ Windows Setttings\ Scripts.



- Nhấp đúp chuột vào mục Logon bên của sổ bên phải. Trong hộp thoại xuất hiện, nhấp chuột vào nút Add để khai báo tên tập tin kịch bản cần thi hành khi đăng nhập. Chú ý tập tin kịch bản này phải được chứa trong thư mục c:\windows\ system32\ grouppolicy\ user\ script\ logon. Thư mục này có thể thay đổi, tốt nhất nên nhấp chuột vào nút Show Files phía dưới hộp thoại để xem thư mục cụ thể chứa các tập tin kịch bản này (Nội dung tập tin kịch bản có thể thay đổi tùy theo yêu cầu)



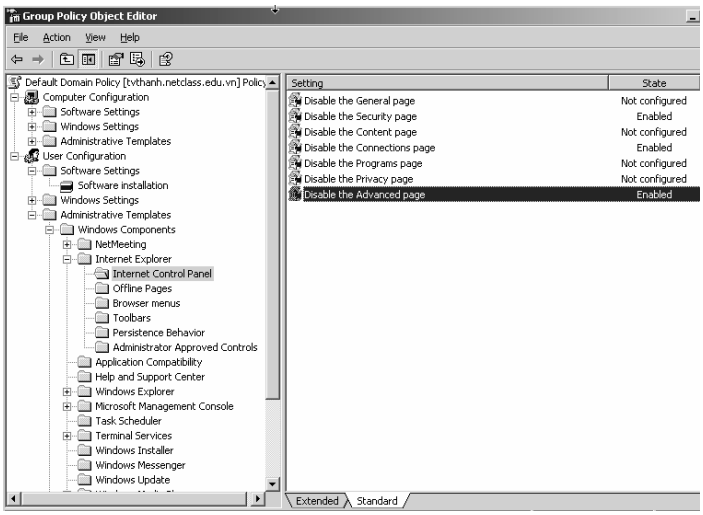
- Để kiểm soát quá trình thi hành của tập tin kịch bản, cần hiệu chỉnh chính sách Run logon scripts visible ở trạng thái Enable. Trạng thái này giúp phát hiện ra các lỗi phát sinh khi tập tin kịch bản thi hành từ đó chúng ta có thể sửa chữa. Để thay đổi chính sách này, nhấp chuột vào mục User Configuration\ Administrative Templates \ System \ Scripts, sau đó nhấp đúp chuột vào mục Run logon scripts visible để thay đổi trạng thái.



3. Hạn chế chức năng của Internet Explorer

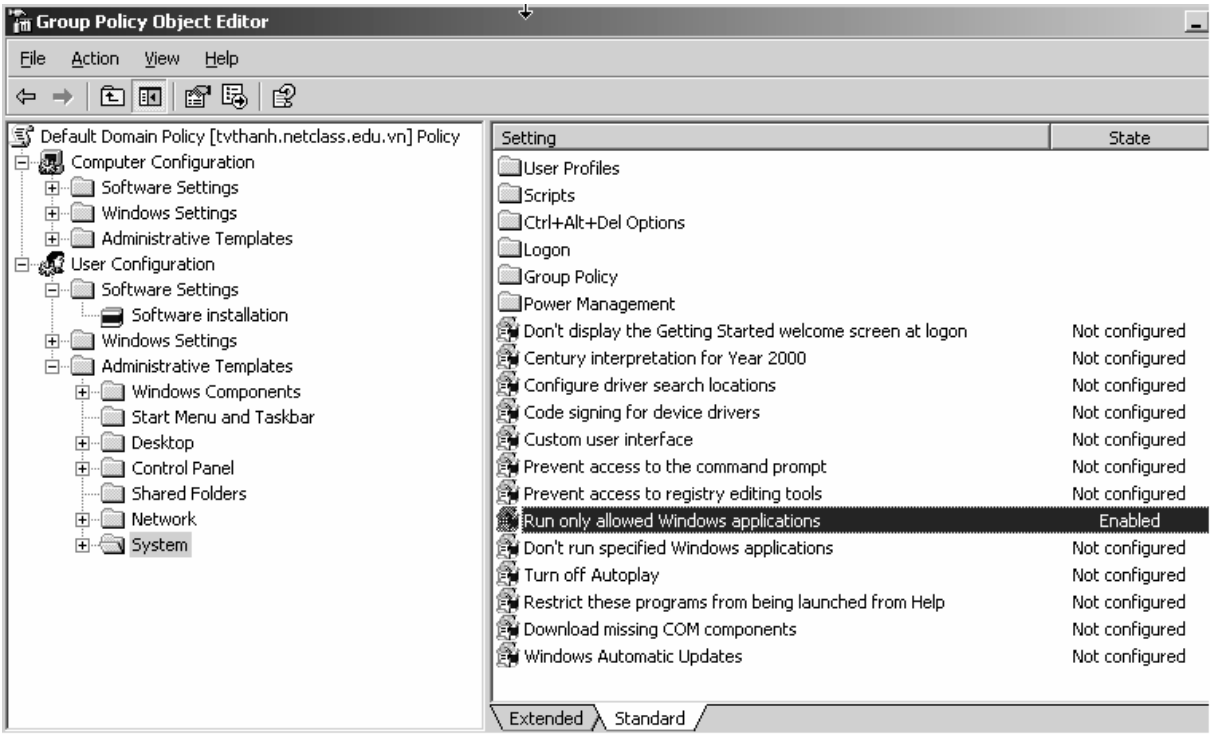
Để người dùng máy trạm không được phép thay đổi bất kì thông số nào trong Tab Security, Connection và Advanced trong hộp thoại Internet Options của công cụ Internet Explorer.

- Trong công cụ Group Policy Object Editor, vào User Configuration\ Administrative Templates\ Windows Components\ Internet Explorer\ Internet Control Panel ; chương trình sẽ hiện ra các mục chức năng của IE có thể giới hạn, chọn khóa các chức năng cần thiết.



4. Chỉ cho phép một số ứng dụng được thi hành

Trong công cụ Group Policy Object Editor, vào User Configuration\ Administrative Templates. Sau đó nhấp đúp chuột vào mục Run only allowed windows applications để chỉ định các phần mềm được phép thi hành.



BÀI 6: GIỚI THIỆU VỀ ISA SERVER

Mã bài: MĐ 36-06

Mục tiêu của bài:

- Trình bày được tầm quan trọng của ISA Server trong việc bảo vệ hệ thống mạng;
- Hiểu được các tính năng trên ISA Server;
- Hiểu được khái quát các khả năng và nét đặc trưng của ISA Server;
- Thực hiện các thao tác an toàn với máy tính.

1. Định nghĩa Firewall

Mục tiêu: Trình bày khái niệm về Firewall và chức năng của Firewall.

Firewall - Tường lửa dùng để ngặn chặn và bảo vệ những thông tin và chống việc truy cập bất hợp pháp của các hacker. Firewall là một giải pháp dựa trên phần cứng và phần mềm dùng để kiểm tra dữ liệu đi từ bên ngoài vào máy tính hoặc từ máy tính ra ngoài mạng Internet. Có thể nói Firewall là người bảo vệ có nhiệm vụ kiểm tra "giấy thông hành" của bất kì gói dữ liệu đi vào hoặc đi ra. Nó chỉ cho phép những gói dữ liệu hợp lệ đi qua và loại bỏ tất cả các gói dữ liệu không hợp lệ. Vì vậy, Firewall rất cần thiết cho hệ thống mạng.

2. Phân loại Firewall

Mục tiêu: Trình bày các loại firewall và một số firewall thông dụng.

2.1. Firewall phần mềm

Firewall phần mềm được sử dụng cho các hệ điều hành Windows. Firewall phần mềm thường không đắt bằng phần cứng. So với Firewall phần cứng, Firewall phần mềm linh động hơn, nó có thể chạy tốt trên nhiều hệ điều hành khác nhau. Một trong những Firewall phần mềm phổ biến là Zonealarm, ISA.

2.2. Firewall phần cứng

Firewall phần cứng có mức độ bảo vệ cao hơn so với Firewall phần mềm, dễ bảo trì hơn và không chiếm dụng tài nguyên hệ thống như Firewall phần mềm. Một trong những hãng chuyên cung cấp Firewall phần cứng là Linksys và NetGar.

2.3. Bộ định tuyến không dây

Bộ định tuyến không dây được sử dụng cho mạng không dây. Nó được xem như một Firewall và cũng được tích hợp một số chức năng tương tự như Firewall.

3. Chức năng của Firewall

Mục tiêu: Giới thiệu đến người học các chức năng chính của firewall.

- Kiểm soát nguồn thông tin giữa mạng Internet và máy tính;

- Cho phép hoặc không cho phép các dịch vụ truy cập từ hệ thống ra bên ngoài;

- Cho phép hoặc cấm cho phép các dịch vụ truy cập từ ngoài vào hệ thống;

- Chức năng theo dõi luồng dữ liệu mạng giữa Internet và máy tính nối mạng;

- Kiểm soát địa chỉ truy cập của người dùng và nội dung nhận được từ Internet;

- Chống lại những đợt truy cập bất hợp pháp của các hacker.

4. Các kiến trúc Firewall cơ bản

Mục tiêu: Trình bày cơ sở xây dựng các lại firewall, kiến trúc, cách hoạt động của các firewall cơ bản cùng với các ưu, nhược điểm của các firewall cơ bản.

Khi nói đến việc lưu thông dữ liệu giữa các mạng với nhau thông qua firewall thì điều đó có nghĩa rằng firewall hoạt động kết hợp chặt chẽ với giao thức TCP/IP. Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DSN, SMNP, NFS,…) thành các gói dữ liệu (data packets) rồi gán cho các packet này những địa chỉ để có thể nhận dạng tái lập lại ở đích cần gửi đến; Do đó, các loại firewall cũng liên quan rất nhiều đến các packet và địa chỉ của chúng. Ngày nay, Firewall được xây dựng dựa trên cơ sở bộ lọc gói (packet filter) và Firewall xây dựng trên cổng ứng dụng (Application gateway) và một số firewall khác Bastion Host Firewall (pháo đài phòng ngự)

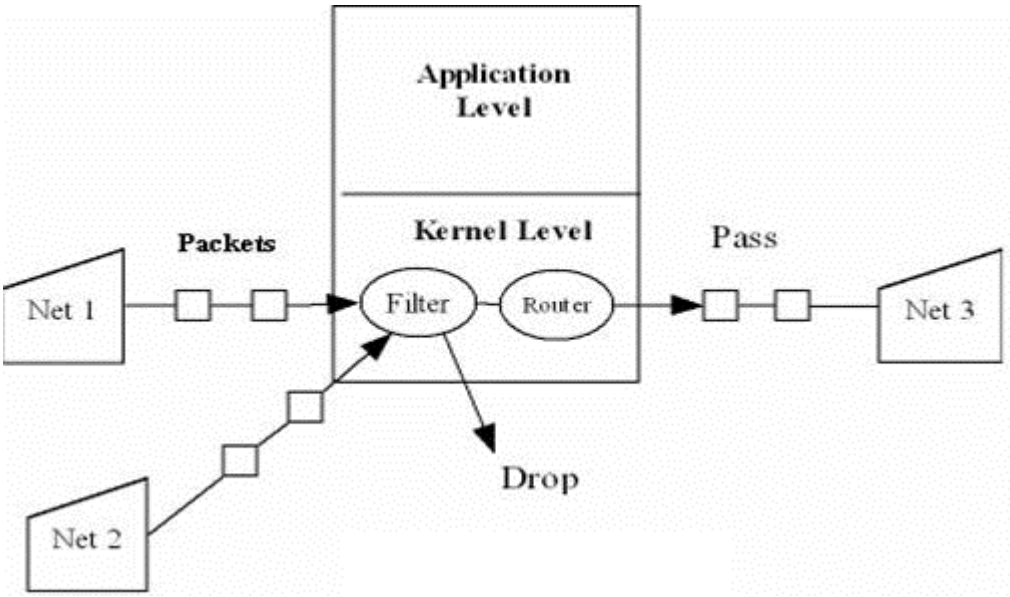
4.1. Tường lửa bộ lộc gói tin (Packet filtering firewall)

Loại firewall này thực hiện việc kiểm tra số nhận dạng địa chỉ của các packet để cho phép chúng có thể lưu thông qua lại hay không. Các thông số có thể lọc được của một packet như sau:

- Địa chỉ IP nơi xuất phát (source IP address);
- Địa chỉ IP nơi nhận (destination IP address);
- Cổng TCP nơi xuất phát (TCP source port) ;
- Cổng TCP nơi nhận (TCP destination port).

Nhờ vậy mà firewall có thể ngăn cản được các kết nối vào những máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống nội bộ từ những địa chỉ không cho phép.

Hơn nữa việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP,…) được phép mới chạy được trên hệ thống mạng nội bộ.



Hình 6.1 – Tường lửa bộ lọc gói

4.2. Cổng tầng ứng dụng (Application gateway)

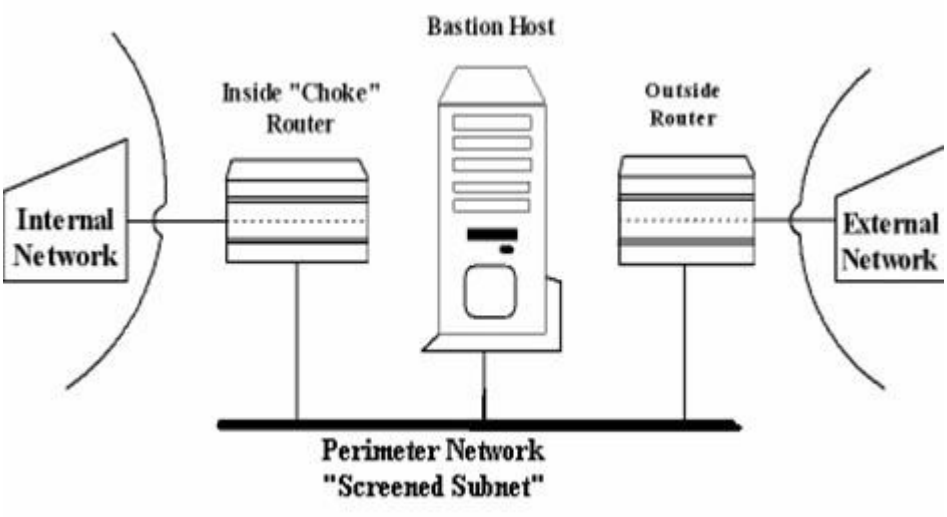
Cổng tâng ưng dụng la`một thiết bị bình phong bảo mật dung để phân tích cać goí dư liệu được chuyển vaò. Khi cać goí dư liệu tư`bên ngoaì đến cổng, chung được kiểm tra va`lượng gia´để xać định xem chính sać bảo mật co´cho phep chung vaò mạng hay không. Maý phục vụ không chỉ định gia´trị cać địa chỉ IP ma`coǹ xem xeť dư liệu trong cać goí để tim lôĩ va`sửa sai.

Một cổng tâng ưng dụng điển hình co´thể cung câp cać dịch vụ ủy quyên cho cać ưng dụng va`giao thưć như Telnet, FTP (File Transfer Protool), HTTP (HyperText Transfer Protocol), va`SMTP (Simple Mail Transfer Protocol). Cổng ứng dụng này không cho phép bất kỳ một gói tin nào đi thẳng trực tiếp giữa hai mạng, mà loại Firewall này được thiết kết để tăng cường khả năng kiểm soát thông qua dịch vụ Proxy. Khi một trạm bên ngoài muốn kết nối với các trạm bên trong tường lửa thông qua một dịch vụ nào đó thì trạm bên ngoài phải thông qua dịch vụ Proxy. Nếu dịch vụ bên ngoài không thuộc diện cấm thông qua đối với Proxy thì dịch vụ Proxy sẽ đi tìm trạm đích bên trong tường lửa để tạo kết nối với trạm bên ngoài; ngược lại các trạm bên trong muốn kết nối ra ngoài cũng vậy. Với cách thức này sẽ ngăn chặn được một số loại tấn công cơ bản như gây tràn bộ đệm của tường lửa.

Tuy nhiên cũng có một số hạn chế đối với dạng tường lửa loại này là: Đây là loại tường lửa được cài đặt cho từng loại dịch vụ riêng rẽ trên mạng ví dụ như Telnet, Mail, FPT… Nếu chúng ta muốn hỗ trợ một dịch vụ nào đó cho mạng của mình thông qua tường lửa thì chúng ta nhất thiết phải thêm vào proxy cho loại dịch vụ đó. Vì vậy nếu trên mạng bên ngoài có thêm một dịch vụ mới nào đó thì người quản trị tường lửa phải xây dựng chính sách đại diện thích hợp với dịch vụ đó. Có hai nguyên tắc để tạo ra chính sách đại diện mặc định ở đây đó là hoặc từ chối tất cả những thứ không được đại diện, hoặc là chấp nhận tất cả những dịch vụ không có dịch vụ đại diện trên tường lửa. Nhưng cả hai cách này đều gây ra những nguy cơ an ninh và bất tiện mới cho hệ thống mạng bên trong tường lửa.

4.3. Bastion Host Firewall (Pháo đài phòng ngự)

Bastion Host Firewall là một trạm được cấu hình để chặn đứng mọi cuộc tấn công từ phía bên ngoài vào. Đây là điểm giao tiếp trực tiếp với mạng không tin cậy bên ngoài, do đó dễ bị tấn công nhất. Có hai dạng của máy phòng thủ:



Hình 6.2 – Bastion Host Firewall

Máy phòng thủ có hai card mạng, một nối với hệ thống bên trong (mạng nội bộ) và card còn lại nối với bên ngoài mạng Internet. Đây là dạng tường lửa có từ rất sớm, nó yêu cầu người sử dụng bên trong phải kết nối với tường lửa trước khi làm việc với mạng bên ngoài. Với giải pháp này tường lửa đã cô lập được mạng bên trong với mạng bên ngoài bằng những máy phòng thủ (host) nhưng nó cũng tạo ra một sự thiếu tự nhiên trong việc kết nối giữa người sử dụng bên trong với mạng bên ngoài.

Dạng thứ hai của cơ cấu phòng thủ này là máy phòng thủ có một card mạng được nối trực tiếp đến một hệ riêng biệt trên mạng – gateway mức ứng dụng. Gateway này cung cấp điều khiển vào ra. Bộ định tuyến (rounter) có nhiều chức năng trong cấu hình này. No´không chỉ định hương cac goi đên hệ nội bộ, ma`còn cho phep cac hệ thông nội mở kêt nôi vơi Internet hoặc không cho phep kêt nôi. Kiến trúc screening subnet còn bổ sung thêm tầng an toàn để tách mạng nội bộ với Internet. Lý do để làm việc này là tránh cho mạng nội bộ khỏi bị tấn công nếu như bastion host bị đánh sập.

5. Giới thiệu về ISA server

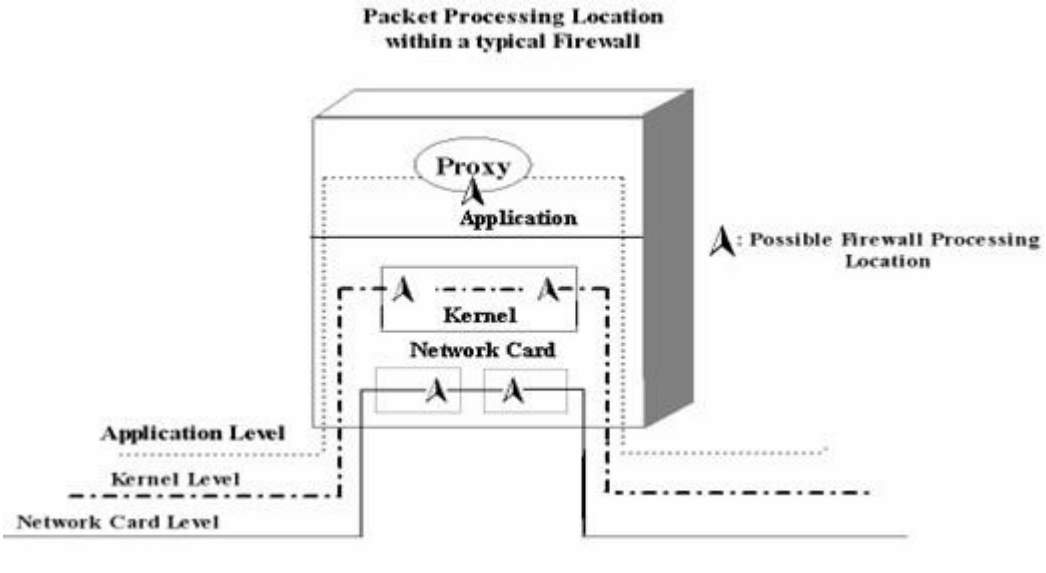
Mục tiêu: Trình bày các hoạt động chính của tường lửa: điều khiển truy nhập (Access control), quản lý xác thực (Authentication) và ghi nhật ký truy nhập (activity logging)

Như trên đã giới thiệu có hai loại tường lửa với 2 cách điều khiển truy nhập khác nhau là quy chế bộ lọc gói (packet filter) và chính sách người đại diện ứng dụng. Điểu khiển truy nhập phụ thuộc vào sự nhận dạng đúng đắn của các yêu cầu đôi khi còn phụ thuộc vào định nghĩa quyền xác thực của người sử dụng.

5.1. Điều khiển truy nhập (Access Control)

5.2. Vị trí xảy ra quá trình xử lý gói

Để hiểu được firewall hoạt động như thế nào, trước hết hãy quan tâm đến đường đi của các gói tin dẫn đến firewall đó. Có 3 đường dẫn phổ biến mà một gói tin có thể đi qua tùy thuộc vào dạng tường lửa được cài đặt. Một gói tin có thể vượt qua một tường lửa ở mức tầng ứng dụng, ở mức nhân hệ điều hành hoặc là mức card giao tiếp mạng. Hầu hết các tường lửa đều kiểm soát và cho phép các gói đi qua 3 mức này.



Hình 6.3 – 3 đường đi phổ biến mà một gói tin có thể đi qua

Để có được tốc độ xử lý cao hơn ở các router, bộ lọc gói được thiết lập trên phần mở rộng của thiết bị trên card giao tiếp mạng với một bộ xử lý đặc biệt tối ưu quá trình xử lý các gói. Để lưu chứa ở đây với tốc độ cao bộ xử lý trên card giao tiếp mạng chỉ hỗ trợ những luật xử lý đơn giản như các phép so sánh nhị phân. Những dịch vụ khác không được hỗ trợ ở đây.

Những router và những trạm luân chuyển gói khác thì quá trình lọc các gói tin thường diễn ra ở mức nhân hệ điều hành hơn là mức card giao tiếp mạng. Thông thường quá trình lọc được thực thi trên các bộ xử lý chuyên dụng cho phép tường lửa có thể thực hiện quá trình lọc và kiểm định một cách chuẩn xác, tinh xảo hơn là trên các card giao tiếp mạng tích hợp tính lọc. Hơn nữa quá trình xử lý các gói tại mức nhân hệ điều hành nhanh hơn ở mức tầng ứng dụng bởi vì quá trình lập lịch và tràn bộ nhớ được tránh. Tuy nhiên quá trình xử lý nhân thường đòi hỏi tất cả các thông tin cần thiết cho việc lọc gói phải được chứa trong bộ nhớ thay vì trên đĩa. Một gói phải được xử lý và được cho qua mà không cần phải đợi trên đĩa điều này sẽ làm hạn chế các dạng gói và số lượng các gói được xử lý ở mức này.

Quá trình xử lý ở mức tầng ứng dụng có thể cung cấp một chính sách an ninh tốt nhất. Mức ứng dụng có thể truy cập đến tất cả các tài nguyên hệ thống bao gồm đĩa, card mạng, bộ nhớ, thư viện các chương trình và cả những tiến trình khác. Tầng ứng dụng là tầng trên cùng trong cấu trúc phân tầng của giao thức mạng, do đó nó không bị giới hạn bởi các tầng thấp hơn nó.

Hoạt động lọc gói (Packet Filtering)

Hoạt động lọc các gói có thể diễn ra ở một trong 3 mức xử lý gói như trên đã trình bày nhưng nó thường được hỗ trợ ở mức card giao tiếp mạng hoặc mức nhân hệ điều hành. Một bộ lọc gói sẽ căn cứ vào phần địa chỉ IP chứa trong gói tin để quyết định xem gói đó có được cho phép vượt qua hay bị chặn lại. Gói được cho qua sẽ được chuyển đến trạm đích hoặc router tiếp theo. Gói bị chặn lại sẽ bị loại bỏ.

5.3. Luật lọc (Filtering Rules)

Bộ lọc sẽ kiểm tra 5 mảng thông tin trong khối IP ở phần đầu của gói tin. Các thông tin đó được mô tả như trong bảng 6.1:

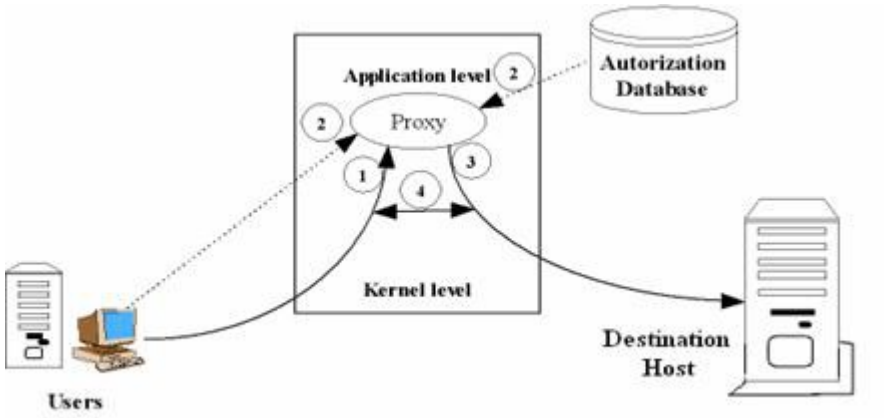
BẢNG 6.1: thông tin trong khối IP ở phần đầu của gói tin

Field	Purpose
Source IP address	Địa chỉ IP của trạm nguồn gửi gói tin
Destination IP address	Địa chỉ IP của trạm đích gói tin sẽ đi tới
Upper level Protocol (đó là TCP hoặc UDP)	Cho giao thức khác và dịch vụ khác
TCP or UDP source port number	Số hiệu cổng của trạm nguồn gửi gói ra
TCP or UDP destination port number	Số hiệu cổng của trạm dích sẽ nhận gói tin

Khi có được các thông tin trên của các gói, bộ lọc sẽ so sánh chúng với một tập hợp các luật để đưa ra quyết định. Một luật lọc là sự kết hợp một giá trị hoặc miền giá trị của mỗi trường thông tin trên và quyết định sẽ được đưa ra nếu tất cả các thông tin của gói được so khớp với các thông tin của các luật. Một bộ lọc gói sẽ thực hiện việc kiểm tra sự hợp lệ của các gói rất đơn giản và rất nhanh chỉ bằng các phép so sánh nhị phân. Quyết định (cho phép hoặc cấm) sẽ được đưa ra ngay sau khi bộ lọc tìm thấy một luật nào đó hoàn toàn so khớp với thông tin mà nó có được về gói tin do đó trật tự sắp xếp các luật cũng rất quan trọng nó góp phần làm cho quá trình lọc được nhanh hơn.

Có một điều đáng quan tâm ở đây đó là danh sách luật là hữu hạn và ta không thể lường hết được các tình huống để đưa ra tất cả các luật được vì vậy phải có một luật mặc định ở đây để nếu như khi xem xét hết tất cả các luật trong danh sách luật rồi mà bộ lọc vẫn không thể đưa ra được quyết định thì luật mặc định này sẽ giúp bộ lọc đưa ra quyết định. Có 2 ý tưởng chủ đạo trong việc tạo ra luật mặc định này đó là hoặc là từ chối tất cả hoặc chấp nhận tất cả, có nghĩa là tất cả các gói có thông tin không thỏa mãn tập luật thì bị từ chối cho qua hoặc chấp nhận cho qua hết.

5.4. Hoạt động của tường lửa người đại diện ứng dụng (Proxy Application)



Hình 6.4 – Hoạt động của tường lửa người đại diện ứng dụng (Proxy Application)

Như mô tả trên hình 6.4, người sử dụng trước hết phải thiết lập một kết nối đến người đại diện ứng dụng trên tường lửa (1). Đại diện ứng dụng này sẽ tập hợp các thông tin liên quan đến mối liên kết và yêu cầu của người sử dụng (2). Tường lửa sẽ sử dụng thông tin này để quyết định liệu yêu cầu có được cho phép thực thi hay không. Nếu yêu cầu từ phía người dùng là thỏa đáng thì người đại diện trên tường lửa sẽ tạo một kết nối khác từ tường lửa đến đích dự kiến (3). Sau đó người đại diện sẽ đóng vai trò như một con thoi để truyền tải dữ liệu giữa 2 mối kết nối (4).

Có 2 điểm cần lưu ý ở đây là:

• Thứ nhất, kết nối đầu tiên phải được thiết lập đến người đại diện trên tường lửa thay vì nối trực tiếp đến trạm mong muôn kết nối.

• Thứ hai, người đại diên trên tường lửa phải có được địa chỉ IP của trạm đích.

Trước khi người sử dụng hoặc một ứng dụng nào đó muốn kết nối đến người đại diên ứng dụng thì phải thiết lập kêt nối đến tường lửa, kết nối này phải sử dụng phương pháp chuẩn để cung cấp tên hoặc địa chỉ IP của trạm đích mong muốn. Đây không phải là một công việc dễ dàng vì giao thức tầng ứng dụng luôn cố định và thường không hỗ trợ sự vượt qua của những thông tin được thêm vào. Để khắc phục đặc điểm này có rất nhiều giải pháp bắt buộc người sử dụng và các ứng dụng phải tuân theo.

Kết nối trực tiếp

Đây là giải pháp đầu tiên cho phép người sử dụng thiết lập kết nối trực tiếp đến tường lửa thông qua địa chỉ và số hiệu cổng người đại diện sau đó người đại diện sẽ hỏi người sử dụng để biết được địa chỉ của trạm mong muốn kết nối. Đây là một phương pháp thô được sử dụng bởi nhưng tường lửa sơ khai vì thế không được ưa dùng.

Sử dụng chương trình hỗ trợ máy khách

Giải pháp tiếp theo sử dụng trong việc cài đặt người đại diện là phải có một chương trình hỗ trợ đặt trên máy của người sử dụng. Người sử dụng sẽ chạy ứng dụng đặc biệt để tạo kết nối đến tường lửa. Người sử dụng chỉ việc cung cấp địa

chỉ hoặc tên của trạm đích cho ứng dụng bổ trợ. Địa chỉ tường lửa sẽ được ứng dụng bổ trợ này lấy ra từ file cấu hình cục bộ sau đó nó sẽ thiết lập kết nối đến người đại diện trên tường lửa. Giải pháp này tỏ ra hữu hiệu và trong suốt đối với người sử dụng; tuy nhiên, hạn chế của nó là mỗi chương trình hỗ trợ máy khách chỉ thực hiện tương ứng với một dịch vụ nào đó của mạng mà thôi.

Sử dụng người đại diện tàng hình

Một phương pháp nữa được sử dụng hiện nay cho việc kết nối đến đại diện ứng dụng trên tường lửa là sử dụng đại diện tàng hình (ẩn). Với giải pháp này thì người sử dụng không cần đến chương trình hỗ trợ máy khách hoặc kết nối trực tiếp đến tường lửa. Ở đây người ta sử dụng phương pháp dò đường căn bản, mọi kết nối đến các mạng bên ngoài đều phải định hướng thông qua tường lửa. Các gói khi vào trong tường lửa tự động sẽ đổi hướng đến một đại diện ứng dụng móng muốn. Ứng dụng đại diện có được địa chỉ trạm đích một cách chính xác bằng cách lấy địa chỉ trạm đích của phiên. Trong trường hợp này tương lửa giả mạo thành một trạm đích và chặn các phiên lại. Khi một kết nối được thiết lập đến đại diện trên tường lửa thì trình ứng dụng máy khách sẽ nghĩ rằng nó đang kết nối đến một trạm đích thật sự. Nếu được phân quyền thì đại diện ứng dụng trên tường lửa sẽ dùng một hàm đại diện để tạo ra liên kết thứ hai đến trạm đích thật.

5.5. Quản lý xác thực (User Authentication)

Đây là chức năng ngăn cản việc truy cập trái phép vào hệ thống mạng nội bộ. Các hệ điều hành quản lý mạng chỉ kiểm soát một cách không chặt chẽ tên người sử dụng và password được đăng ký, và đôi lúc chính người sử dụng được ủy nhiệm lại vô ý để lộ password của mình. Hậu quả của việc này có khi là rất nghiêm trọng. Nó càng trở nên quan trọng hơn đối với những hệ thống mạng lớn có nhiều người sử dụng. Có hai giao thức chuẩn thông dụng nhất hiện nay để kết hợp làm việc với LAN.

- RADIUS (Remote Authen-tication Dial-In User Service)
- TACAS+ (Terminal Access Controller Access Control System Extended)

Thông thường chức năng authentication được thực hiện với sự phối hợp của một thiết bị phần cứng hoặc phần mềm được tích hợp sẵn bên trong các phần mềm (giải mã theo thuật toán và tiêu chuẩn khóa mã định trước). Khi một thao tác truy cập vào mạng được thực hiện (kiểm tra đúng User Name và Password), hệ quản lý xác thực sẽ gửi đến máy tính của người dùng đang xin truy cập vào mạng một chuỗi các ký tự gọi là Challenge (câu thách đố), người dùng này sẽ nhập vào Token chuỗi Challenge và sẽ nhận được một chuỗi ký tự mới gọi là PIN (Personal Identification Number - số nhận dạng cá nhân). Nhờ PIN mà người dùng có thể truy cập vào hệ thống mạng. Điều đặc biệt là Challenge và PIN thay đổi từng phút một, các Token có thể được định và thay đổi Cryptor Key (khóa mã) tùy người sử dụng nên việc bảo mật gần như là tuyệt đối.

5.6. Kiểm tra và Cảnh báo (Activity Logging and Alarms)

a. Activity logging

Để cung cấp thông tin về những hoạt động của mạng tới người quản trị hầu hết

các tường lửa ghi chép các thông tin vào files (log files) và lưu giữ trên đĩa. Một tường lửa hoàn chỉnh phải ghi chép đầy đủ các thông tin về các kết nối thành công và cả không thành công. Các thông tin này rất hữu ích cho việc phát hiện kịp thời những lỗ hổng trên tường lửa. Một log file chuẩn phải có các thông tin sau:

- Thời gian bắt đầu và kết thúc của một phiên;
- Địa chỉ trạm nguồn;
- Địa chỉ trạm đích;
- Giao thức sử dụng (TCP hay UDP);
- Cổng được mở trên trạm đích;
- Kết quả của việc kết nối (thành công hay bị từ chối);
- Tên người sử dụng nếu xác thực được sử dụng.

Ngoài ra còn có thể có thêm các thông tin về số gói được chuyển qua, số lần lặp lại của kết nối đó…

b. Alarm

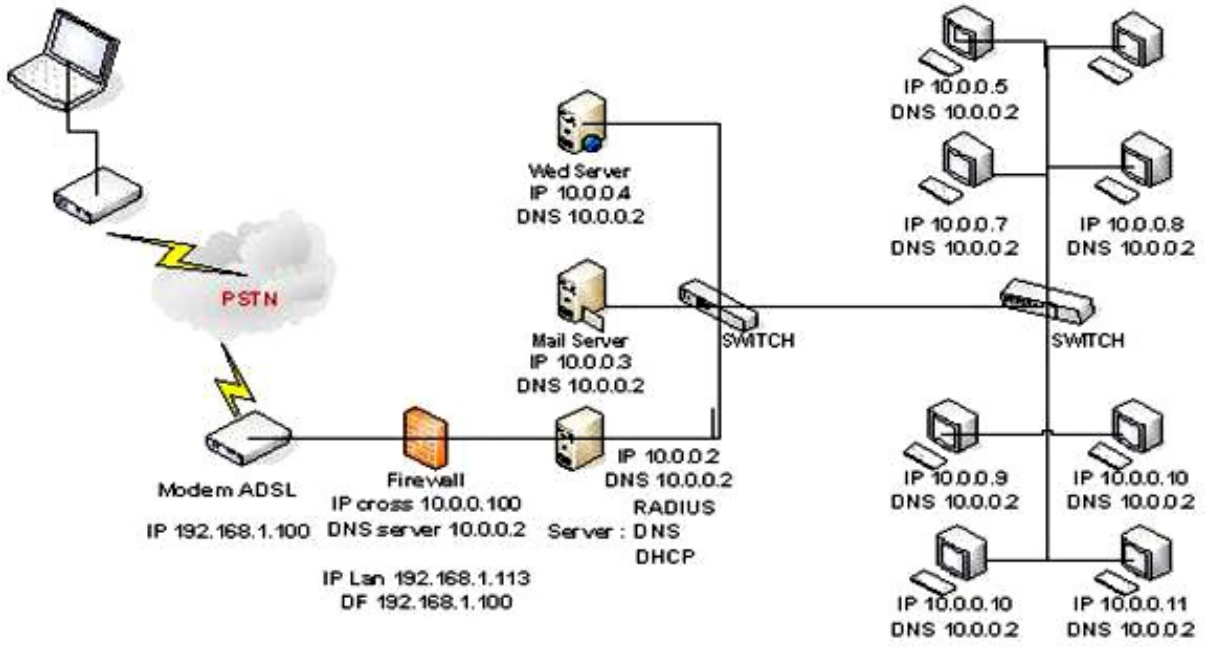
Hoạt động báo động cũng rất quan trọng đối với người quản trị. Khi có một kết nối đến mạng thì tường lửa sẽ phát tín hiệu để người quản trị biết. Đồng thời hoạt động cảnh báo cũng đưa ra tình trạng lỗi của các gói.

Khi một gói bị chặn lại không qua được tường lửa thì hoạt động cảnh báo của tường lửa cũng gửi một cảnh báo đến trạm nguồn thông báo về nguyên nhân loại bỏ gói đó.

6. Các mô hình Firewall cơ bản và phức tạp

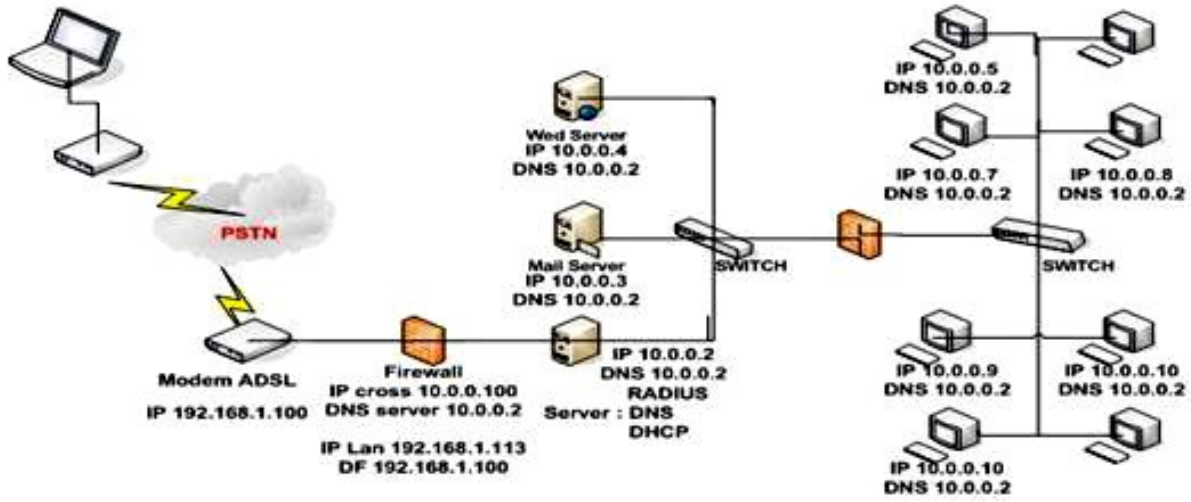
Mục tiêu: Trình bày các mô hình firewall cơ bản và phức tạp thường được sử dụng trong các doanh nghiệp.

6.1. Mô hình Firewall cơ bản thường được sử dụng đến:



6.2. Mô hình Firewall phức tạp thường sử dụng trong các doanh nghiệp lớn

Nó có thể chống để các đợt tấn công và xâm nhập bức hợp pháp cả bên trông lẫn bên ngoài Internet

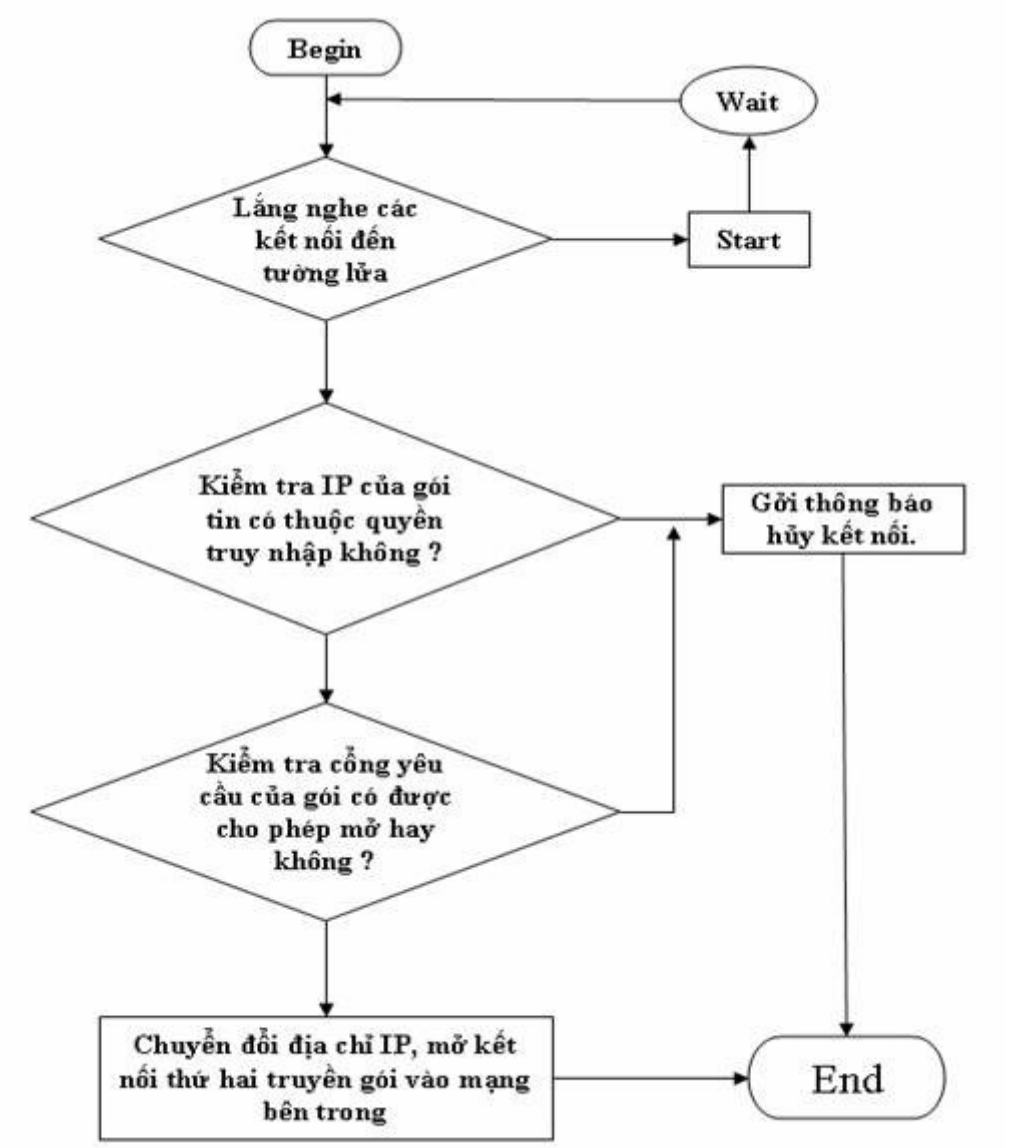


Firewall Cross IP 10.0.0.100 Server IP 10.0.0.2 Clien IP 10.0.0.3
SM 255.0.0.0 SM 255.0.0.0 SM 255.0.0.0
DF không DF 10.0.0.100 DF 10.0.0.100
DNS 10.0.0.2 DNS 10.0.0.2 DNS 10.0.0.2
Lan IP 192.168.1.113
SM 255.255.255.0
DF 192.168.1.100

DNS không

7. Sơ Đồ hoạt động của ISA

Mục tiêu: Trình bày sơ đồ hoạt động của ISA theo dạng sơ đồ khối. Trong đó, các tiến trình cùng với trình tự sẽ được biểu diễn.



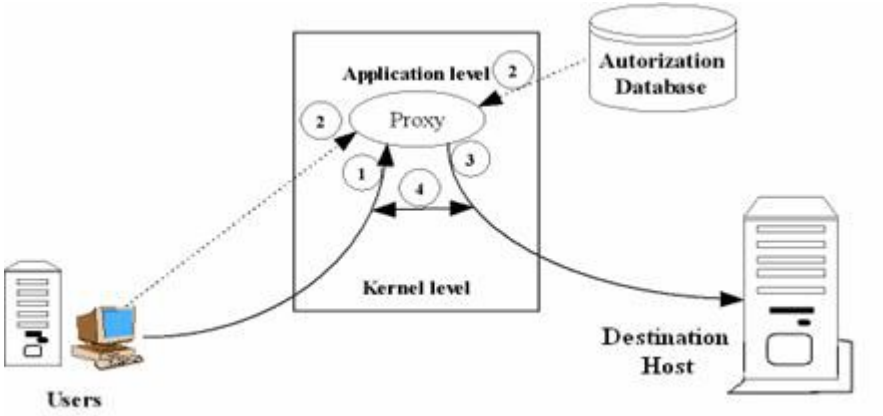
Câu hỏi

1. Firewall là gì? Hãy phân loại Firewall.

2. Trình bày các kiến trúc Firewall cơ bản.

3. Trình bày quá trình hoạt động của firewall.

4. Theo sơ đồ cho dưới đây, cho biết quá trình hoạt động của tường lửa ứng dụng (Proxy Application).


Application level
2
Autorization Database
2
Proxy
1
3
4
Kernel level
Destination Host
Users

BÀI 7: CÀI ĐẶT VÀ CẤU HÌNH SỬ DỤNG CÁC RULE TRONG ISA

Mã bài: MĐ 36-07

Mục tiêu của bài:

- Cài đặt được ISA Server trên Windows Server theo đúng qui trình;
- Thiết lập được các rule để bảo mật cho hệ thống;
- Thực hiện các thao tác an toàn với máy tính.

1. Cài đặt ISA

Mục tiêu: Trình bày yêu cầu đối với máy cài đặt ISA, trình tự các bước thực hiện cài đặt và cấu hình ISA. Ngoài ra, trình tự thực hiện các luật cũng được nêu rõ.

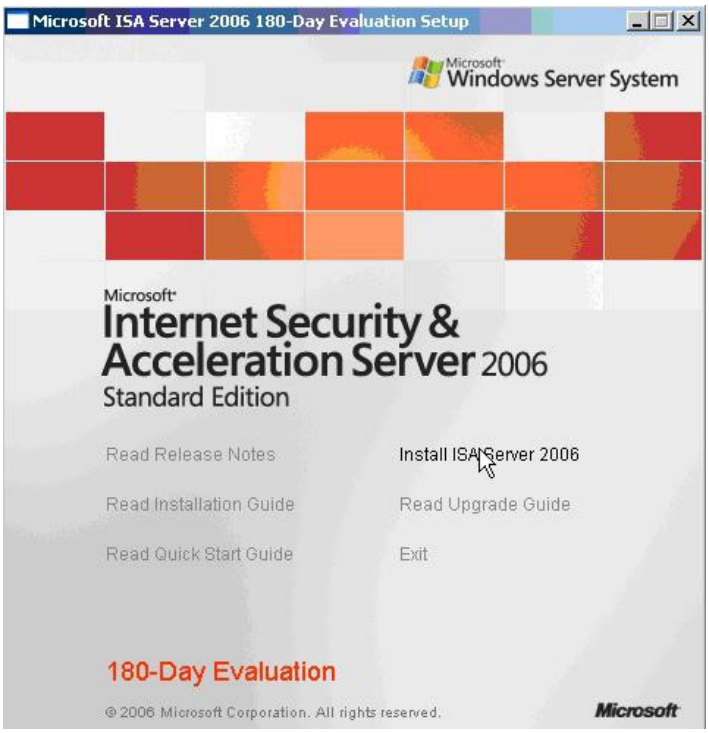
Máy cài ISA phải có 2 card khi đó ta cấu hình IP như trong mô hình cơ bản

- Card trong nội bộ đặt tên là **Cross**

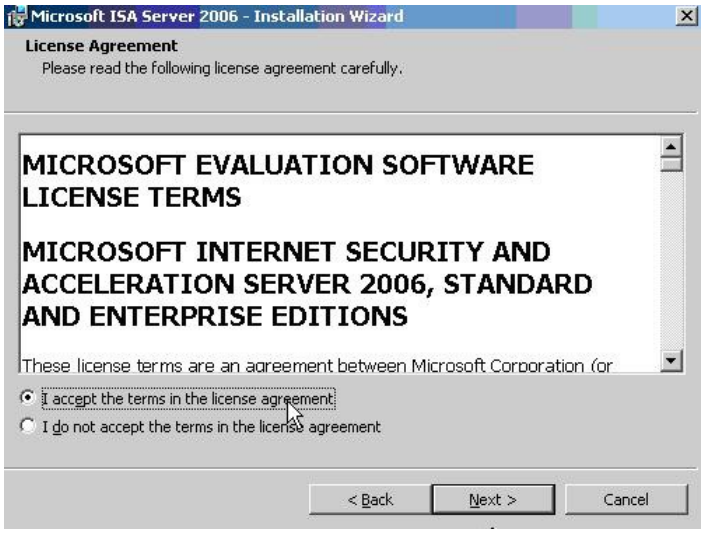
- Card đi ra ngoài internet tên là **Lan**

Các bước thực hiện:

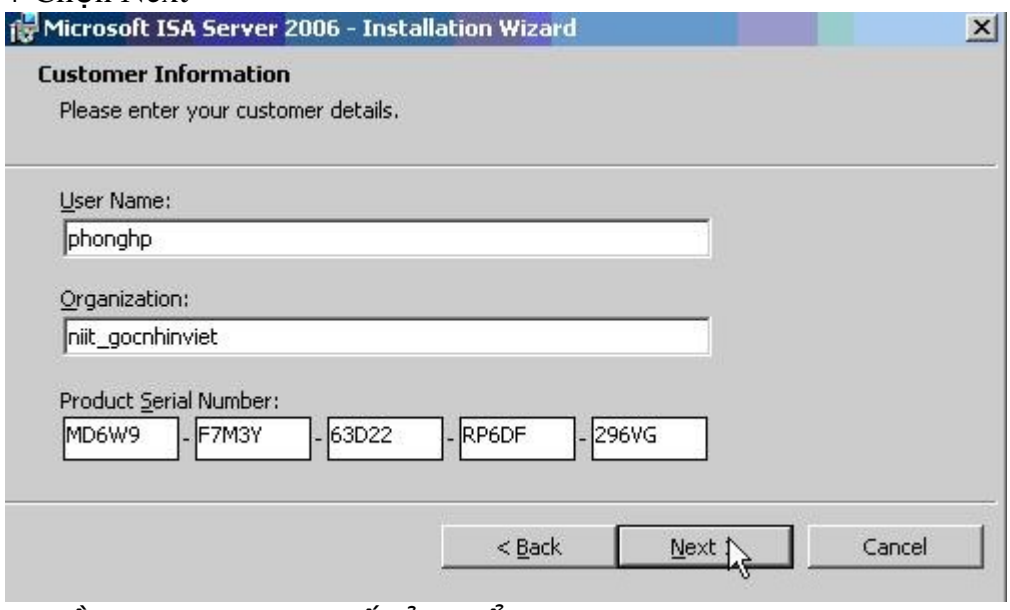
+ Bỏ đĩa ISA 2006 vào rồi nhắp đúp vào file setup



+ Chọn Install ISA Server 2006



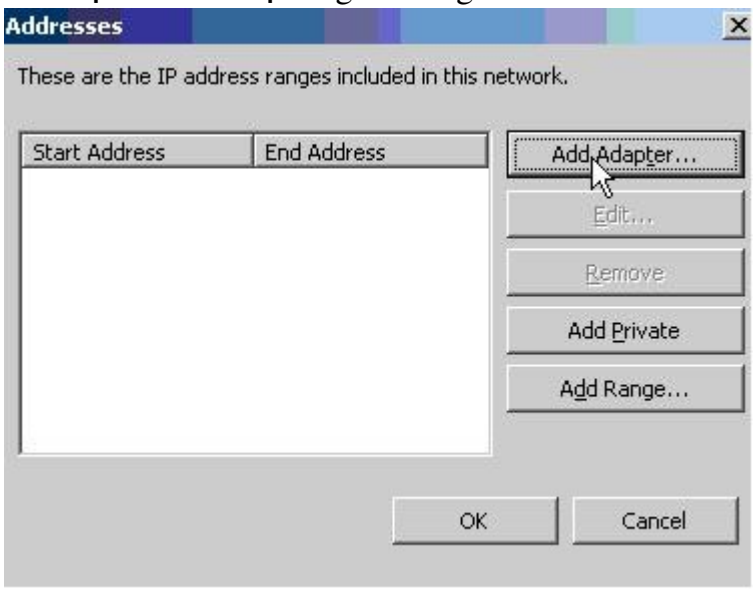
+ Chọn Next



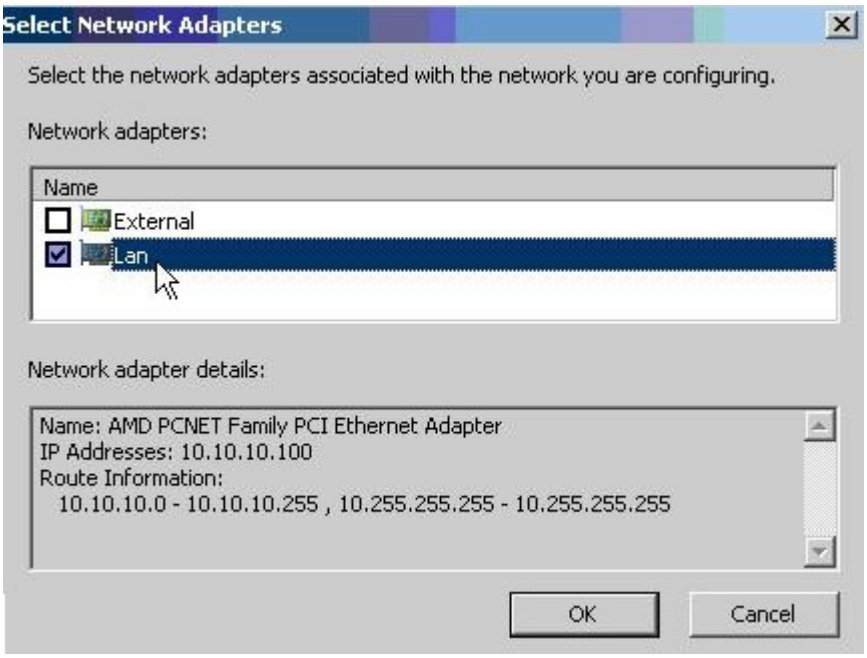
+ Điền các thông tin và số sản phẩm, chọn Next

+ Chọn kiểu cài đặt, chọn Next

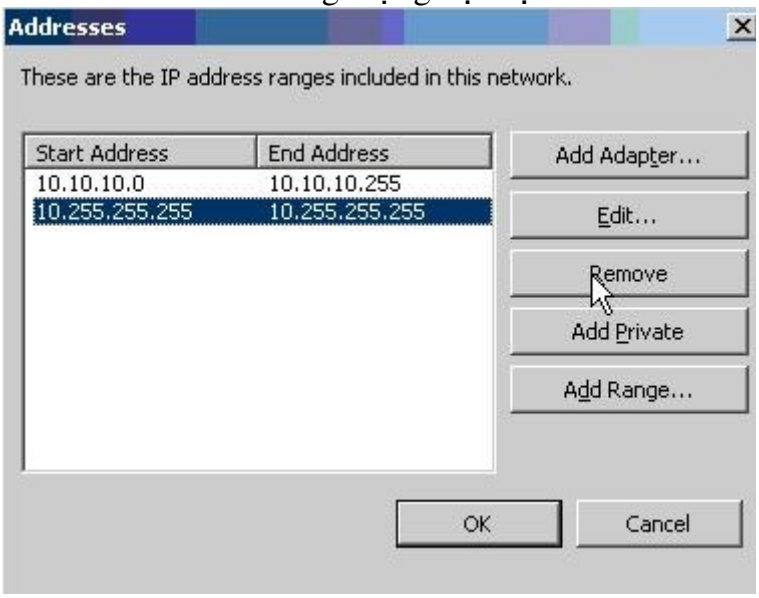
+ Chọn Add để định nghĩa vùng **Internal Network**



+ Chọn Add Adapter để khai báo vùng địa chỉ card IP Internal

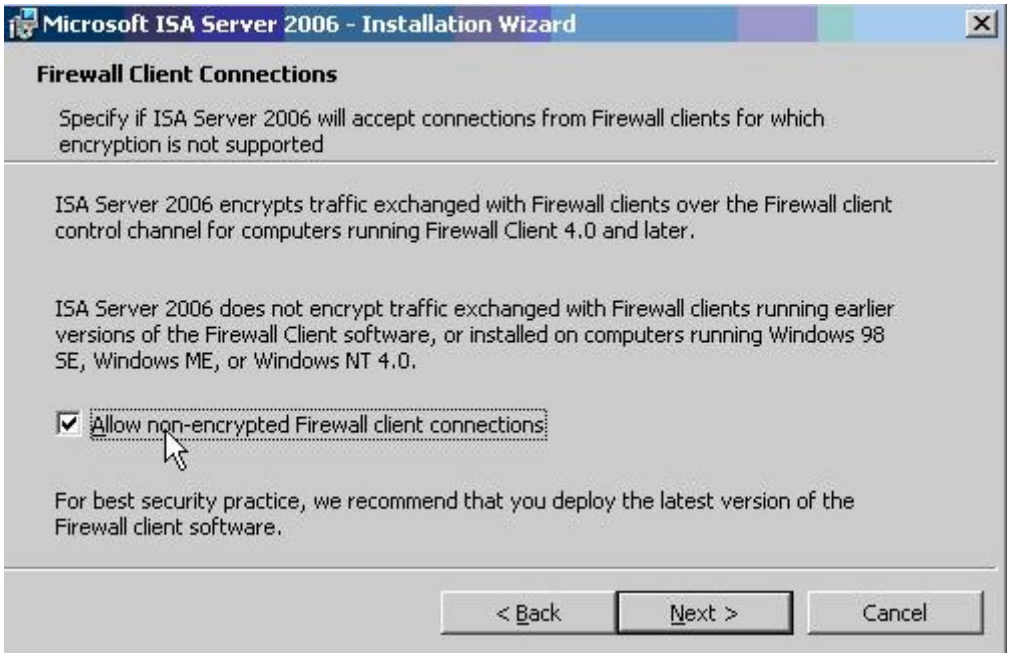


+ Chọn card lan là card bên trong mạng nội bộ



+ Chọn Remove

+ Next



+ Next

+ Màn hình xuất hiện một số cảnh báo đối với các dịch vụ đang hoạt động, chọn Next

+ Chọn Install để thực hiện cài đặt

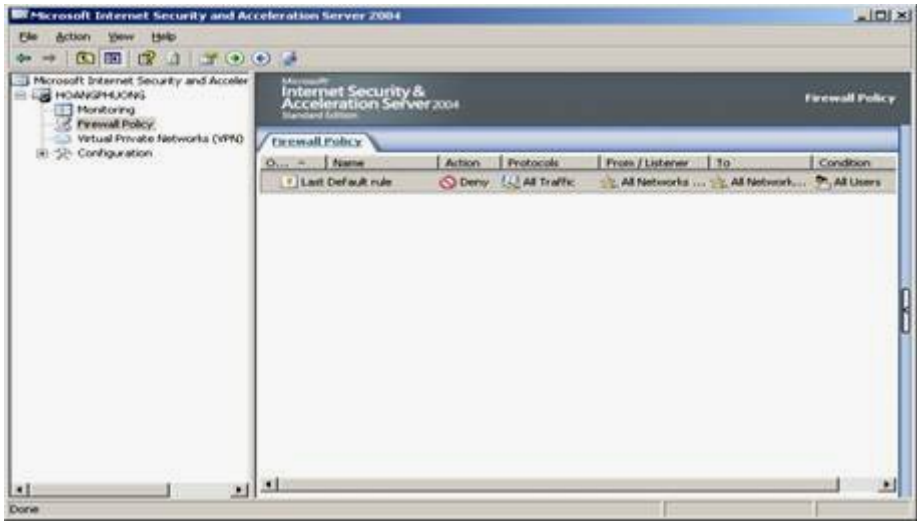
+ Chọn Finish để kết thúc quá trình cài đặt

Khi ISA được cài vào, việc đầu tiên **ISA** sẽ cấm mọi người ping tới nó và không cho ra **Internet;** vậy muốn ping hay ra **Internet**, phải tạo ra **rule** và **Allow** cho nó.

Mở ISA, chọn **Firewall Policy**, nhìn vào cửa sổ ở giữa nó sẽ liệt kê 1 rule trong **Policy. Rule** này có tên là **Last Default rule;** Đây là rule mặc định nên ta không thể nào xoá được.

Rule này nói lên là đang thực thi 1 hành động là cấm đoán "**Deny**". Nó cấm đoán tất cả mọi hành động "**All Traffic**". Và cấm tất cả mọi người ở vùng **Network** nào "**All Network (and Local Host)"**. Đi đâu cũng cấm "**All Network (and Local Host)**". Đối với người nào cũng cấm "**All Users**"

ISA hệ thống được sắp xếp theo thứ tự rule từ trên xuống thỏa rule nào thì được ứng xử theo hành động rule đó



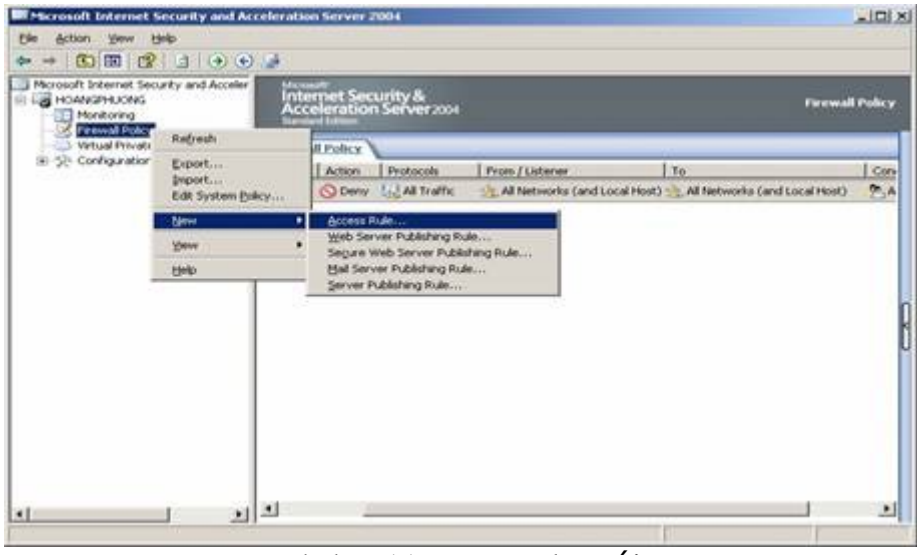
Hình 7.10 – Rule mặc định trong Firewall Policy

2. Tạo Rule cho Admin đi ra ngoài Internet sử dụng tất cả các giao thức

Mục tiêu: Sau khi cài đặt, ISA server lập tức ngăn cách giữa Internal Network và External Network bởi chính nó, khi đó các máy trong Internal Network không thể truy cập được ra ngoài (mạng Internet) và ngược lại. Nói cách khác ISA Server đã khóa tất cả mọi Port ra vào hệ thống.

Trong phần này sẽ trình bày cách thức mở các Port để có thể truy cập Internet. Lưu ý: Không nên mở các cổng một cách tùy tiện mà chỉ mở khi thực sự cần thiết.

Nhắp chuột phải vào **Firewall Policy,** chọn **New** rồi chọn tiếp **Access rule**



Hình 7.11 – Tạo rule mới

Hộp thoại **Access rule name:** Ta điền Amin ra Internet rồi chọn **Next**

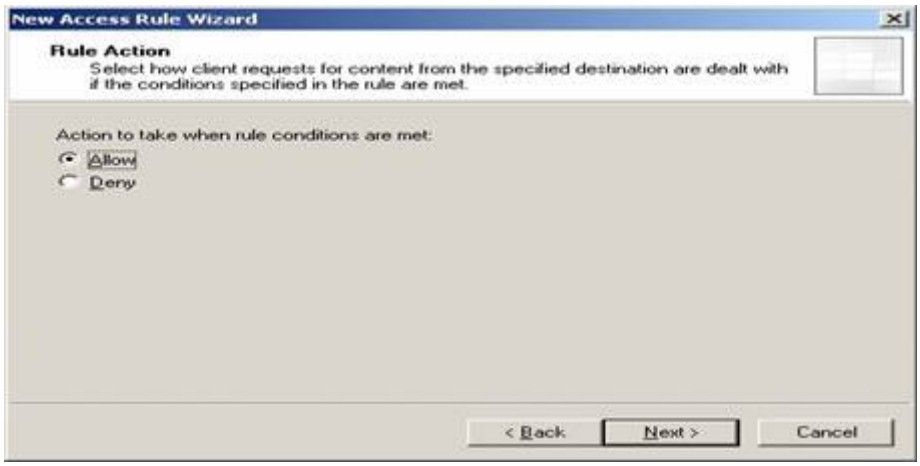
- Rule Action (Hành động)

- Action to take when rule condition are met:

- Allow: (cho phép)

- Deny: (Cấm)

Rule ở đây là ra **Internet** nên ta chọn **Allow** rồi bấm **Next**



Hình 7.12 – Cho phép Admin ra Internet

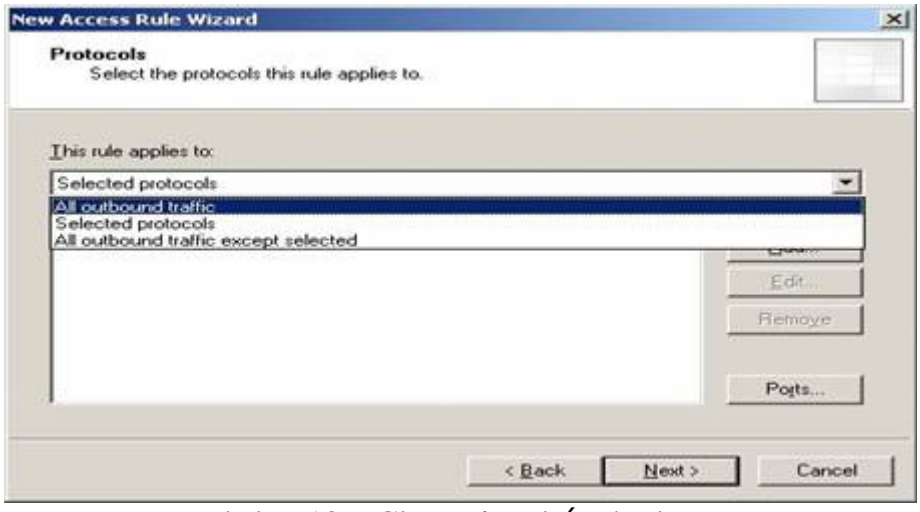
Protocols (Gồm những hành động nào đi ra ngoài)

This rule applies to:

Chọn hành động **All outbound trafic:** hành động này đi ra ngoài sử dụng được tất cả các **Protocol**. Chọn **Next**

Selected protocols: Muốn **Protocol** nào đi ra ngoài thì chọn mục này

All outbound traffic except selected: Cho phép sử dụng tất cả **Protocol** nhưng muốn không dùng **Protocol** nào thì chọn mục này



Hình 7.13 – Chọn giao thức áp dụng

Acces Rule Sources (nguồn xuất phát từ đâu)

Ta chọn **Add** xuất hiện 1 cái bảng **Add Network Entities**

Ta chọn mục Network: Internal là bên trong

External là bên ngoài

Local Host là máy ISA

Ta muốn ra ngoài **Internet** nên ta chọn nơi xuất phát từ **Internal** rồi **Close**

Hình 7.14 – Chỉ định vị trí xuất phát

Lúc này Access Rule Sources có Internal ta bấm Next

Access Rule Destinations (Đích đến)

Ta tiếp tục bấm **Add**. Muốn đi đâu, ra ngoài **Internet** ta chọn **External** rồi **Close**

Hình 7.15 – Chọn đích đến (ra Interrnet)

Lúc này, ngoài Access rule Destinations có External ta bấm Next

User Sets (Ai đi ra)

Ta muốn Admin đi ra thì bỏ **All Users** bằng cách bấm vào **All Users** bấm nút **Remove**

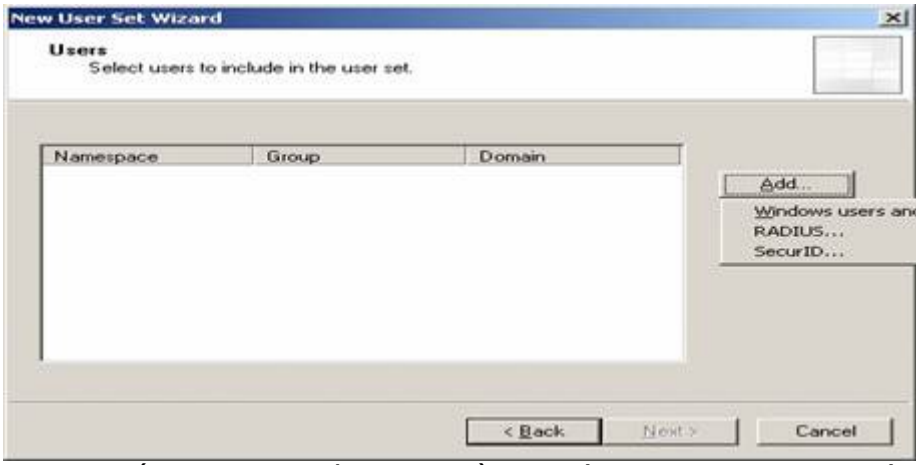
Hình 7.16 – Giới hạn người dùng

Rồi bấm **Add:** Màn hình **Add Users** xuất hiện, chọn **New**

Hình 7.17 – Thêm người dùng chịu tác động

Màn hình **New User Set Wizard** xuất hiện: Ta điền là **Admin** rồi chọn **Next**

Khi đó ta chọn **Add** sẽ xuất hiện lên 3 lựa chọn, chọn **Windows users and groups**



Hình 7.18 – Đối tượng tác động bao gồm người dùng và nhóm người dùng

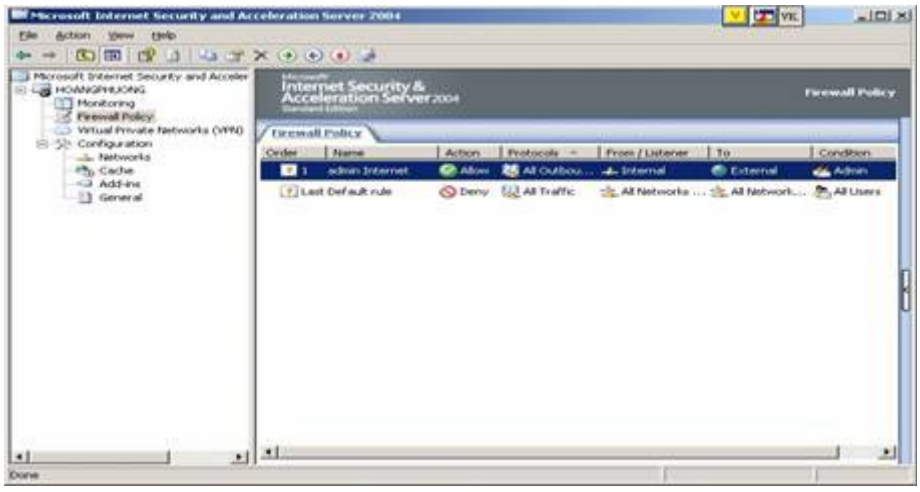
Chọn nút **Location** chọn **Entire Directory** rồi chọn **"tên miền"** rồi **OK,** sau đó bấm vào **Advanced** rồi bấm nút **Find Now** ta sẽ thấy mục **Search results** có **Administrator** ta chọn rồi **OK** rồi **Next** sau đó **Finish.**

Hình 7.19 – Chỉ định người dùng và nhóm người dùng

Bây giờ ta thấy có **Admin** do ta làm hồi nãy ta chọn **Admin** rồi **Close**

Hình 7.20 – Đối tượng được thêm vào là Admin

Bây giờ **User Sets** không phải là chữ **All Users** mà là chữ **Admin** ta bấm **Next** tiếp rồi **Finish** rồi **Apply**

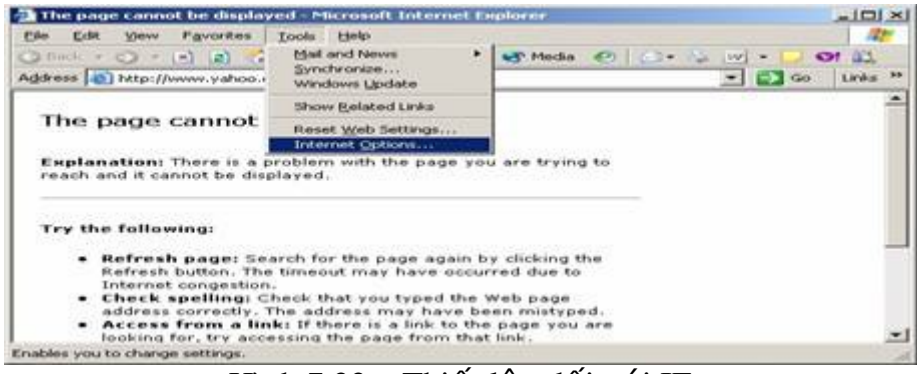


Hình 7.21 – Đối tượng chịu tác động là Admin

Kể từ bây giờ **admin** có thể truy cập được **Internet**

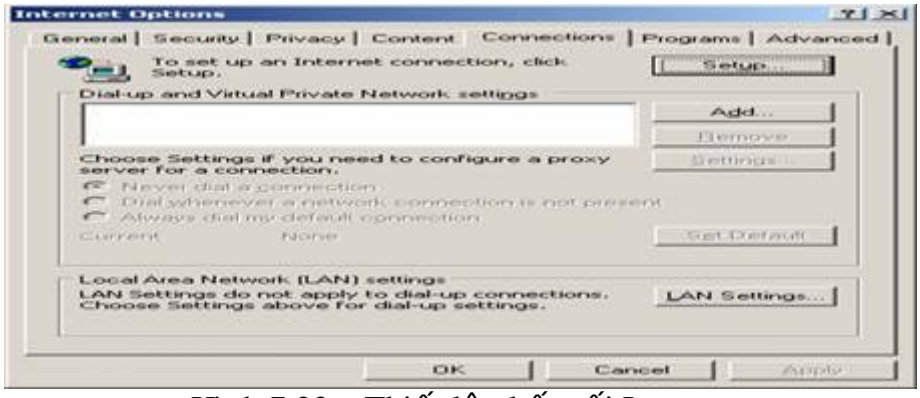
Bây giờ **Client** bỏ DF 10.0.0.100 đi thì không vô **Internet** được

Máy **Client** mở **IE** lên chọn **Tab Menu Tool** chọn **Internet Options**



Hình 7.22 – Thiết lập đối với IE

Rồi chọn **Tab Connection** rồi chọn **Lan Setting**



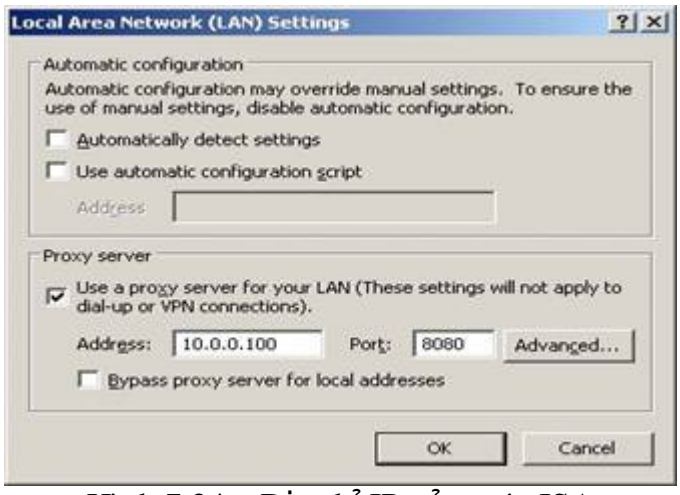
Hình 7.23 – Thiết lập kết nối Internet

Mục **Proxy server**

- Đánh dấu chọn **Use a proxy server for your LAN (These setting will not apply to dial-up or VPN connections)**

- Address ta đánh địa chỉ **IP** của máy **ISA** 10.0.0.100 **Port** 8080 rồi **OK**

Lúc này ta lại vô được **Internet**



Hình 7.24 – Địa chỉ IP của máy ISA

Ta không cần có **DF** vẫn ra **Internet**, 2 kiểu đi ra **Internet** khác nhau là:

- Máy Client ta để **DF** đến ISA lúc đó máy **ISA** đang đóng vai trò **NAT**

- Còn lúc **Client** trong trình duyệt **IE** mà cấu hình **Proxy** lúc đó máy **ISA** đóng vai trò **Proxy Server**

Ta mở **IE** lên vào **Proxy** bỏ hết các thông số ta sẽ không đi bằng kiểu **NAT** hoặc **Proxy** nữa mà đi bằng kiểu 3

Máy **Client** mở hộp thoại **RUN** lên đánh địa chỉ **IP** của máy **ISA** file:///\\10.0.0.100 ta sẽ thấy bên máy **ISA** có 1 thư mục đặt tên là **mspclnt** ta nhắp đúp vào đó rồi chạy file **Setup** ta cứ việc **Next** rồi **Next** thêm cái nữa. Màn hình **ISA server Computer Selection** xuất hiện

Ta chọn **Connect to this ISA Server computer** ta đánh **IP** của **ISA** 10.0.0.100 rồi **Next**

Hình 7.25 – Chỉ định IP của ISA

Bấm **Install** rồi bấm **Finish** và khi cài xong máy **client** sẽ có biểu tượng và lúc này ta không có **DF** và **Proxy** nhưng vẫn truy cập được **Internet**

Kết luận: Máy **Client** khi mà để **DF** thì gọi là **Secure NAT**

Máy **Client** không để **DF** nhưng sử dụng **Proxy** gọi là **Proxy Client**

Khi **Client** không dùng **DF** và **Proxy** mà đi cài **Tool ISA Client** gọi là **Firewall Client**

Mỗi cách sẽ có 1 ưu nhược điểm riêng:

- Nếu dùng **Secure NAT** thì **Client** có thể ra Internet và dùng bất kì **Protocol** nào mà **ISA allow** cho cái **rule** của nó

- Nếu dùng **Proxy** chỉ đi ra được **Internet** bằng **HTTP** và **FTP** bất chấp máy **ISA** có allow mọi **Protocol** nhưng bù lại phương pháp đi bằng **Proxy** tận dụng được **CACHING** bởi vì lúc đó máy **ISA** đi dùng. Nếu có máy **Client** khác hỏi lại 1 trang **web** nào mà **ISA** nhớ nó có nằm trong **cache** lúc đó máy **ISA** trả lời lại liền.

Firewall Client là dạng tổng hợp của 2 dạng trên và nó sẽ tự biết là khi nào nên dùng **Secure NAT** và khi nào dùng **Proxy.**

3. Cấu hình cho các client ra Internet nhưng chỉ sử dụng giao thức HTTP, HTTPS

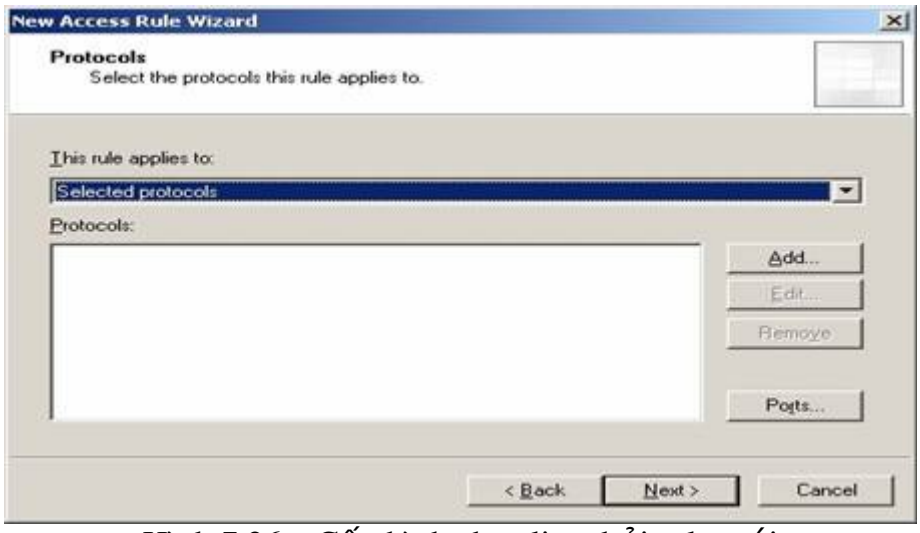
Mục tiêu: Trình bày cách tạo các rule để các client ra internet nhưng chỉ sử dụng giao thức HTTP, HTTPS

Nhắp chuột phải vào **Firewall Policy**, chọn **New** rồi chọn **Access rule**

- Acces rule name ta điền: **Users ra Internet (HTTP và HTTPS)**

- Rule Action: ta chọn **Allow**

- Protocols: Ta chọn **Sellected protocols** rồi chọn **Add**



Hình 7.26 – Cấu hình cho client bởi rule mới

Hình 7.27 – Chỉ định giao thức HTTP, HTTPS

Chọn mục **web** rồi chọn 2 giao thức **HTTP** và **HTTPS -** Close - Next

Access Rule Sources: ta bấm **Add** rồi bấm vào **Network** chọn **Internal** rồi **Close** rồi **Next**

Access Rule Destinations: ta chọn **External** rồi bấm **Next** tiếp

User Sets: mặc định là **All Users** ta tiếp tục bấm **Next** rồi **Finish** Và **Apply**

Lúc này User chỉ sử dụng được có 2 giao thức HTTP và HTTPS.

4. Cấu hình DNS phân giải tên

Mục tiêu: Trình bày cách cấu hình thiết lập để phân giải tên miền trên ISA server.

Bấm vào **Firewall Policy** nhắp chuột phải chọn **New** rồi **Access Rule**

Access rule name: DNS

Rule Action: Allow

Protocols

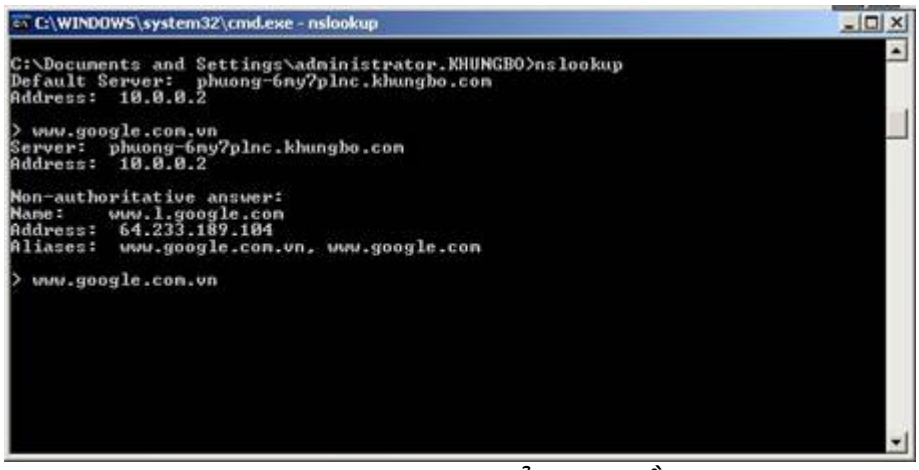
This rule appiles to: ta chọn **Selectes protocols** rồi bấm **Add** ta chọn **Comomn Protocols** rồi chọn **DNS** rồi **Close** rồi **Next**

Access Rule Sources: Internal

Access Rule Destinations: External

User Sets: All Users rồi **Next** rồi **Finish** ta **Apply**

Trong cửa sổ Run, gõ **CMD / OK**. Trong cửa sổ DOS, gõ **nslookup** rồi đánh **www.google.com.vn** ta thấy phân giải tên được là 64.233.189.104



Hình 7.27 – Phân giải tên miền

BÀI 8: DỊCH VỤ VIRTUAL PRIVATE NETWORK (VPN)

Mã bài: MĐ 36-08

Mục tiêu của bài:
- Trình bày được bản chất và lợi ích của VPN;
- Mô tả được mô hình VPN to site;
- Mô phỏng được mô hình site to site;
- Thực hiện các thao tác an toàn với máy tính.

1. Giới thiệu về VPN

Mục tiêu: Trình bày chức năng của VPN và các dạng VPN cùng với cách hoạt động và các ích lợi đạt được đối với VPN.

- VPN như là một mạng LAN ảo mạng trong môi trường Internet.

- Công dụng của VPN là nhằm truy xuất được tài nguyên của mạng nội bộ khi người muốn truy cập không ở trong mạng nội bộ. Ta truy xuất được thông qua đường internet. Cho phép người dùng ngoài Internet dùng một account có sẵn trong nội bộ để truy cập vào mạng nội bộ (client to Site);

- VPN có hai dạng Client to Site và Site to Site.

+ **Client to Site:** Một người ở nhà có kết nối internet muốn truy xuất được tài nguyên ở công ty như là đang ngồi ở công ty. Một nhân viên khi đi công tác có lúc cần lấy dữ liệu, hay cần trao đổi dữ liệu trong cơ quan,… Để đáp ứng được những yêu cầu thực tế này trong cơ quan, công ty,… phải xây dựng mô hình VPN theo kiểu Client to Site: cho phép một kết nối từ xa qua đường truyền internet để truy xuất, trao đổi được tài nguyên của mạng nội bộ.

+ **Site to Site:** Một công ty có nhiều chi nhánh ở xa có kết nối lên đường internet. Yêu cầu thực tế là các chi nhánh của công ty tuy ở xa nhưng cần phải lấy dữ liệu của nhau, cần phải có nhu cầu trao đổi dữ liệu qua lại giữa các chi nhánh,… để đáp ứng yêu cầu này, mô hình VPN theo kiểu Site to Site cần được xây dựng ở các chi nhánh của công ty.

Khi VPN được xây dựng bất kì thành phần nào bên mạng LAN này cũng truy xuất được bất kì thành phần nào ở mạng LAN bên kia và ngược lại. mọi chuyện đều được xảy ra một cách tự động, diễn ra một cách trong suốt mà không cần người Admin đứng ra làm điều gì cả.

1.1. Bản chất hoạt động của VPN

Giả sử có gói tin được truyền theo VPN đến người cần truy xuất, cơ chế gói tin được xử lý như sau:

+ Đầu tiên gói tin (ta xét 3 trường chính trong một header của gói tin là Source Address, Destination Address và trường Data) được truyền có Source Address là địa chỉ của máy nguồn, Destination Address là địa chỉ của máy cần gởi, và trường chứa dữ liệu cần gởi.

+ Khi gói tin đi qua một router, gói tin nầy được router hiện thời bao lại bởi một gói tin khác có Source Address là địa chỉ card ngoài của router hiện thời, gói tin mới có Destination Address vẫn là Destination Address của gói tin được bọc lại, còn trường Data của gói tin mới chứa toàn bộ gói tin cũ, cứ như thế trong đường truyền khi gói tin đi qua mỗi router đều được áp dụng tính chất tương tự.

+ Khi gói tin đi đến đích, ở đây gói tin mới được tháo ra từng lớp như khi đã bị bọc lại khi trong đường đi qua mỗi router, lúc nầy dữ liệu đã được truyền đến đích như mong muốn. Giao thức đứng bao bọc và ngược lại thực hiện lột từng lớp cho gói tin này là giao thức **PPTP (Point to PointTunneling Protocol)** hoặc giao thức **L2TP (Layer Two Tunneling Protocol).**

• **PPTP (Point to Point Tunneling Protocol)** cung cấp mật độ bảo mật tốt dựa trên mức độ phức tạp của Password được dùng để tạo **PPTP** connection. Những thuận lợi khi áp dụng **PPTP** cho **VPN** là không yêu cầu certificate cho quá trình chứng thực và client có thể đặt phía sau **NAT Router**.

• **L2TP (Layer Two Tunneling Protocol)** là sự kết hợp của **PPTP** và **Layer 2 Forwading**; Đồng thời cung cấp mức độ bảo mật cao hơn bởi vì sử dụng giao thức **IP SEC** để bảo mật kết nối. Cũng có thể dùng computer và user certificate để cung cấp mức độ bảo mật cao hơn nữa khi thực hiện kết nối dùng **L2TP/IPSEC**. Trên hệ thống **Microsoft, L2TP** được kết hợp với **IPSec Encapsulating Security Payload (ESP)** cho quá trình mã hóa dữ liệu, gọi là **L2TP/IPSec.** Sự kết hợp này không chỉ cho phép chứng thực đối với người dùng **PPTP** mà còn cho phép chứng thực đối với các máy tính thông qua các chứng chỉ, nâng cao hơn độ an toàn của dữ liệu khi truyền.

• **ESP (Encapsulating Security Payload):** Nội dung thông tin được mã hóa, ngăn chặn các trường hợp hacker đặt chương trình nghe lén và chặn bắt dữ liệu trong quá trình truyền

1.2. Lợi ích của VPN

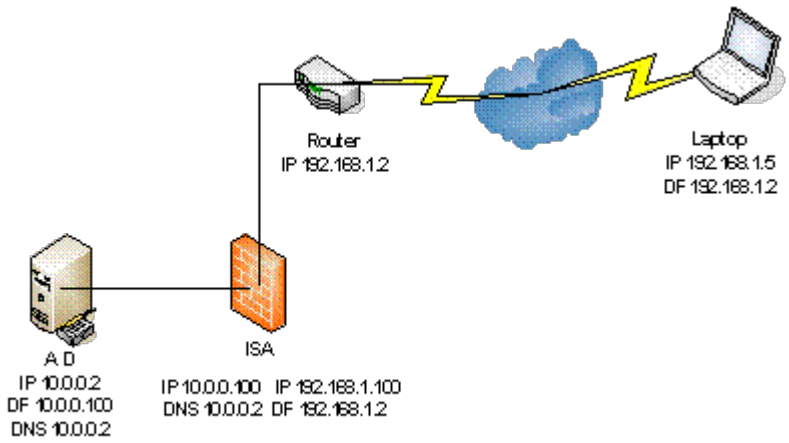
- Mở rộng vùng địa lý có thể kết nối được
- Tăng cường bảo mật cho hệ thống mạng
- Giảm chi phí vận hành so với mạng WAN truyền thống
- Giảm thời gian và chi phí truyền dữ liệu đến người dùng ở xa
- Tăng cường năng suất
- Giảm đơn giản hoá cấu trúc mạng
- Cung cấp thêm một phương thức mạng toàn cầu
- Cung cấp khả năng hỗ trợ thông tin từ xa
- Cung cấp khả năng tương thích cho mạng băng thông rộng
- Cung cấp khả năng sinh lợi nhuận cao hơn mạng WAN truyền thống

Một mạng VPN được thiết kế tốt sẽ đáp ứng được các yêu cầu sau:

- Bảo mật (Security)
- Tin cậy (Reliability)
- Dễ mở rộng, nâng cấp (Scalability)
- Quản trị mạng thuận tiện (Network management)
- Quản trị chính sách mạng tốt (Policy management)

2. Mô hình VPN client to site dùng giao thức PPTP

Mục tiêu: Trình bày cách cấu hình VPN trong môi trường có ISA Server.

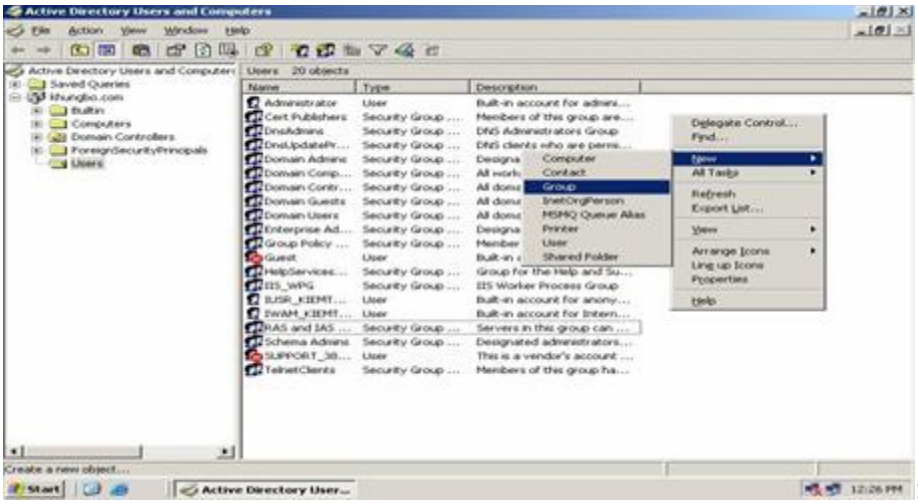


Hình 8.1 – Mô hình VPN client to site dùng giao thức PPTP

Mô hình **Client to site** ta cần 3 máy tính: 1 máy làm **Domain**, 1 máy cài **ISA** và join vào Domain và 1 "máy tính ngoài mạng".

➥ Tại Domain ta tạo 1 **Group** tên là **Admin** (hình 8.2) và bật **Allow access** cho **Administrator** và cho **Administrator** tham gia vào **Group Admin**; **Administrator** có **Password** là 123456

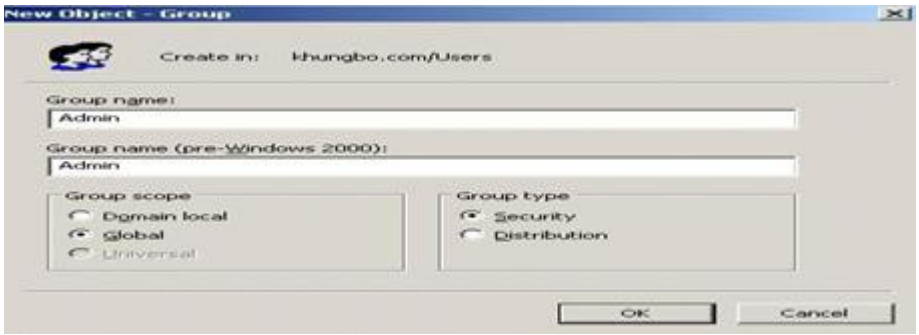
Cách tạo group: Nhắp chuột phải, chọn New, chọn **Group**



Hình 8.2 – Tạo Group

Màn hình **New Object – Group** xuất hiện

Group name: ta điền Admin rồi **OK.**



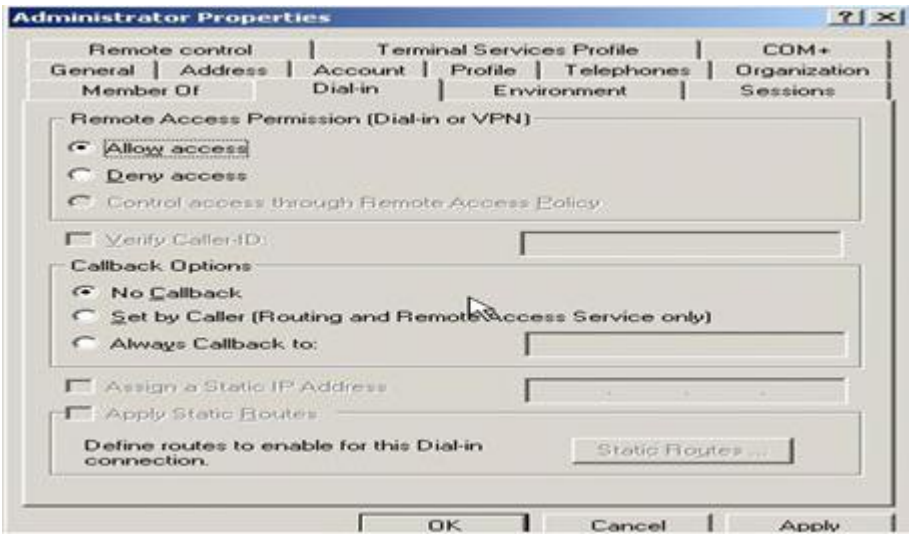
Hình 8.3 – Hộp thoại chỉ định tên group cùng với các tùy chọn

Bật **Allow access** cho Administrator

Ta chọn **Administrator** rồi bấm chuột phải chọn **Properties**

Màn hình **Administrator Properties** xuất hiện (hình 8.4), chọn tab **Dial – in**.

Trong **Remote Access Permission** (Dial –in or VPN), chọn **Allow access / OK**

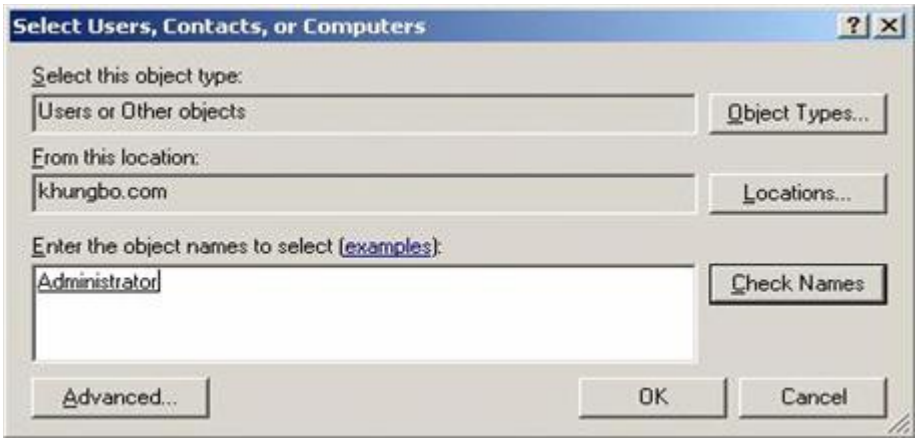


Hình 8.4 – Giao diện Administrator Properties – Tab Dial-in

Cho **Administrator** vào trong **Group Admin**

Ta chọn **Group Admin** rồi nhắp chuột phải chọn **Properties**. Chọn Tab **Members** bấm **Add**

Màn hình Select Users Contacts or Computers xuất hiện (hình 8.5); trong khung "Enter the object name to select", gõ administrator rồi bấm Check Names rồi bấm OK



Hình 8.5 – Màn hình Select Users Contacts or Computers

Lúc này ta quay lại sẽ thấy màn hình **Admin Properties** có **Administrator** xuất hiện ta bấm **OK**.

➥ Tại **ISA,** chọn **Vitual Private Networks:** khi đó ta nhìn bên **VPN Clients Tasks,** chọn **Enable VPN Client Access,** chọn **Apply**.

Hình 8.6 – Kích hoạt VPN Client

Lúc này ta nhìn lại **VPN Client Tasks** không phải là **Enable VPN Client Access** nữa mà là **Disable VPN Client Access**

Ta tiếp tục chọn **Configure VPN Client Access.** Khi màn hình **VPN Client Properties** xuất hiện, chọn tab **General**

Ta đánh dấu vào **Enable VPN client access** và **Maximum number of VPN client allowed**: **10**

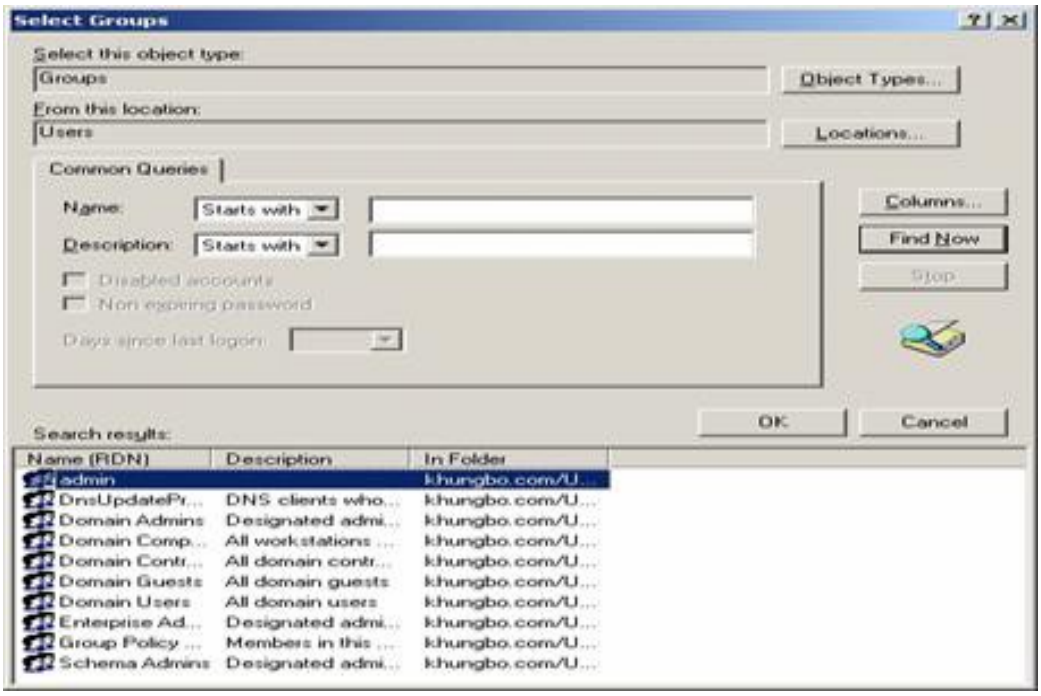
Hình 8.7 – Số kết nối truy nhập tối đa cùng lúc

Chọn tab **Group** rồi nhắp vào nút **Add**. Trong khung Select group, chọn nút Locations **rồi** chỉ định tên miền; chọn **Users** rồi **OK**

Hình 8.8 – Chỉ định vị trí tìm kiếm

Quay lại **Select Groups**, lúc này khung **From this location** được chỉ định là **Users**

Chọn nút **Advanced**. Khi hộp thoại xuất hiện, chọn nút **Find Now.** Lúc này khung **Search rerults** xuất hiện **Group Admin** ta chọn rồi bấm **OK**



Hình 8.9 – Chọn tên nhóm

Lúc này **VPN Client Properties** sẽ xuất hiện **Group Admin**, chọn nút OK

Tab **Protocols**: đánh dấu vào **Enable PPTP** và **Enable L2TP/ IPSec** để chỉ định giao thức kết nối (hình 8.10). Chọn Apply để chấp nhận thiết lập.

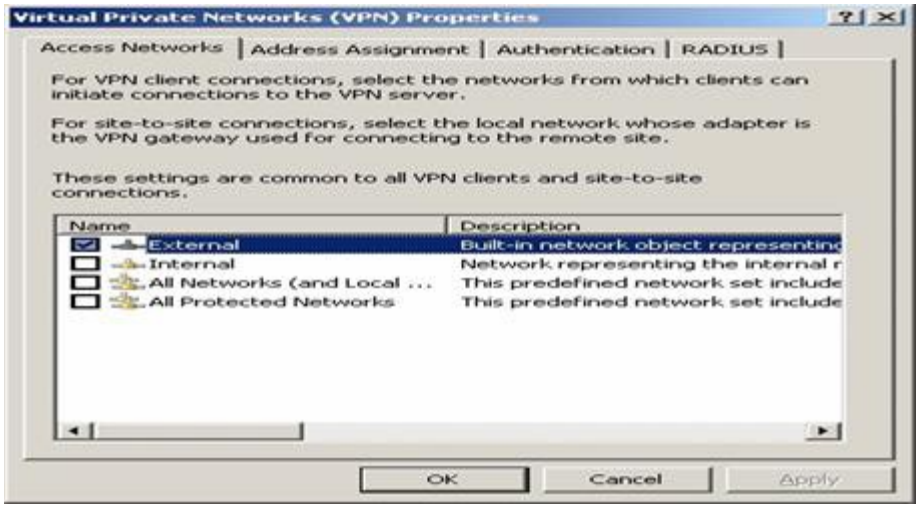
Hình 8.10 – Tab Protocols chỉ định giao thức kết nối

Quay lại cửa sổ Configure VPN Client Access, chọn **Select Access Network**

Hình 8.11 – Cửa sổ Configure VPN Client Access với tùy chọn **Select** Access Network

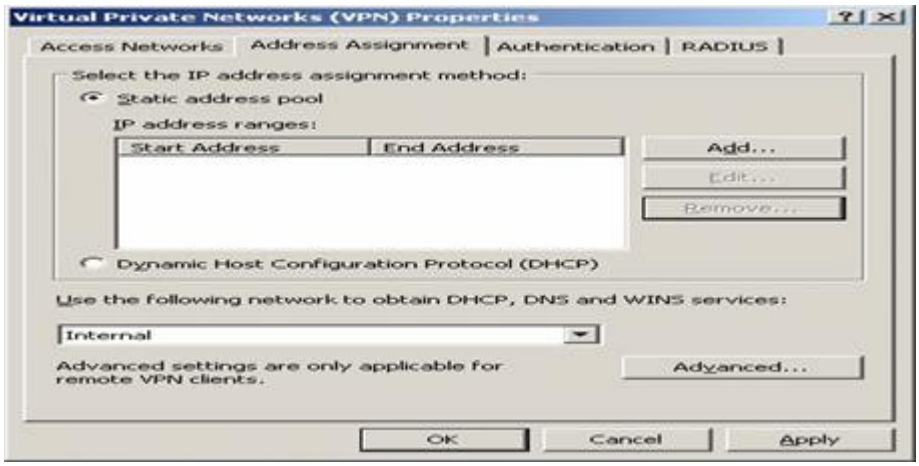
Màn hình **Virtual Private Network (VPN) Properties** xuất hiện

- Tab **Access Network:** Ta đánh dấu vào **External**



Hình 8.12 – Tab **Access Network** với tùy chọn External

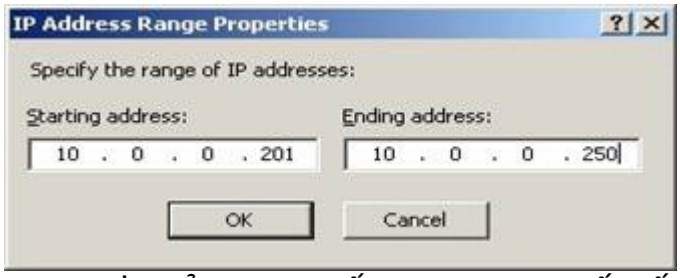
- Tab **Address Assignment:** Đánh dấu vào **Static address pool** rồi chọn **Add**



Hình 8.13 – Tab **Address Assignment** với tùy chọn Static address pool

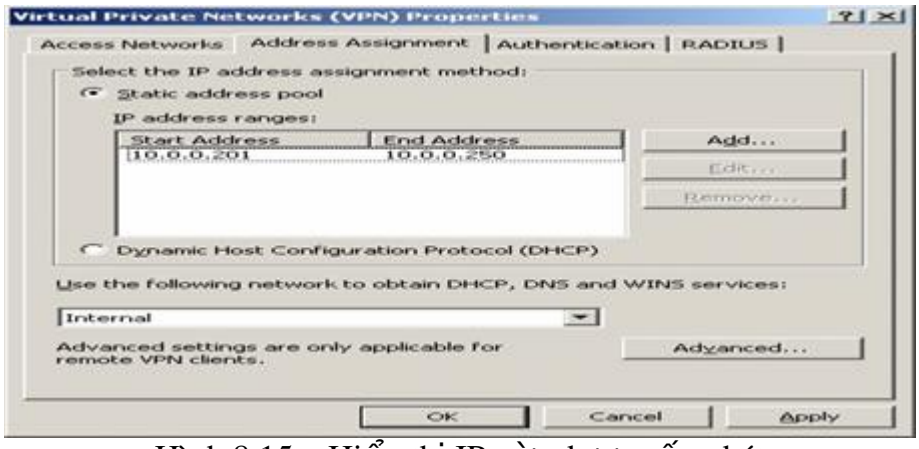
Ta cung cấp khi một ai kết nối bằng **VPN** để truy cập mạng nội bộ sẽ phát sinh ra 1 địa chỉ **IP** (Lưu ý: địa chỉ IP cấp phát này không được trùng với **Internal**)

Internal đã lấy địa chỉ **IP** 10.0.0.2 đến 10.0.0.200 thì ở đây phải cấp phát địa chỉ IP là 10.0.0.201 đến 10.0.0.250



Hình 8.14 – Vùng địa chỉ IP được cấp phát cho các kết nối bằng VPN

Quay lại cửa sổ **Virtual Private Network (VPN) Properties** (hình 8.15), trong **IP address ranges** sẽ hiển thị IP vừa được cấp phát, chọn **OK** rồi chọn **Apply**



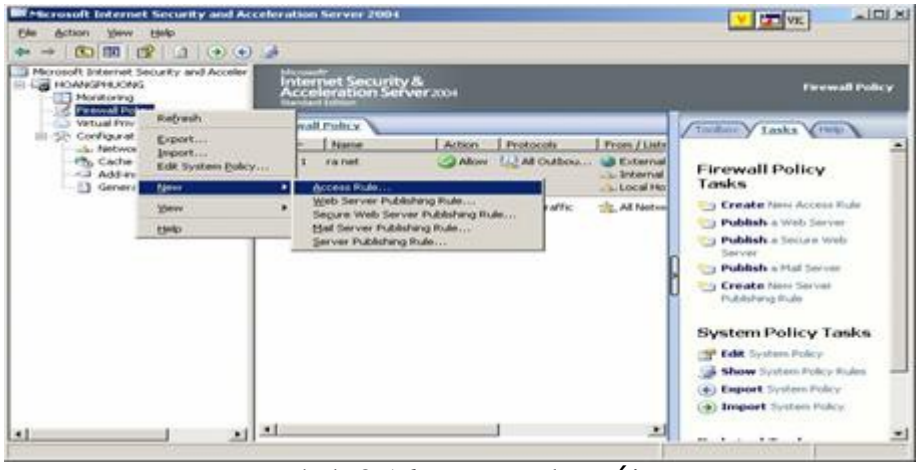
Hình 8.15 – Hiển thị IP vừa được cấp phát

Khi cấu hình **Virtual Private Network (VPN)** xong, tiến hành tạo ra 1 **rule** để cho mọi người khi kết nối **VPN** có thể xâm nhập vào mạng nội bộ được.

Lưu ý: nếu không tạo rule cho các **VPN Client** thì cho dù kết nối VPN thành công cũng không thể nào truy xuất dữ liệu trong mạng nội bộ được.

Cách tạo rule cho VPN Client truy xuất dữ liệu được

Chọn **Frewall Policy** nhấp chuột phải chọn **New** rồi **Access Rule**



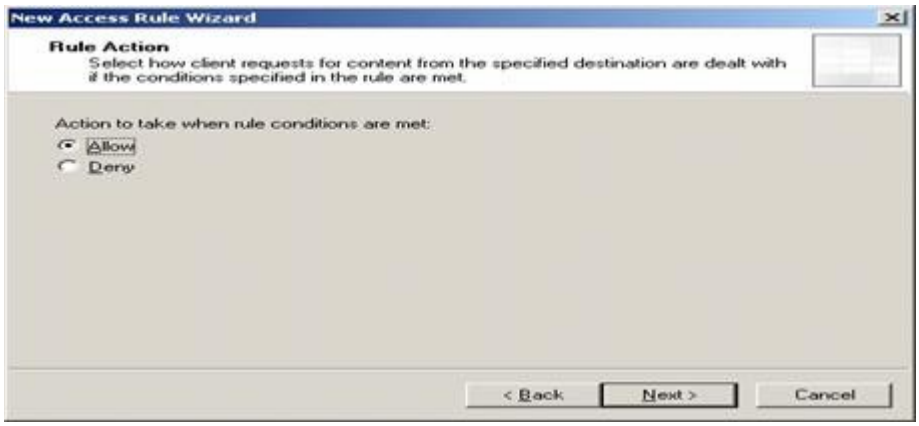
Hình 8.16 – Tạo rule mới

Màn hình **Wellcome to the New Access Rule Wizard** xuất hiện

Trong **Access rule name:** điền **VPN Client** rồi **Next**

Hình 8.17 – Tên rule cần tạo

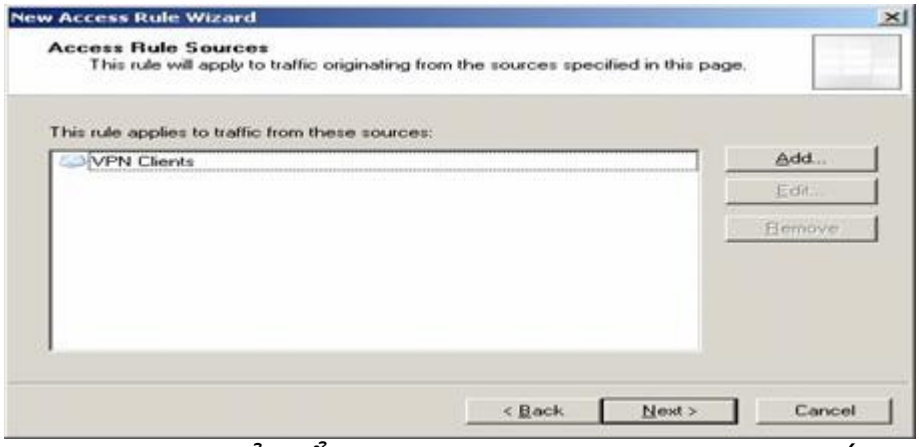
Rule Action xuất hiện; Trong **Action to take when rule condtions are met:** Ta chọn **Allow** rồi **Next**



Hình 8.18 – Cho phép **VPN Client** kết nối và truy xuất dữ liệu trong mạng nội bộ

Trong cửa sổ **Protocols**, chọn **All outbound traffic** trong **This rule applies to,** rồi chọn **Next.**

Khi cửa sổ **Access Rule Sources** xuất hiện (hình 8.19), chọn nút **Add** rồi bấm vào **Network** chọn **VPN client** rồi **Close** lúc này **This rule applies Clients** xuất hiện **VPN Client** rồi bấm **Next**



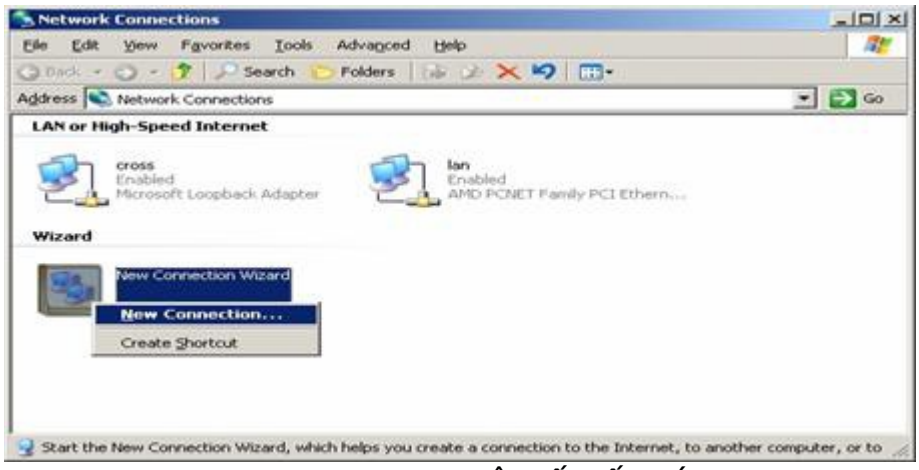
Hình 8.19 – Cửa sổ **Access Rule Sources** – thêm rule mới

Access Rule Destinations: Ta cũng bấm **Add** rồi bấm vào **Network** chọn **Internal** rồi **Close** lúc này ta cũng sẽ thấy **This rule applies to traffic sent to these destinations** xuất hiện **Internal** rồi bấm **Next.**

Users Sets: Lúc này đã có sẵn **All Users**, chọn Next rồi **Finish, Apply.**

➧ Cấu hình máy client để sử dụng VPN

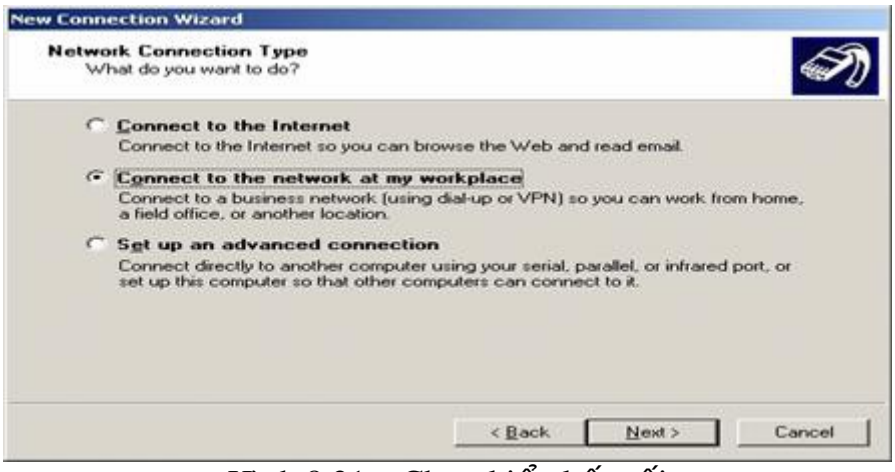
Mở cửa sổ Netwwork Connection: Nhắp phải chuột vào **My Network Places**, chọn **Properties;** sau đó, nhắp phải chuột vào **New Connection Wizrad**, chọn **New Connection** (Xem hình 8.20).



Hình 8.20 – Tạo một kết nối mới

Màn hình **Wellcome to the New Connection Wizard** rồi bấm **Next**

Khi màn hình **Network Connection Type** xuất hiện, chọn **Connect to the network at my workplace** (hình 8.21), chọn **Next**



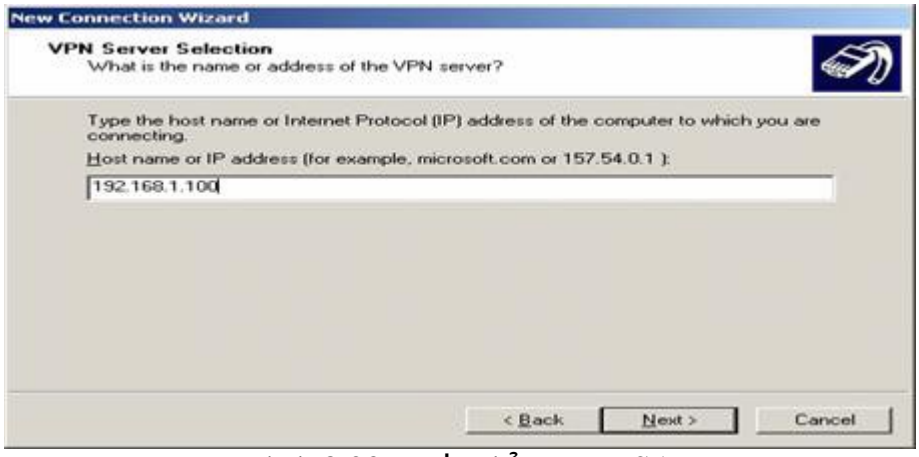
Hình 8.21 – Chọn kiểu kết nối

Network Connection: Ta chọn **Virtual Private Network connection** rồi **Next**

Hình 8.22 – Thực hiện kết nối VPN

Trong màn hình **Connection Name**, điền **PPTP** trong **Compary Name** (hình 8.23), rồi chọn **Next**

Khi màn hình **VPN Server Selection** xuất hiện (hình 8.23), điền địa chỉ của server (192.168.1.100) trong **Host name or IP address**, chọn **Next**



Hình 8.23 – Địa chỉ server ISA

Màn hình **Connection Availability** xuất hiện, chọn **My use only**, rồi chọn Next

Màn hình **Completing the New Connection** xuất hiện, đánh dấu vào mục **Add a shortcut to this connection to my desktop** để tạo một shortcut trên Desktop.

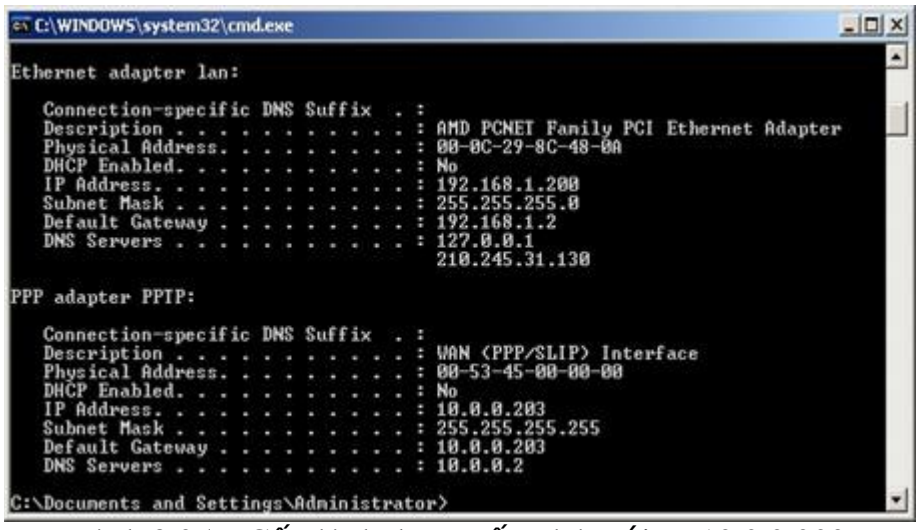
Nhắp đúp chuột vào shortcut **PPTP** để thực hiện kết nối

- User name: ta điền Administrator

- Password: 123456 rồi bấm **Connect**

Hình 8.24 – Kết nối PPTP

Mở cửa sổ Commandline trong giao diện DOS, thực hiện lệnh **ipconfig /all** (xem hình 8.25) sẽ thấy xuất hiện thêm 1 địa chỉ **IP** (do kết nối **VPN** tới mạng cục bộ và được **ISA** cung cấp).



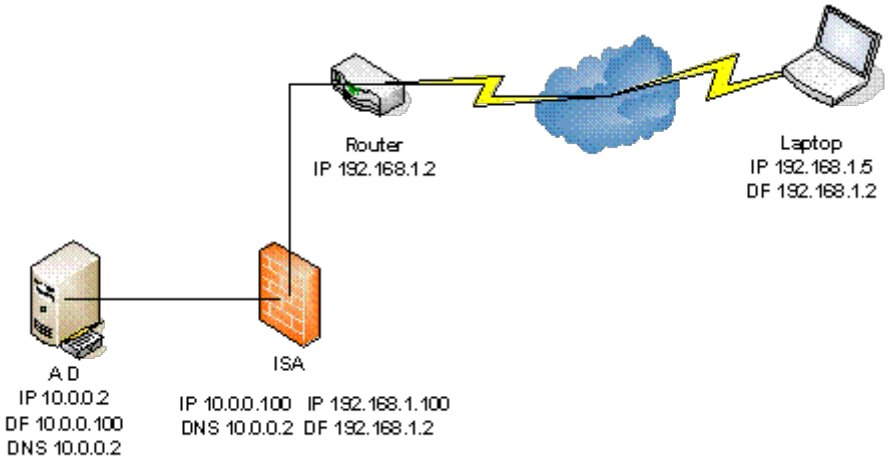
Hình 8.25 – Cấu hình được cấp phát với IP 10.0.0.203

Và ta tiến hành **Ping** đến mạng cục bộ thử là 10.0.0.2 thì thấy nó trả lời lại tín hiệu **127**

Và kể từ lúc này ta có thể truy xuất được dữ liệu trong mạng cục bộ

3. Mô hình VPN Client to Site dùng giao thức L2TP/IPSEC

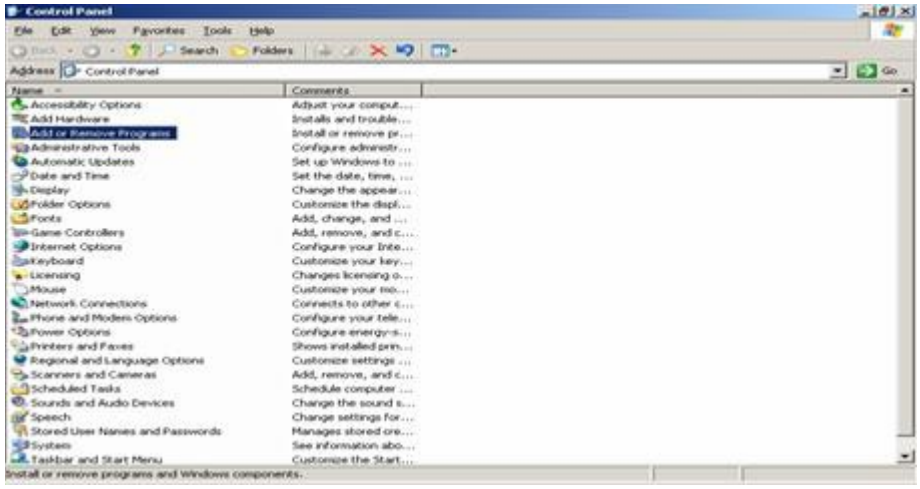
Mục tiêu: Trình bày cách cấu hình VPN trong môi trường có ISA Server.



Máy AD cài dịch vụ **IIS** và **Enterprise CA**

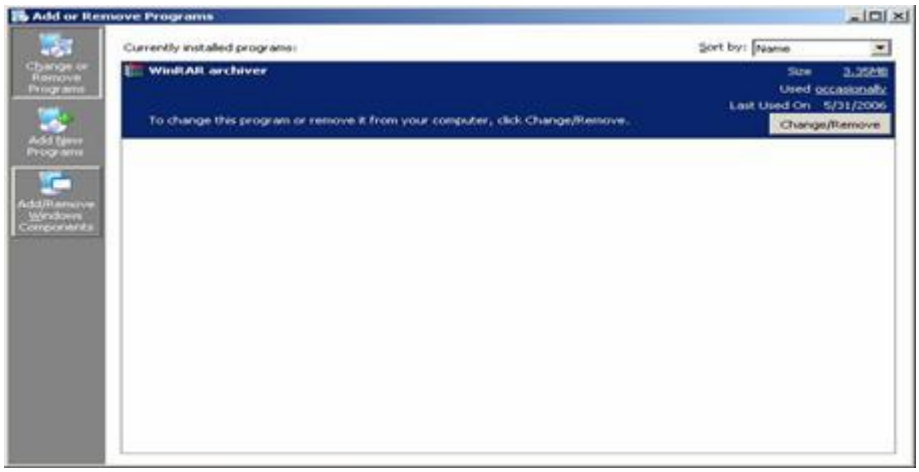
Ta bấm vào **Start** rồi chọn **Setting** rồi chọn **Control Panel**

Màn hình **Control** xuất hiện: Ta chọn **Add or Remove Programs**



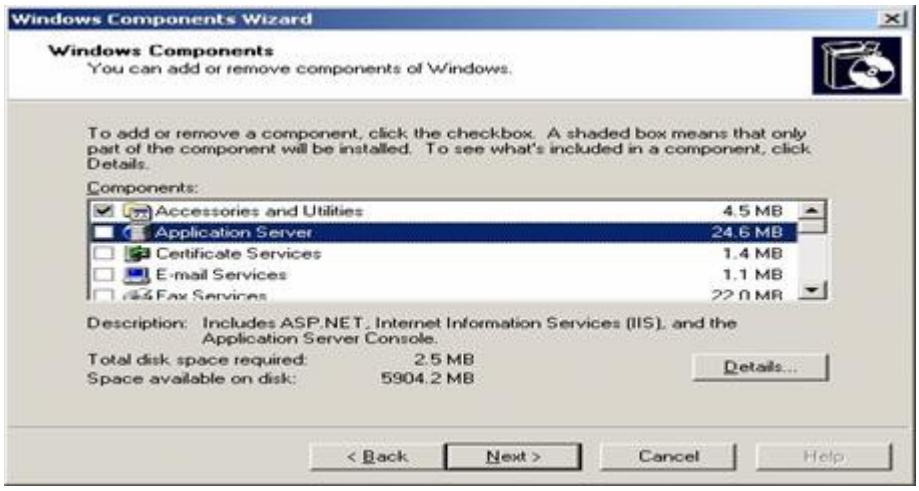
Màn hình **Add or Remove Programs** xuất hiện

Ta bấm vào **Add\Remove Windows Components**



Màn hình **Windows Components Wizard** xuất hiện

Ta chọn **Application Server** rồi bấm vào nút **Detals**

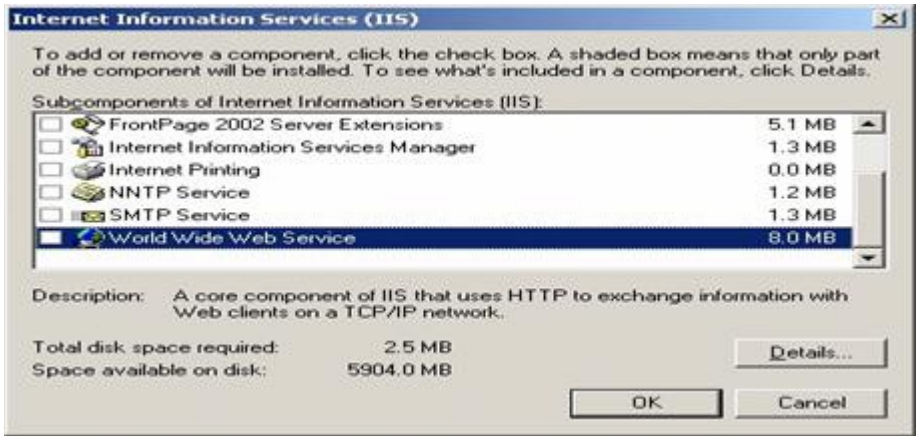


Màn hình **Application Server** xuất hiện

Ta chọn **Internet Information Service (IIS)** rồi bấm nút **Details**

Màn hình **Internet Information Services (IIS)** xuất hiện

Ta chọn **World Wide Web Service** rồi bấm **Details**



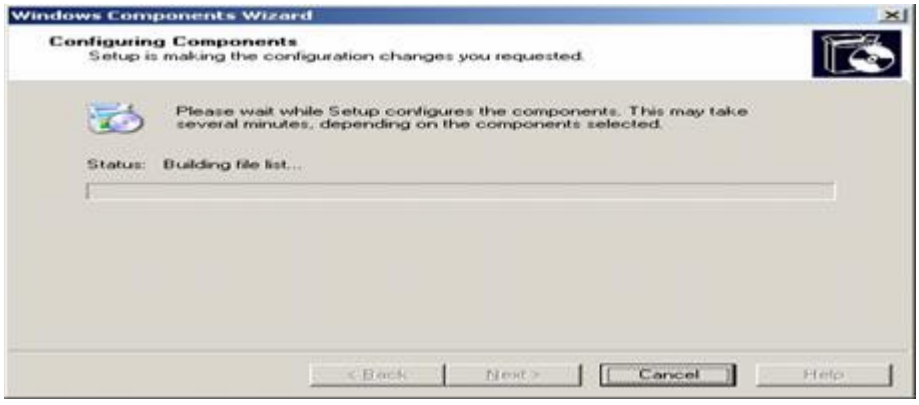
Màn hình **World Wide Web Service**

Ta chọn **World Wide Web Service** rồi bấm **OK** rồi bấm 2 lần **OK** nữa

Thì lúc này ta trở về màn hình **Windows Components Wizard**

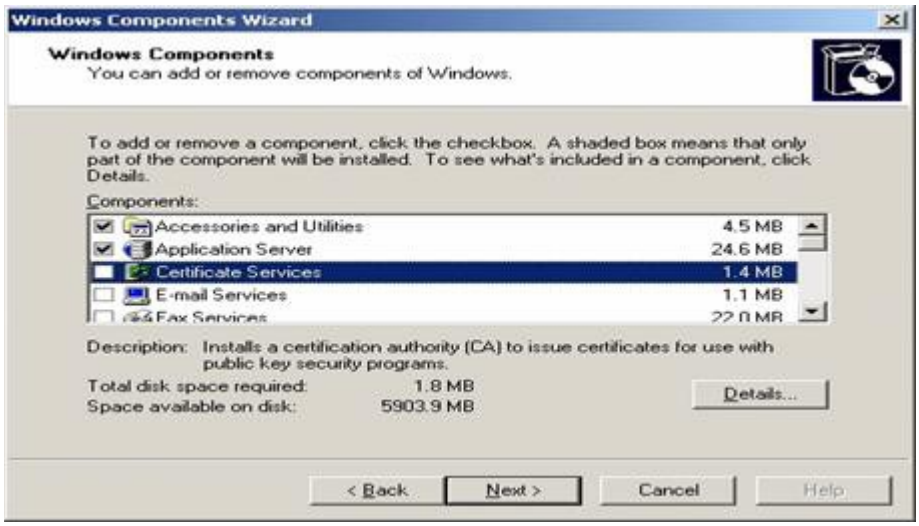
Ta thấy **Application Server** có đánh dấu và ta bấm **Next**

Màn hình cài **IIS** chạy



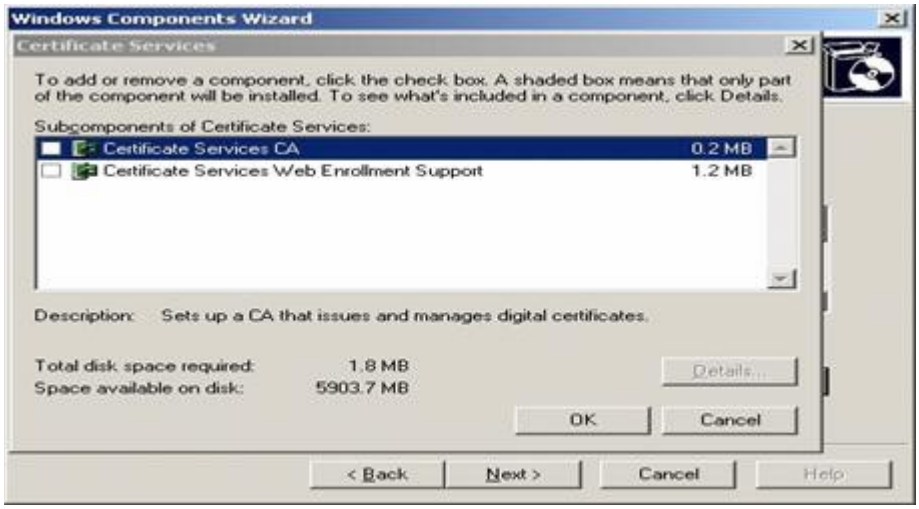
Sau khi cài **IIS** xong thì ta tiếp tục cài **Enterprise CA**

Ta chọn **Certificate Services** rồi bấm **Details**

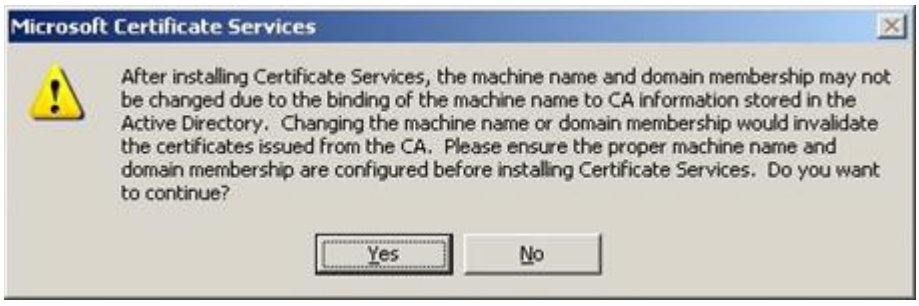


Màn hình **Certificate Services** xuất hiện

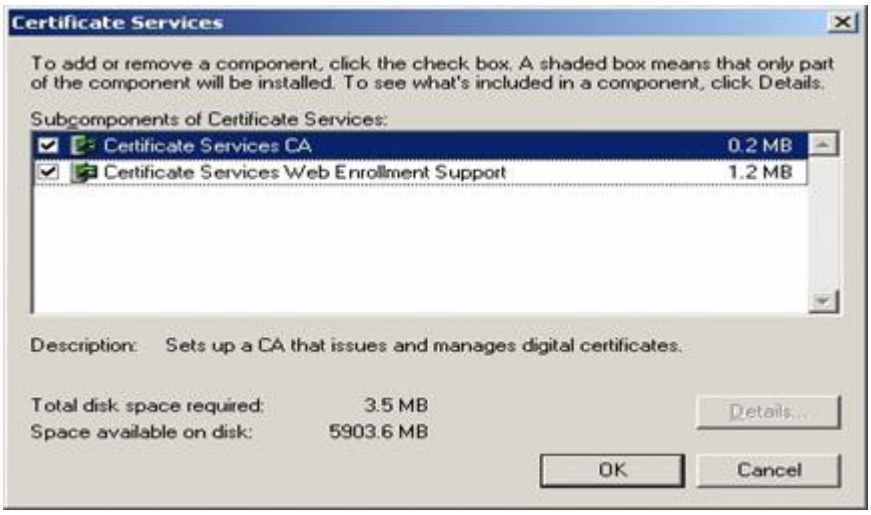
Ta chọn **Certificate Services Ca**



Màn hình hiện ra **Microsoft Certificate Services:** Ta chọn **Yes**

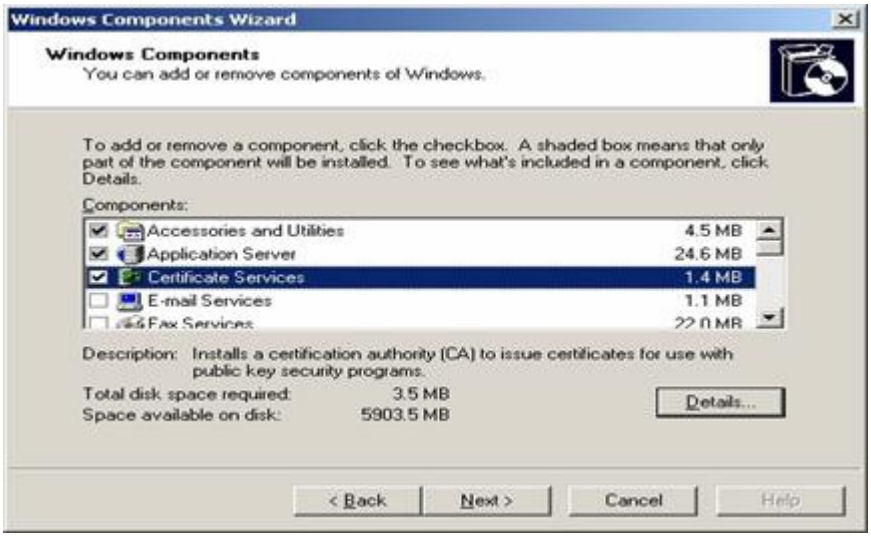


Lúc này, ta thấy **Certificate Services CA** và **Certificate Services Web Enrollment Support** đã được đánh dấu ta bấm **OK**

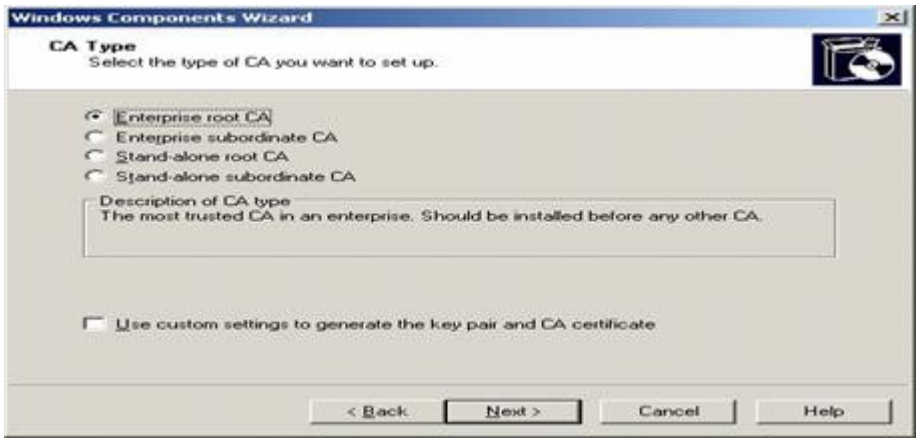


Lúc này ta thấy màn hình **Windows Components Wizard**

Ta thấy **Certificate Services** lúc này được đánh dấu và ta bấm **Next**

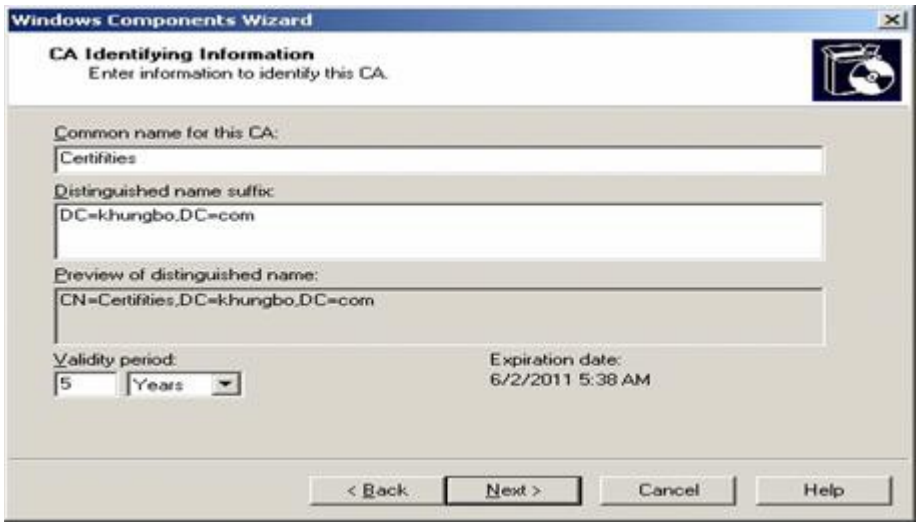


Màn hình **CA type** xuất hiện: Ta chọn **Enterprise root CA** rồi bấm **Next**

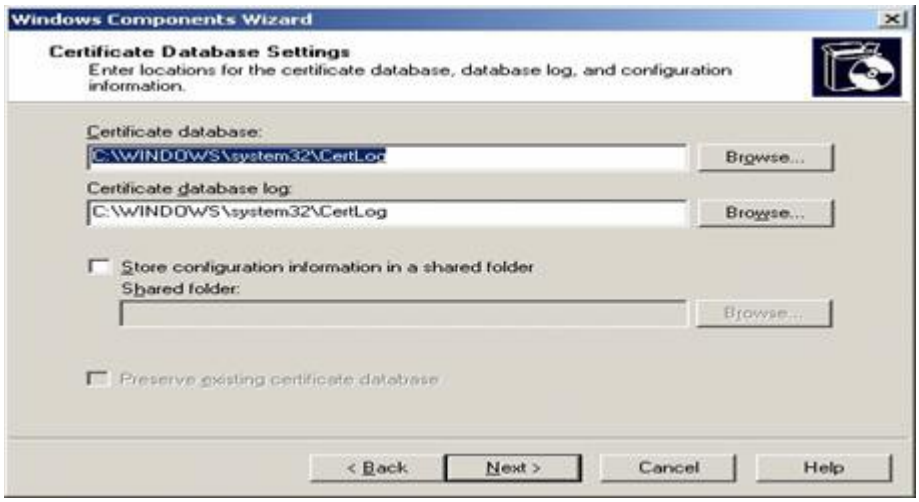


Màn hình **CA Identifying Information** xuất hiện

Common name for this CA: ta điền **Certifities** rồi **Next**

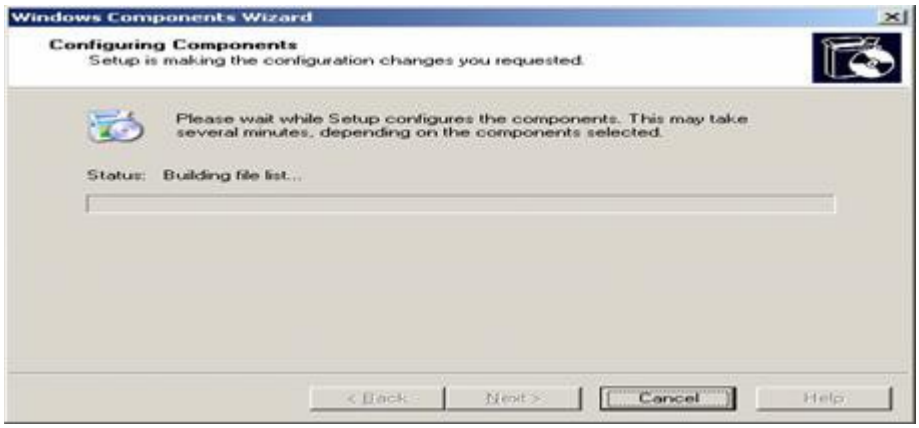


Màn hình **Certificate Database Settings** xuất hiện: Ta tiếp tục bấm **Next**

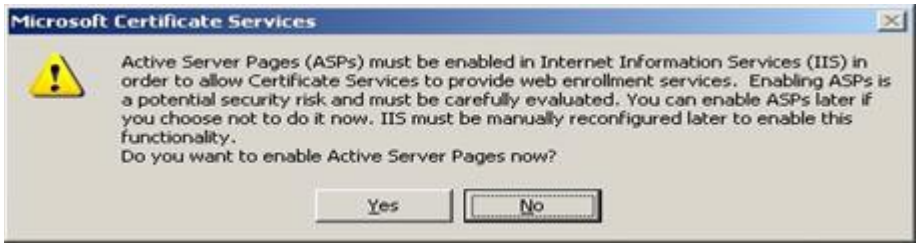


Màn hình **Microsoft Certificate Services** xuất hiện: Ta bấm **Yes**

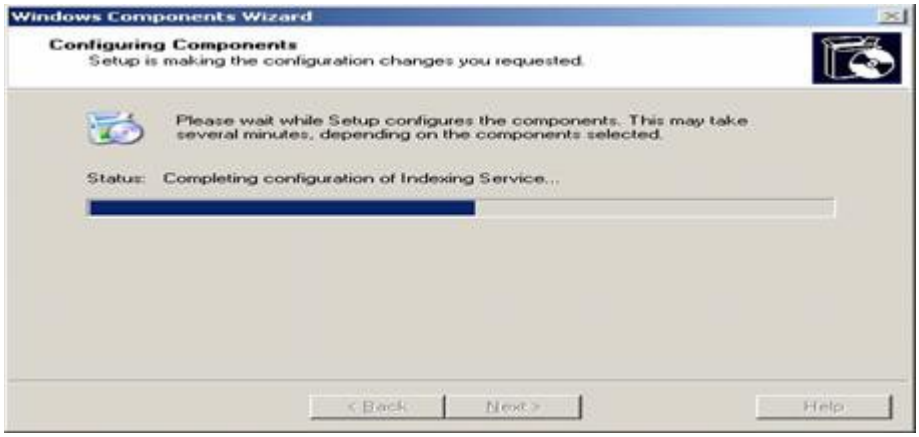
Màn hình **Configuring Components** xuất hiện và bắt đầu cài **Enterprise CA**



Trong quá trình cài **Enterprise CA** nó sẽ ngừng lại và xuất hiện màn hình **Microsoft Certificate Services**



Tiếp tục chọn **Yes** để chương trình tiếp tục cài

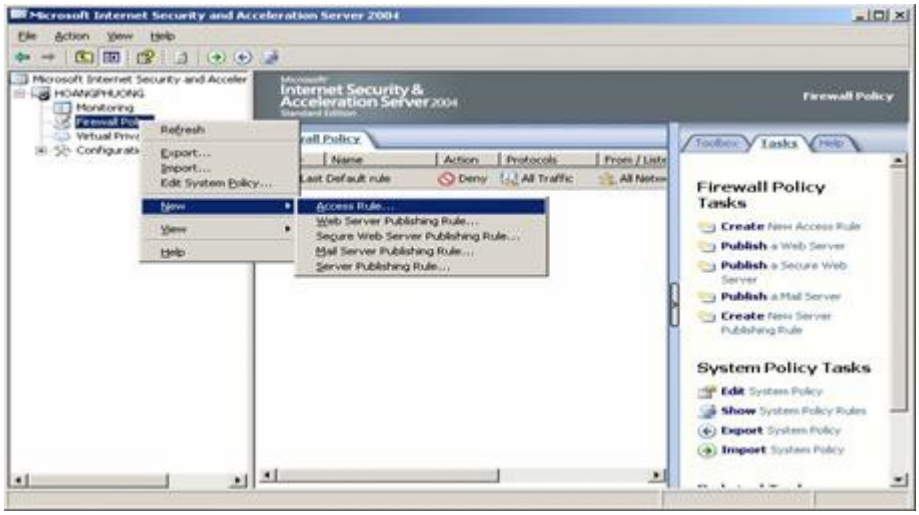


Sau khi cài xong chọn **Finish.** Vậy là đã cài xong **IIS** và **Enterprise CA**

Máy ISA

Bây giờ ta đi xin chứng nhận **CA** cho **máy ISA**. Để xin chứng nhận **Certificate** dễ dàng ta cần phải tạo ra **1 rule** để cho **Local** thông với **Internal.** Và sau khi chứng nhận **Certificate** thành công ta phải xoá rule này đi.

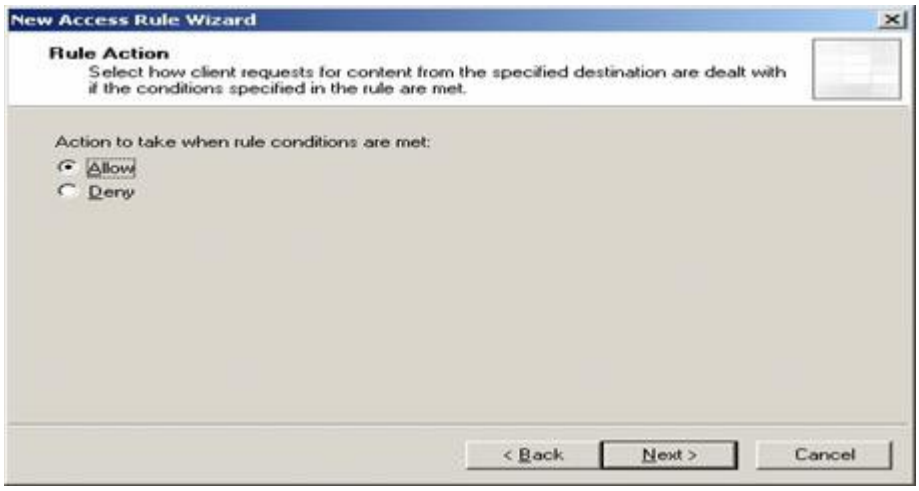
Ta chọn **Firewall Policy** rồi nhắp chuột phải chọn **New** rồi **Access Rule**



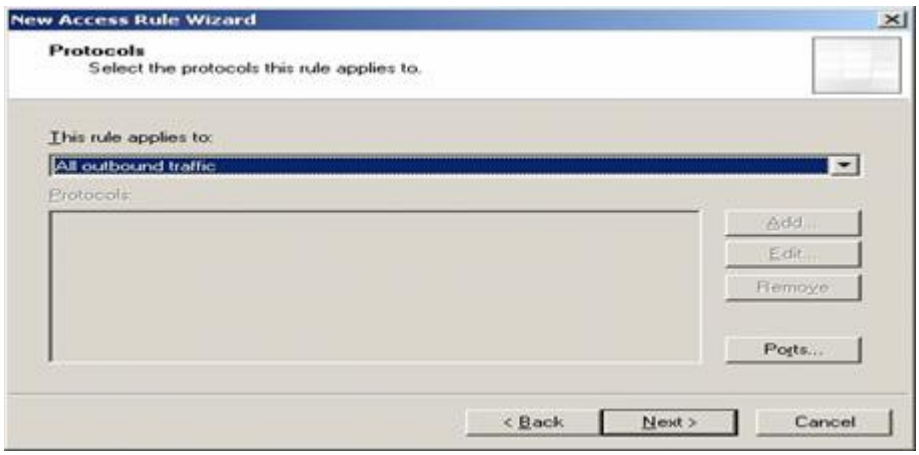
Màn hình **Wellcome to the New Access Rule Wizard** xuất hiện

Access rule name: Ta điền **All Open from Local Host to Internal** rồi **Next**

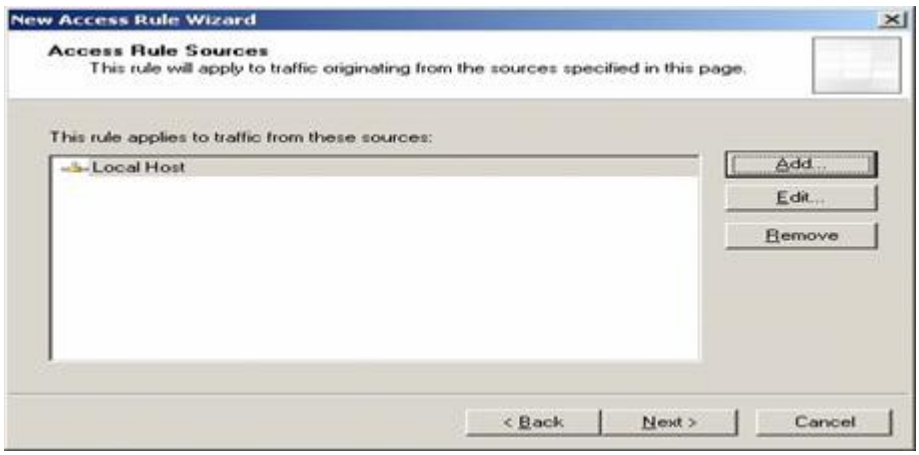
Màn hình **Rule Action** xuất hiện: Ta chọn **Allow**



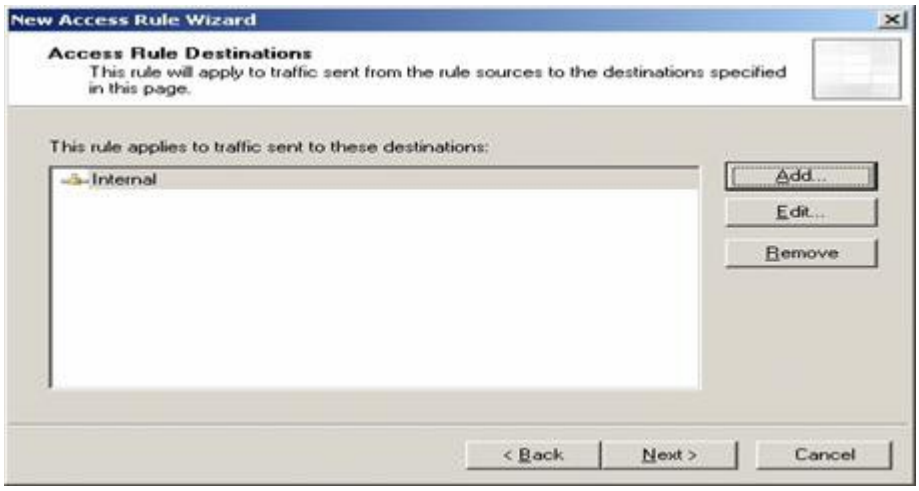
Màn hình **Protocols** xuất hiện: Ta chọn **All outbound traffic** rồi bấm **Next**



Màn hình **Access Rule Source** xuất hiện: Ta bấm nút **Add** rồi chọn **network** ta chọn **Local Host** rồi **Close** sau đó **Next**



Màn hình **Access Rule Destination** xuất hiện: Ta bấm **Add chọn Network** rồi chọn **Internal** sau đó **Close** rồi **Next** tiếp tục

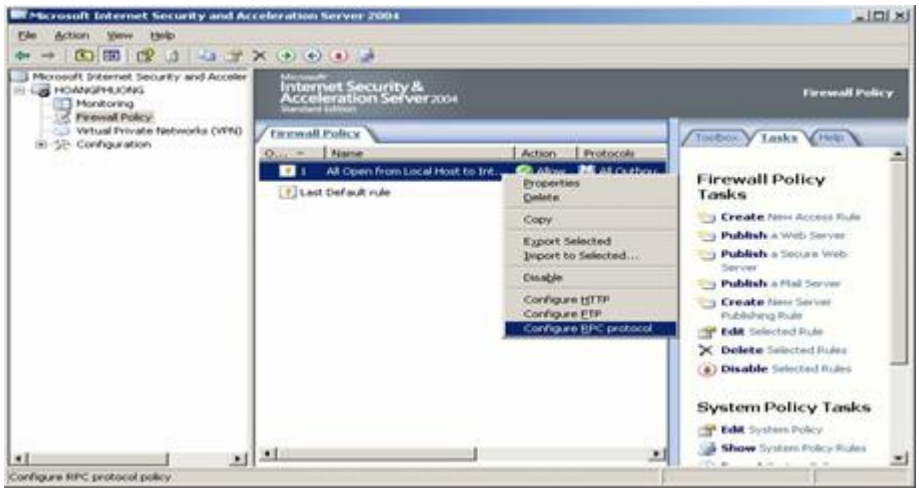


Màn hình **User Sets** xuất hiện: Ta chọn **All Users** rồi **Next**

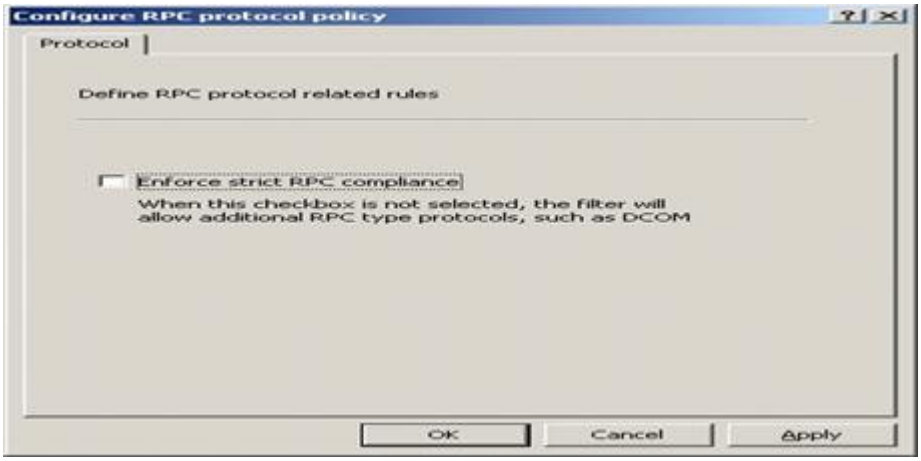
Màn hình **Completing the New Access Rule Wizard** xuất hiện: Ta bấm **Finish** rồi sau đó **Apply**

Sau khi tạo xong **rule All Open from Local host** to **Internal**

Ta bấm vào **rule All Open from Local Host to Internal** rồi nhắp chuột phải chọn **Configue RPC protocol**

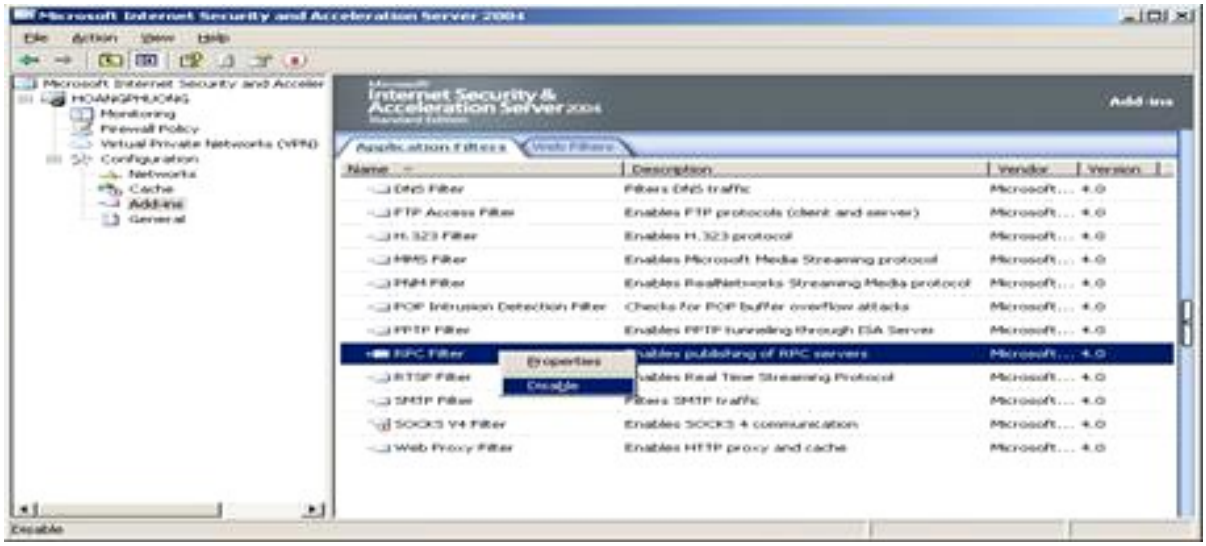


Màn hình **Configure RPC protocol policy** xuất hiện: ta bỏ dấu **Enforce strict RPC compliance** đi rồi bấm **OK** sau đó Apply



Ta chọn tiếp **Configuration** rồi chọn **Add-ins**

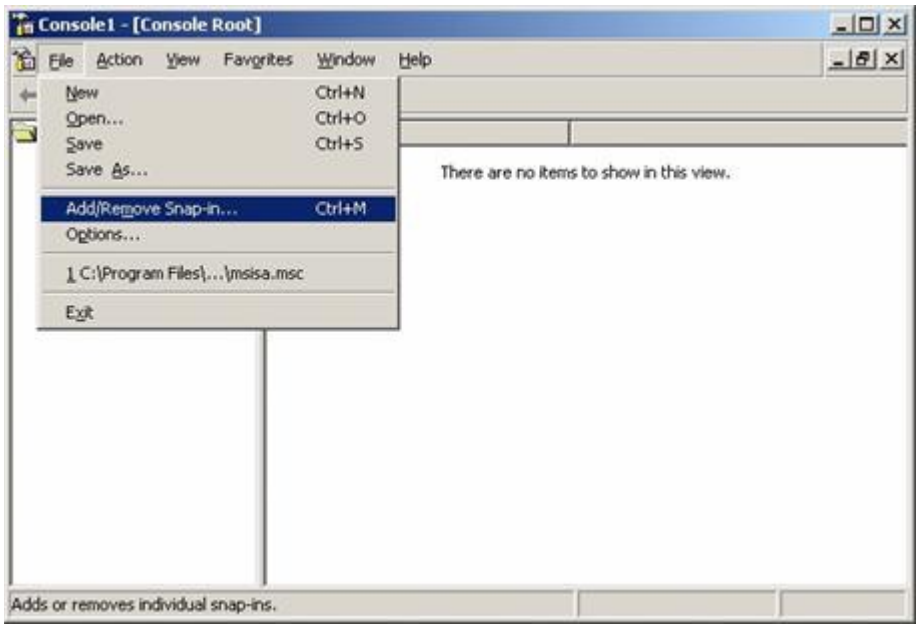
Chọn **RPC Filter** nhắp chuột phải và chọn **Disable**



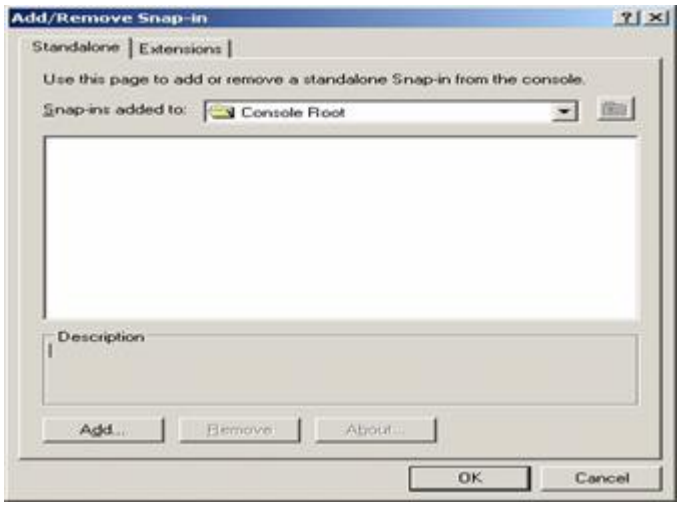
Màn hình **ISA Server Warning:** chọn **Save the change and restart the services**

Ta bấm vào **Start** rồi chọn **Run** hộp thoại **Run** xuất hiện ta bấm **mmc**

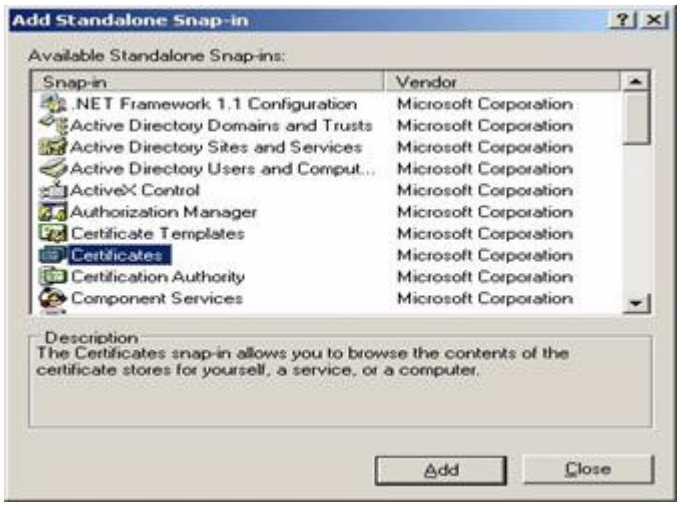
Màn hình **Console** xuất hiện ta bấm vào **File** rồi chọn **Add/Remove Snap-in**



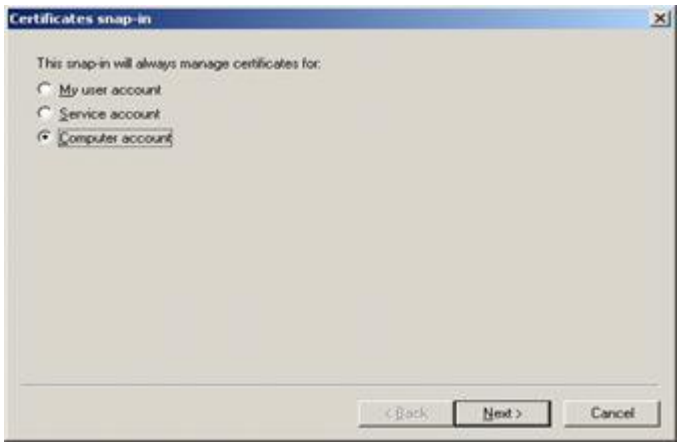
Màn hình **Add/Remove Snap-in** xuất hiện: Ta bấm **Add**



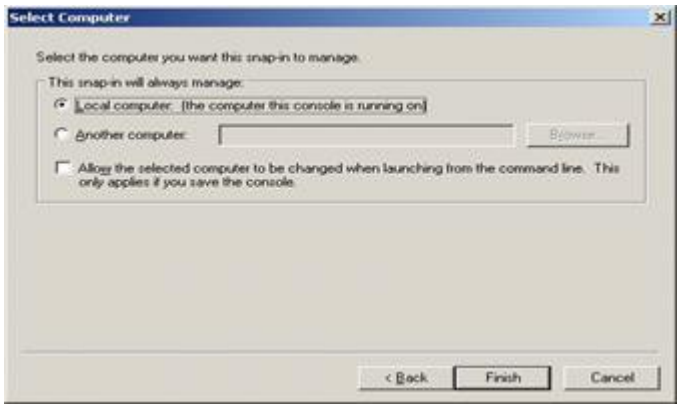
Màn hình **Standalone Snap-in** xuất hiện ta chọn **certificate** rồi bấm **Add**



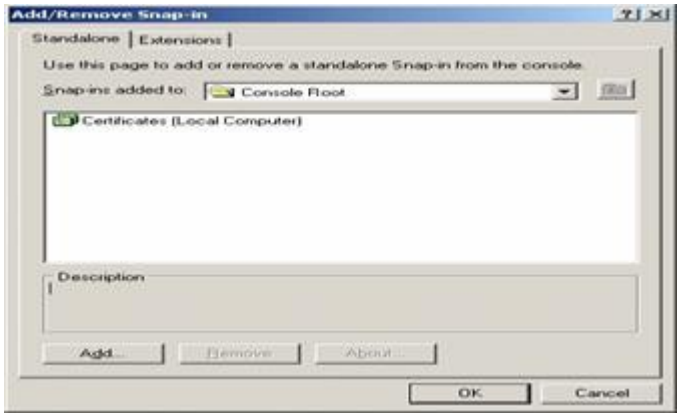
Màn hình **Certificates snap-in:** Ta chọn **Computer account** rồi **Next**



Màn hình **Select Computer** xuất hiện: Ta chọn **Local compurter** rồi **Finish**

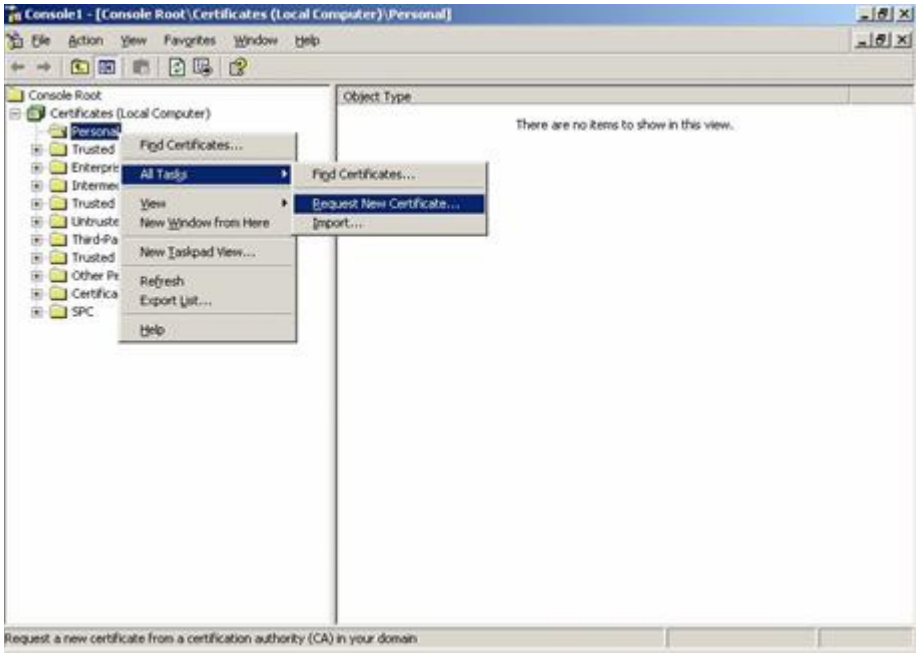


Lúc này ta thấy màn hình **Add/Remove Snap-in** đã có **Certificate (Local Computer)**



Bây giờ ta thấy **Console Root** đã có **Certificate (Local Computer)**

Ta chọn **Personal** nhấp chuột phải chọn **All Task** rồi chọn **Request New Certificate**



Màn hình **Welcome to the Certificate Request Wizard** xuất hiện: ta bấm **Next**

Màn hình **Certificate Types** xuất hiện: ta bấm **Next** tiếp tục

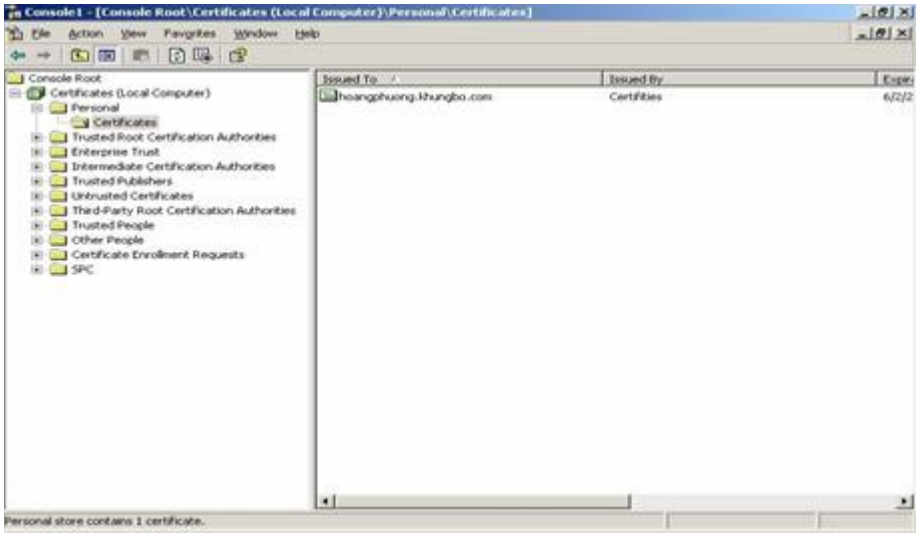
Màn hình **Certificate Friendly Name and Description**

Friendly name: ta điền **Firewall Computer Certificate**

Màn hình **Completing the Certificate Request Wizard** xuất hiện, chọn **Finish**

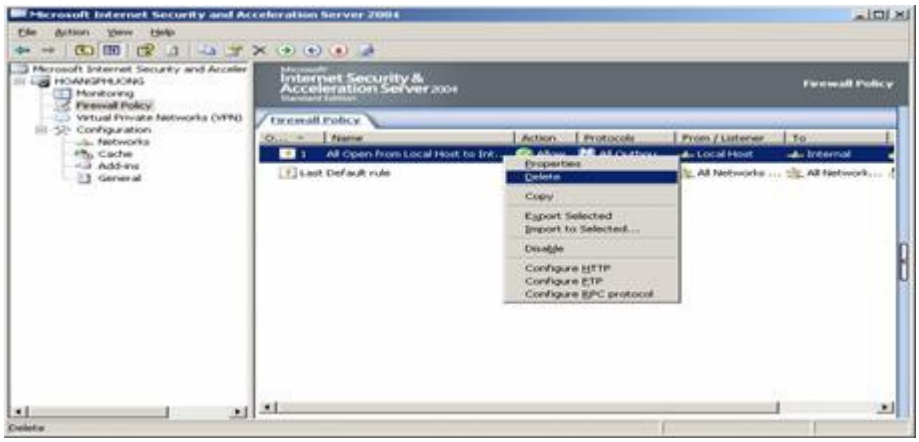
Màn hình **Certicate Request Wizard** xuất hiện báo đã xin **Certificate** thành công ta bấm **OK**

Và ta thấy **Personal** bây giờ có mục **Certificates** và có **Certificate** như đã yêu cầu

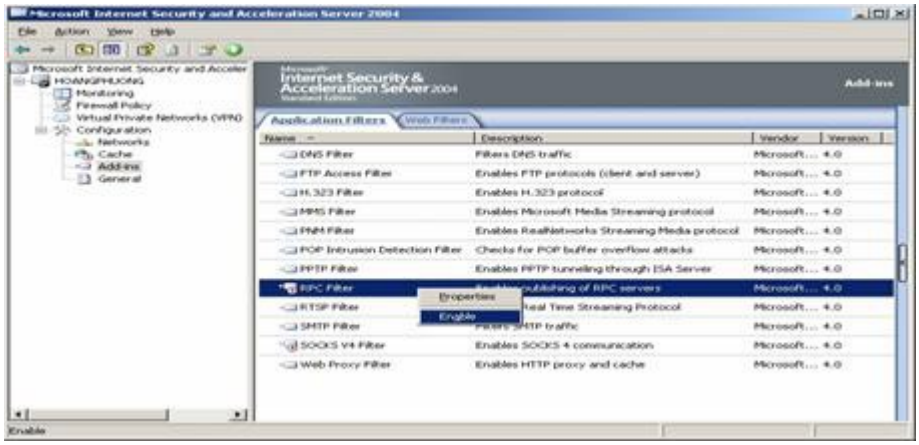


Bây giờ thì ta có thể xoá rule **All Open from Local host to Internal**

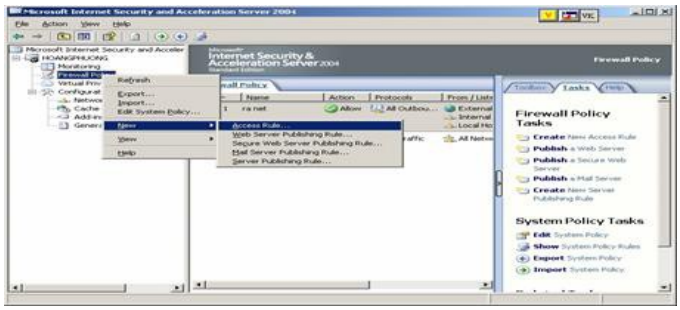
Nhắp chuột phải lên **All Open from Local Host**… chọn **Delete**; chọn **Apply**



Rồi chọn **Configuration** chọn **Add-ins** rồi chọn **RPC Fiter** nhắp chuột phải chọn **Enable**



Màn hình **ISA Server Warning:** chọn **Save the Changes and restart the service**



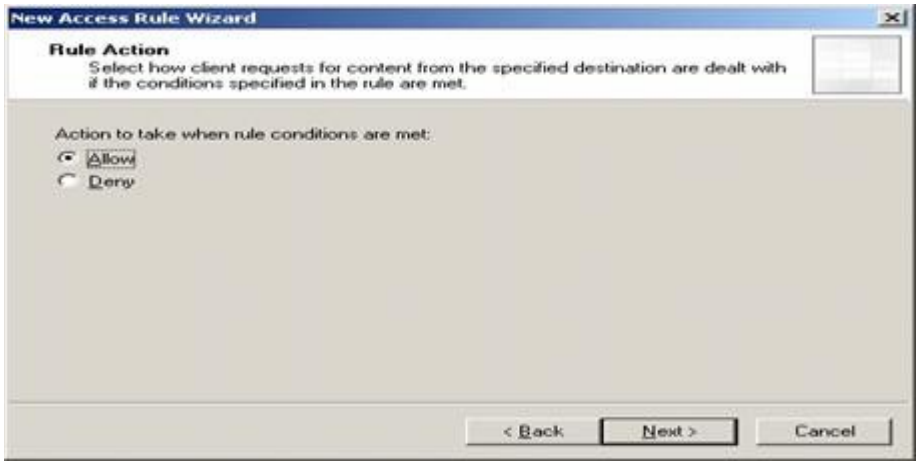
Ta đã chứng nhận **Certificate** cho **máy ISA** xong rồi bây giờ ta chứng nhận cho máy **VPN Client** là bằng cách:

Muốn chứng nhận cho máy **VPN Client** ta thực hiện **VPN** kết nối bằng **PPTP** trước (Xem lại cách cấu hình **Client** to **Site** bằng **PPTP)**

"Máy tính ngoài mạng" thực hiện kết nối **VPN** bằng **PPTP** tới máy ISA

Khi kết nối thành công **VPN** bằng giao thức **PPTP** thành công, mở chương trình **Internet Explorer.** Từ **Desktop** nhắp đúp chuột vào **Internet Explorer**

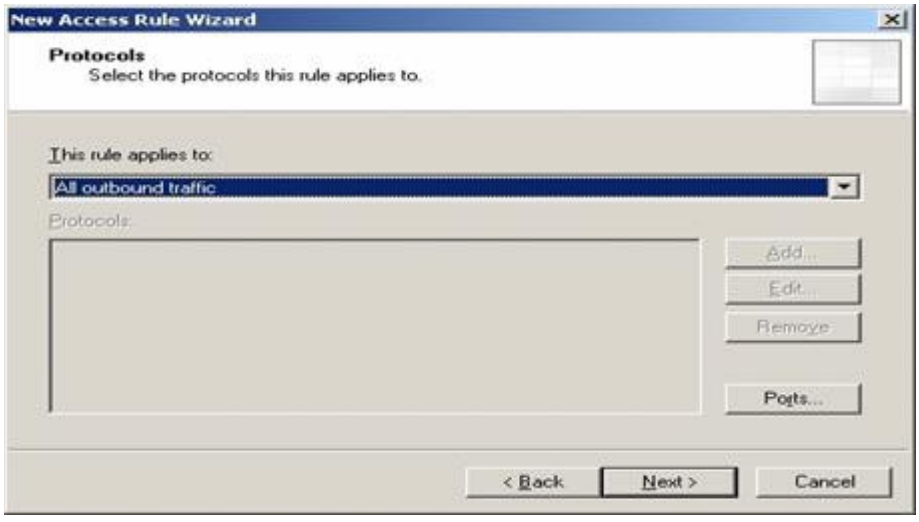
Trên thanh **Address:** ta gõ địa chỉ **http://10.0.0.2/certsrv**



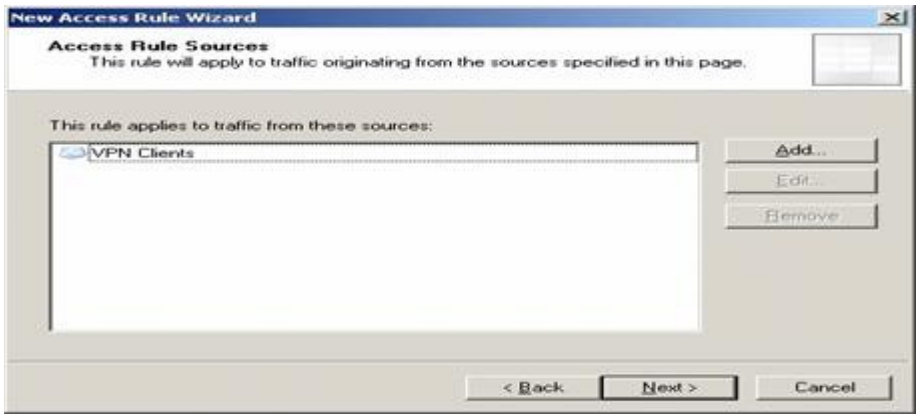
Màn hình **Connetcting to 10.0.0.2** xuất hiện:

Users name: ta điền **miền\administrator**

Password: ta điền **123456** rồi **OK**

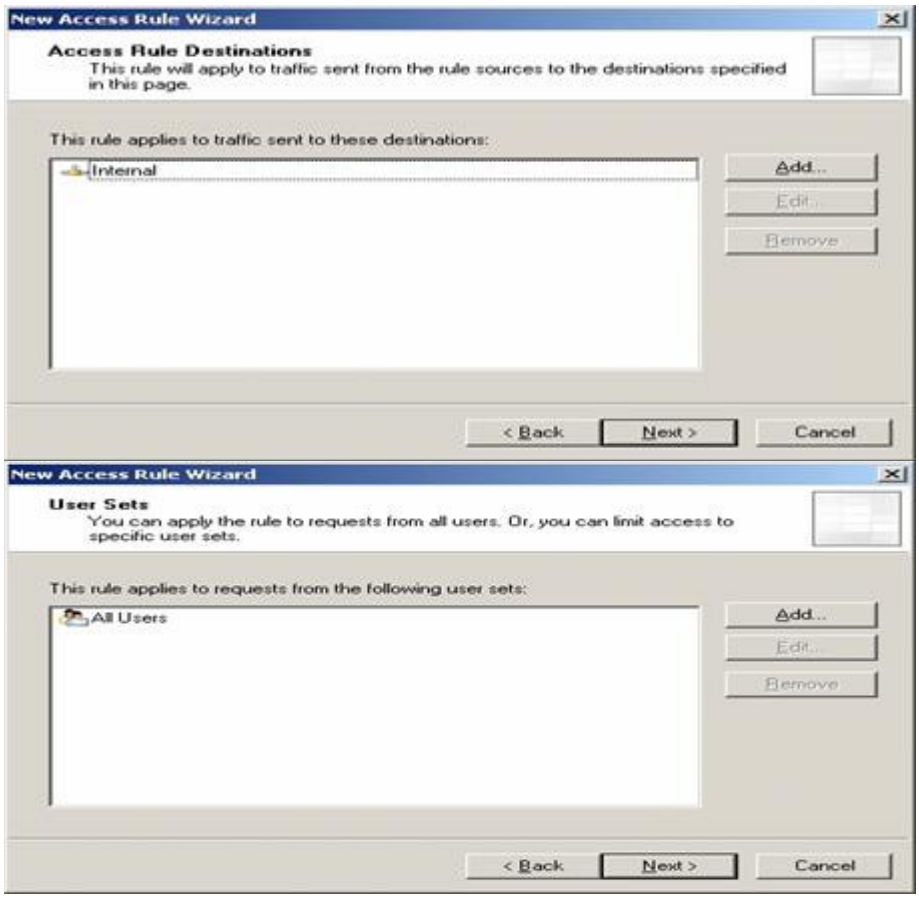


Trang web xin **Certificate** sẽ hiện ra: Ta bấm vào **Request certificate**



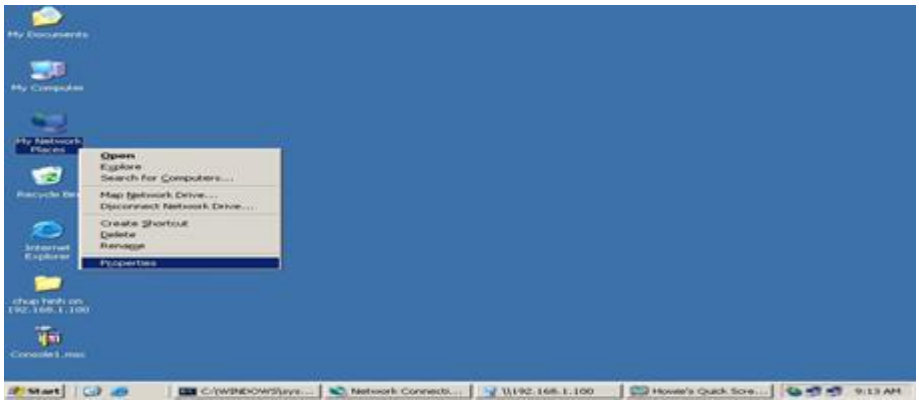
Trong màn hình **Request a Certificate**, chọn **advanced certificate request**

Trong màn hình **Advanced Certificate Request**, chọn **Create and submit a request to this CA**



Certificate Template: Ta chọn **Administrator**

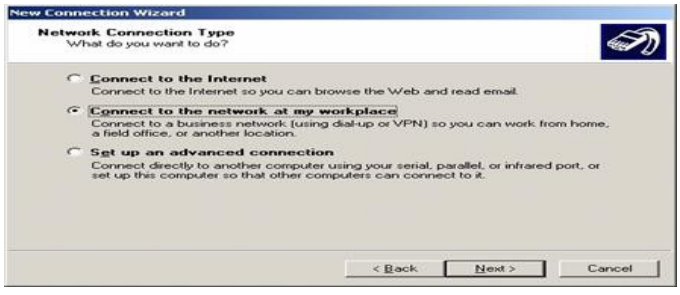
Key Options: Ta đánh dấu vào **Store certificate in the local computer certificate store** rồi bấm **Submit**



Trong hộp thoại **Potential Scripting Violation,** bấm **Yes**

Màn hình **Certificate Issued** xuất hiện: Ta bấm vào **Install this certificate**

Hộp thoại **Potential Scripting Violation** xuất hiện: Ta bấm **Yes**

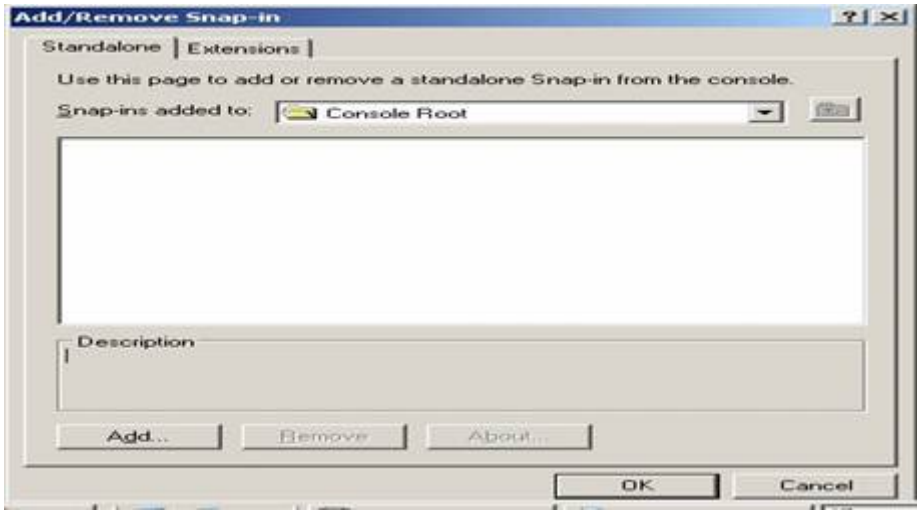


Màn hình **Certificate Installed** xuất hiện với thông báo **Your new certificate has been successfully installed**, nghĩa là đã xin thành công

Ta tiếp tục vào **Run** rồi đánh **mmc** tiếp

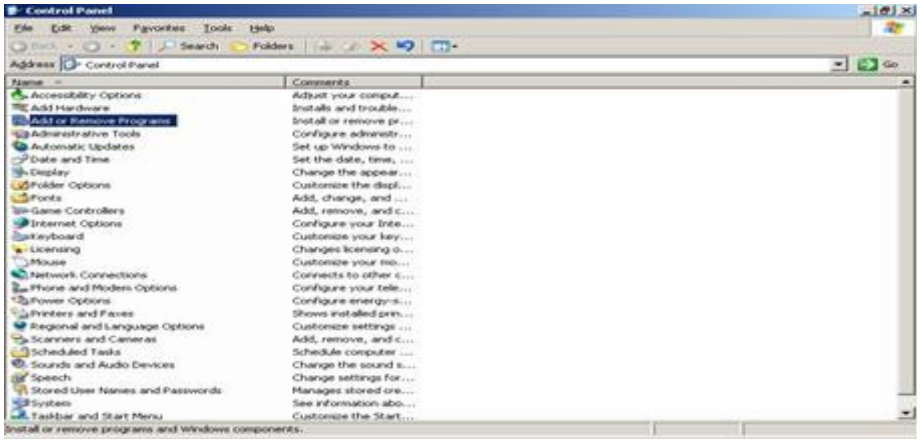
Màn hình **Console1** xuất hiện: Ta bấm vào **File** rồi **Add/Remove Snap-in**

Màn hình **Add/Remove Snap-in** xuất hiện: Ta bấm **Add**

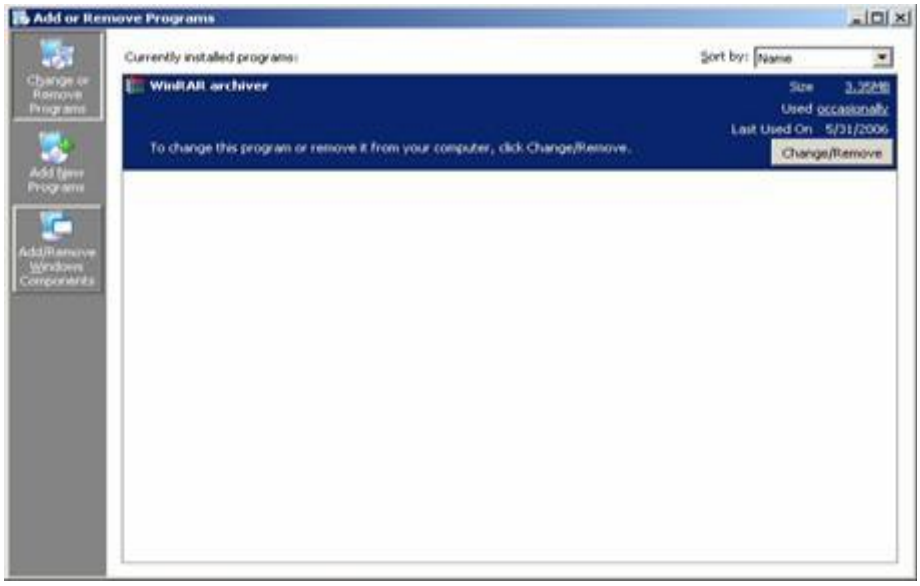


Màn hình **Add Standlone Snao-in** xuất hiện: Ta chọn **Certificate** rồi **Add**

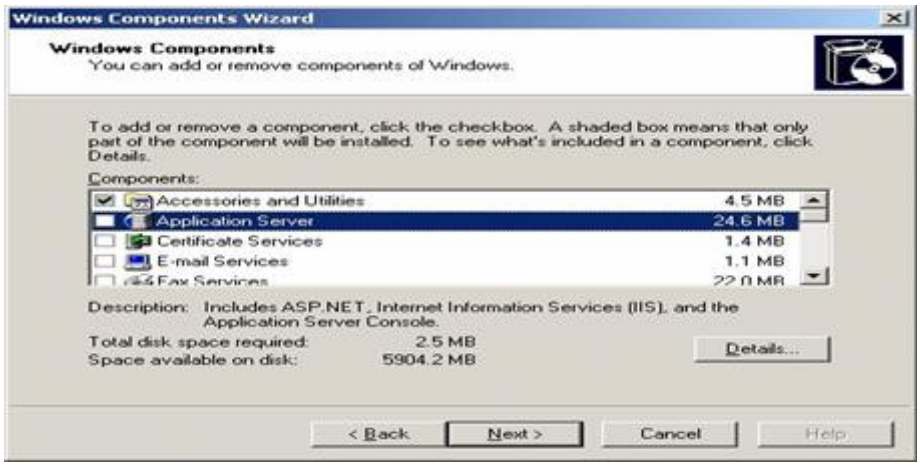
Màn hình **Certificate Snap-in** xuất hiện, chọn **Computer account** rồi **Finish**



Màn hình **Select Computer** xuất hiện: Ta chọn **Local computer** rồi **Finish**

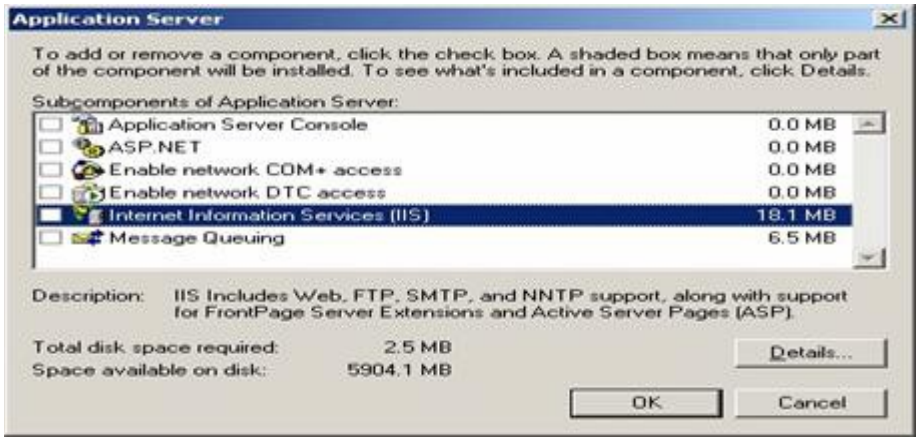


Bây giờ ta thấy màn hình Add/Remove Snap-in có Certicate (local Computer) rồi OK

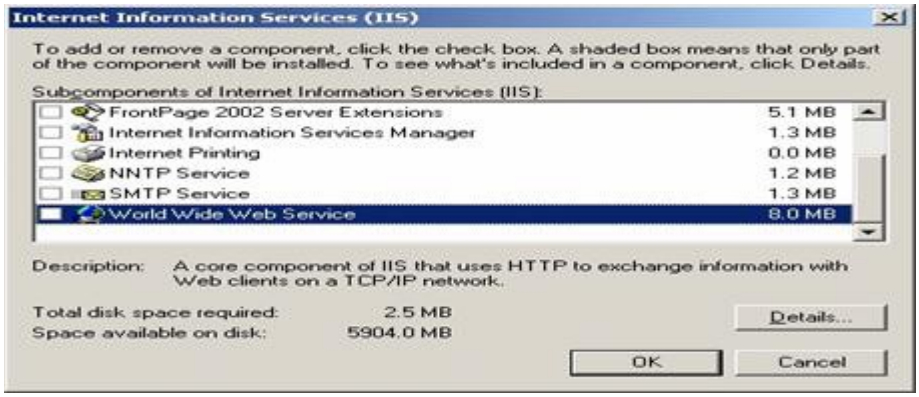


Bây giờ màn hình **Console1** có **Certificate (Local Computer)**

Ta nhắp vào **Personal** rồi **Certificate** rồi nhắp đôi chuột vào **Administrator**



Màn hình **Certificate** xuất hiện: Ta chọn Tab **Certification Path**

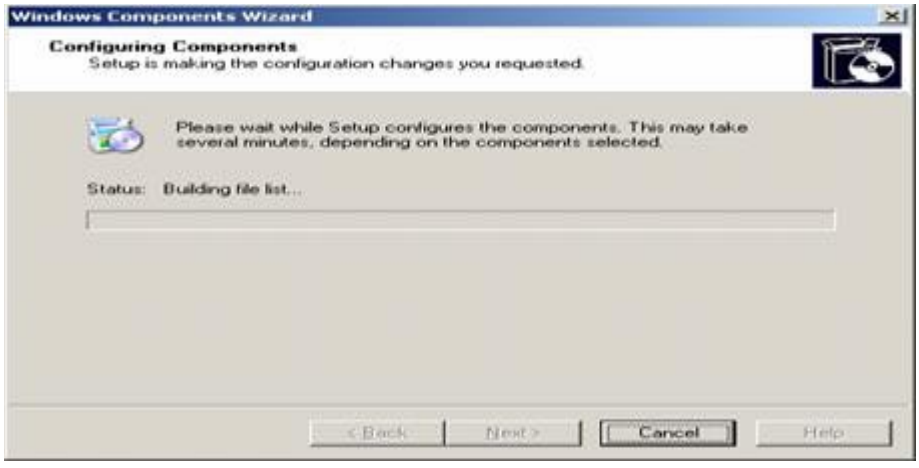


Ta thấy **Certification path** nó vẫn có dấu chéo đỏ

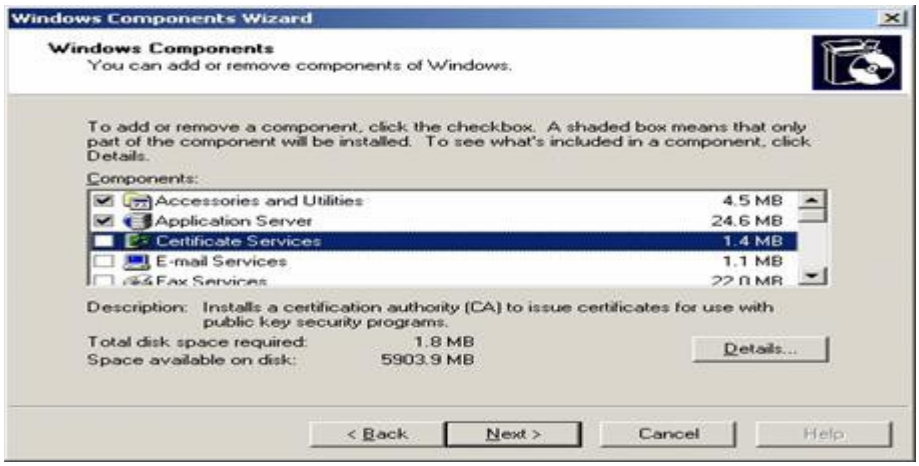
Ta chọn **Certifities:** rồi bấm **View Certificate**

Rồi ta chọn Tab **Details** rồi bấm **Copy to File**

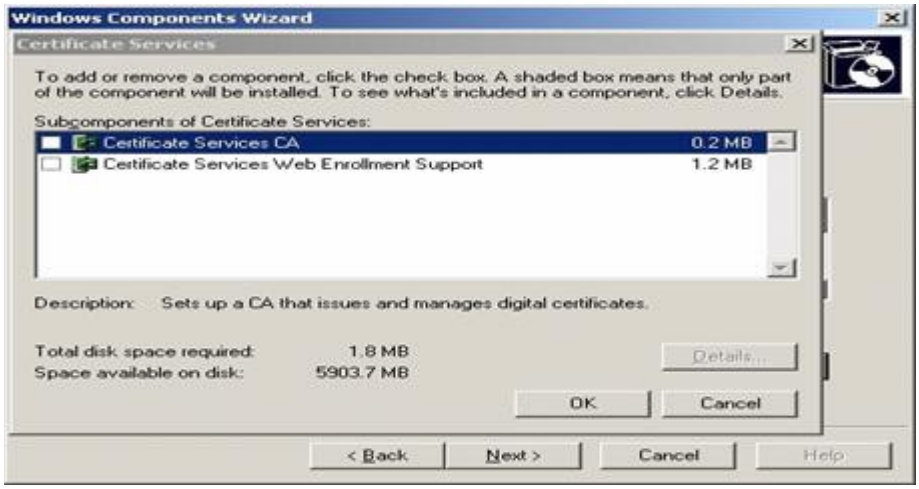
Màn hình **Welcome to the Certificate Export Wizard** xuất hiện, chọn **Next**



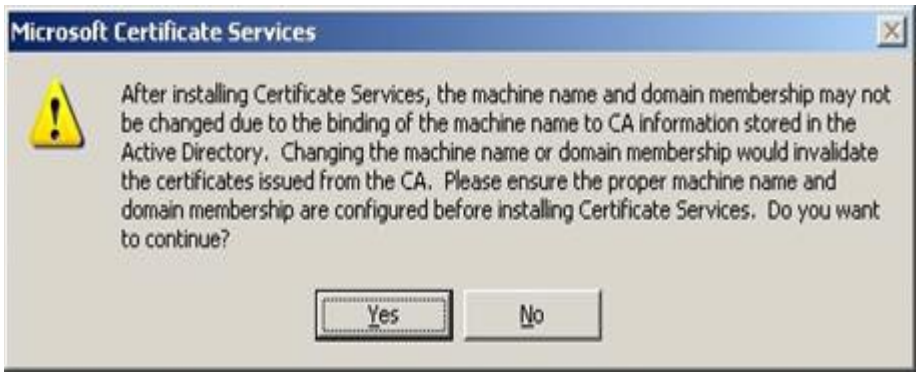
Trong cửa sổ **Export File Format**, chọn **Cryptographic Message Syntax Standard – PKCS #7 Certificate** và đánh dấu vào **Include all certificate in the certification path if possble**, chọn **Next**



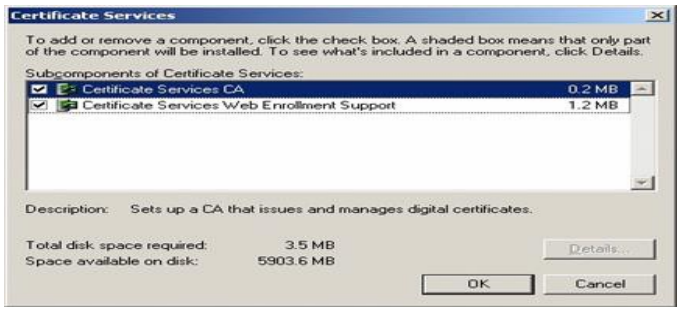
Màn hình **File to Export** xuất hiện; trong **File name**, điền **C:\CA_Certificate** rồi **Next**



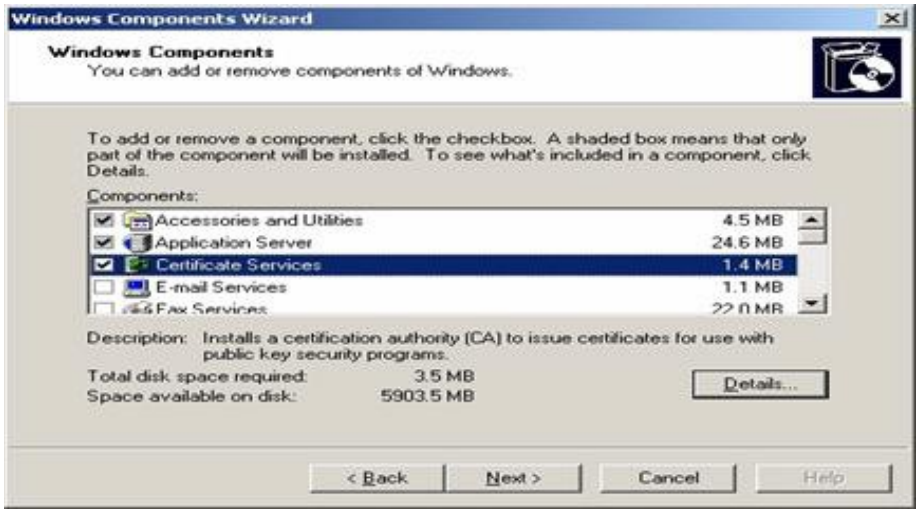
Màn hình **Completing the Certificate Export Wizard** rồi bấm **Finish**



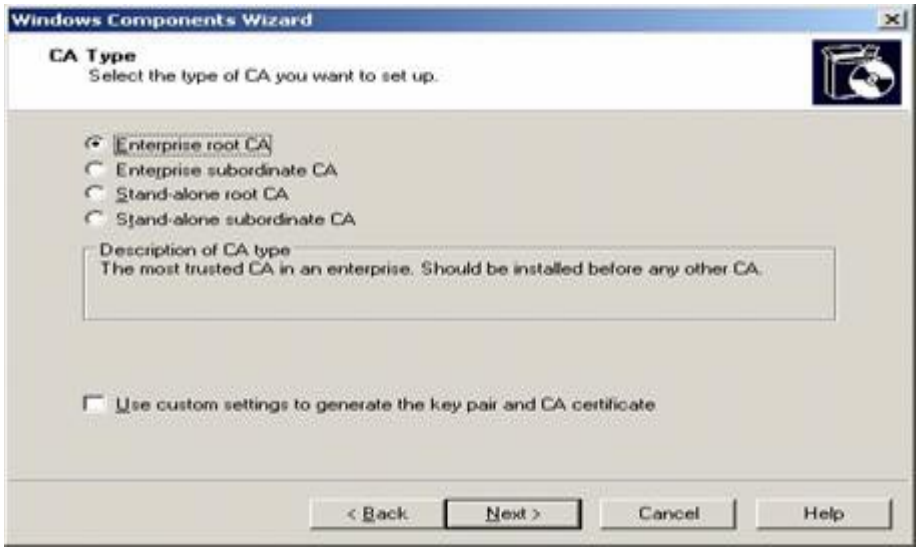
Hộp thoại **Certificate Export Wizard** báo là **The export was successful** ta bấm **OK**; Rồi ta bấm **OK** mấy lần nữa



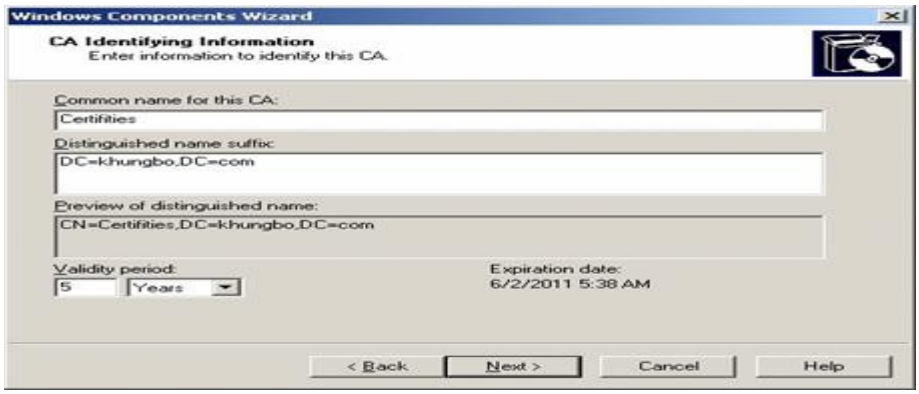
Ta lại chọn lại **Trusted Root Certificate Authorities** rồi chọn **Certaficate** bấm chuột phải chọn **All Tasks** rồi **Import**



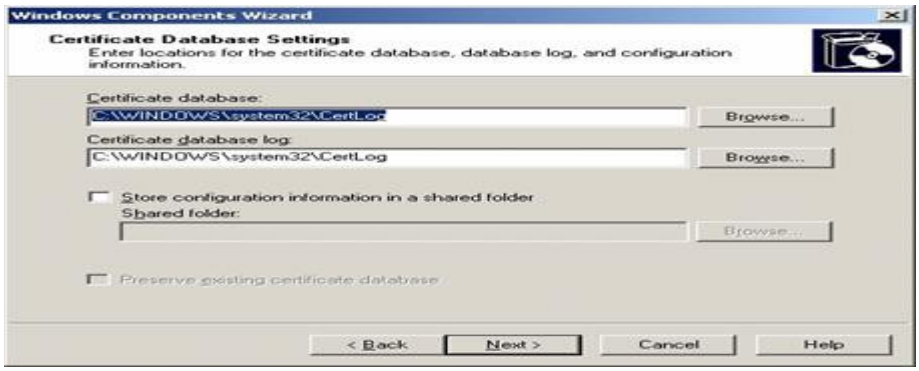
Màn hình **Welcome to the Certificate Import Wizard** rồi bấm **Next**



Màn hình **File Import** xuất hiện ta bấm **Browse**



Hộp thoại **Open** xuất hiện khung **Files of type** ta chọn là **All Files (*.*)** rồi chọn đường dẫn đến C: ta sẽ thấy **CA_Certificate** (do đã tạo ra) ta bấm vào đó rồi Open sau đó ta bấm Next

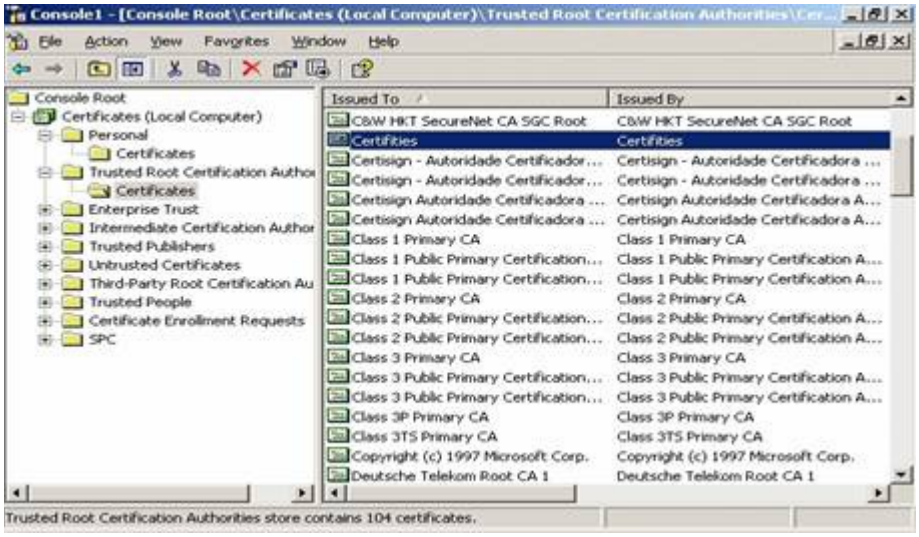


Màn hình **Certificate Store** xuất hiện

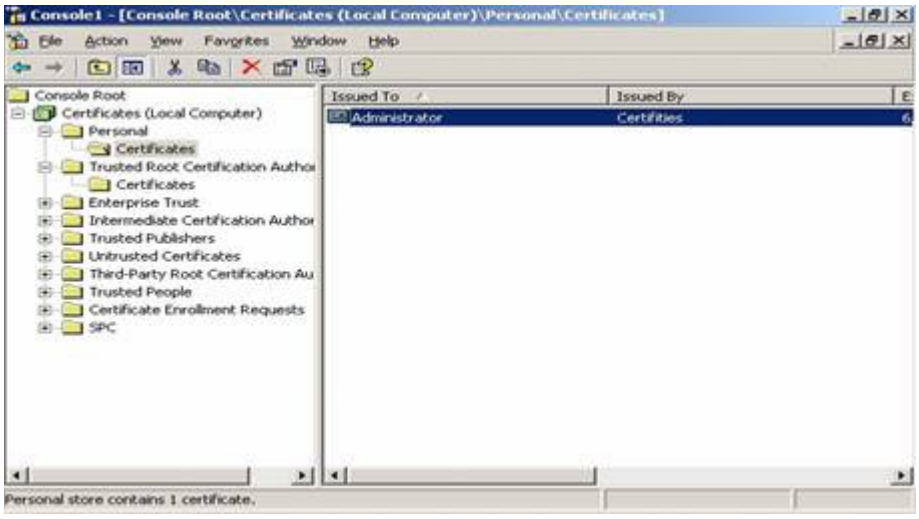
Ta chọn **Place all certificates in the following store** rồi bấm **Next**

Màn hình **Completing the Certificate Import Wizard** ta bấm **Finish**

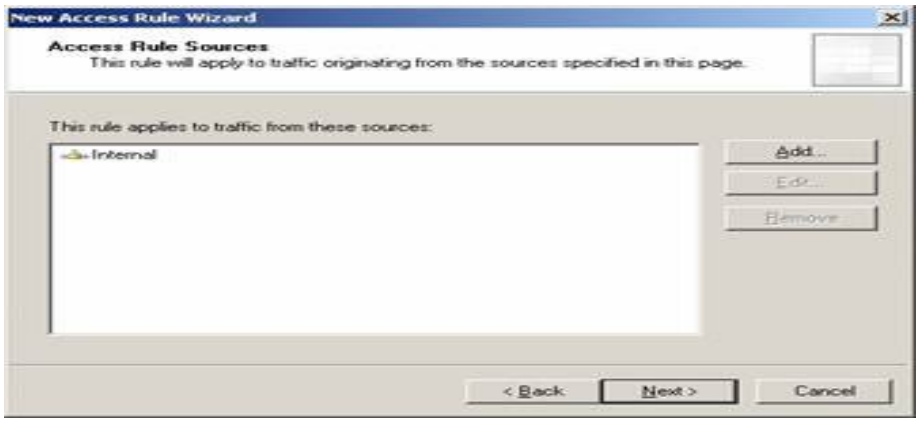
Lúc này ta thấy trong **Trusted Root Certificate Authoritoes\Certificate** thấy có **Certifities**



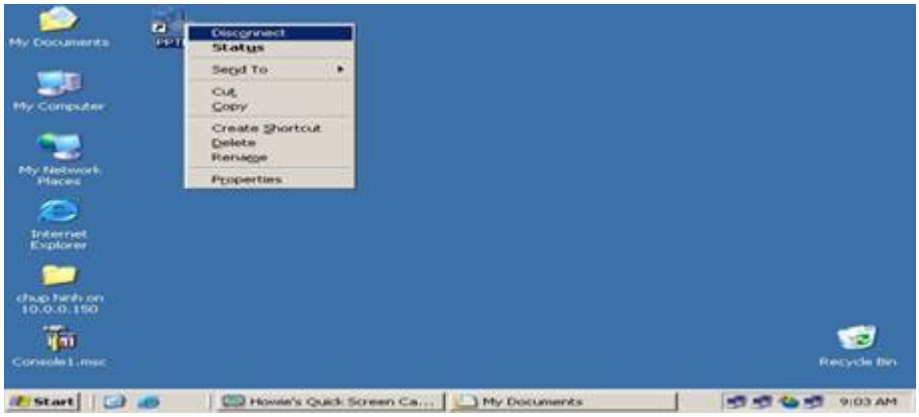
Và ta bấm lại **Personal** rồi **Certificate** rồi nhấp đúp chuột vào **Administrator**



Lúc này ta không thấy dấu chéo đỏ nữa. Sau đó ta đóng lại hết



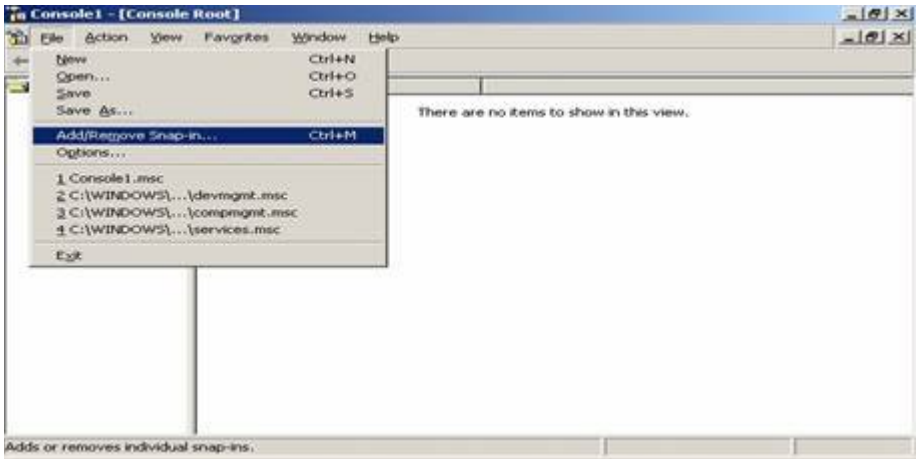
Khi đó Ta **Disconnect**



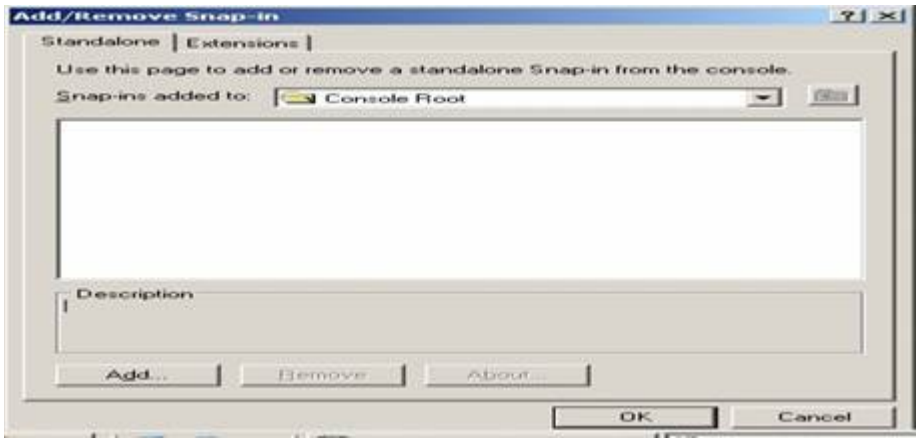
Sau khi đã chứng nhận dùng bằng **Certificate** cho máy **ISA** và **VPN Client** xong, ta tiếp tục chứng nhận cho **User** cho **VPN Client**

Ta tiếp tục Vào **Run** đánh **mmc** tiếp

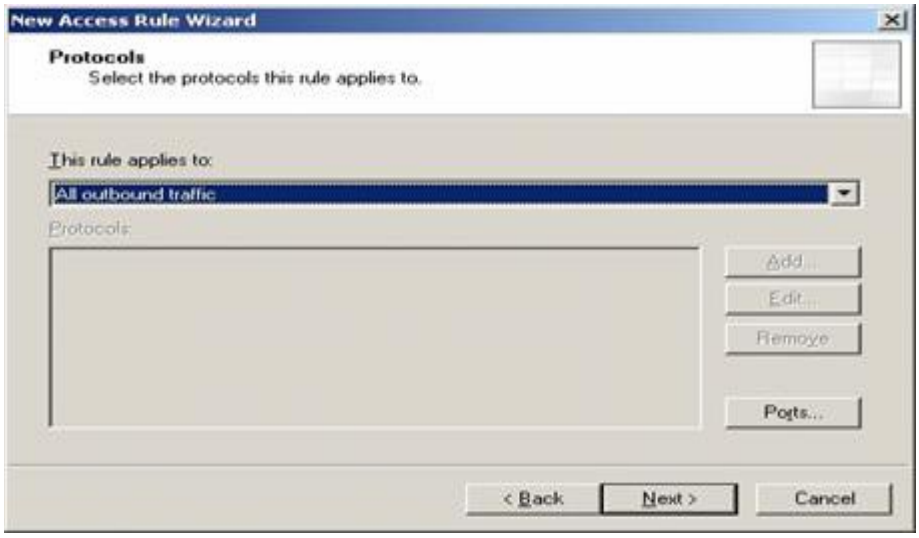
Màn hình **Console** xuất hiện: Ta chọn **File** rồi chọn **Add/Remove Snap-in**



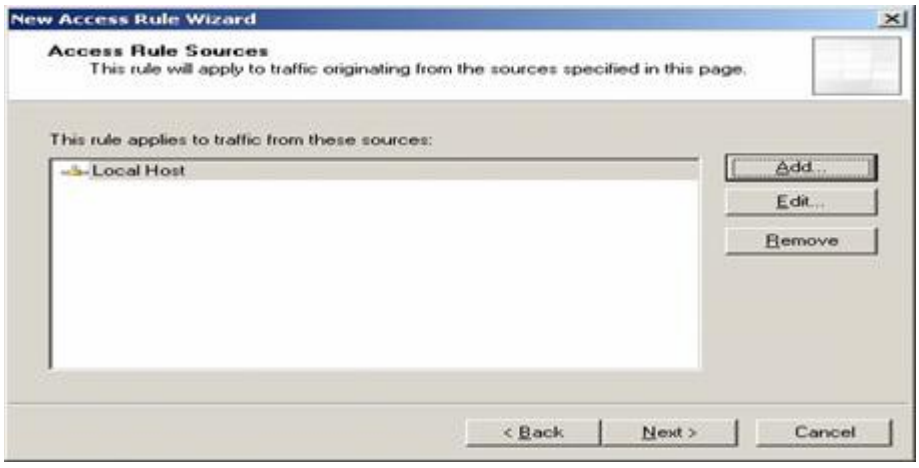
Màn hình **Add/Remove snap-in** xuất hiện Ta bấm **Add**



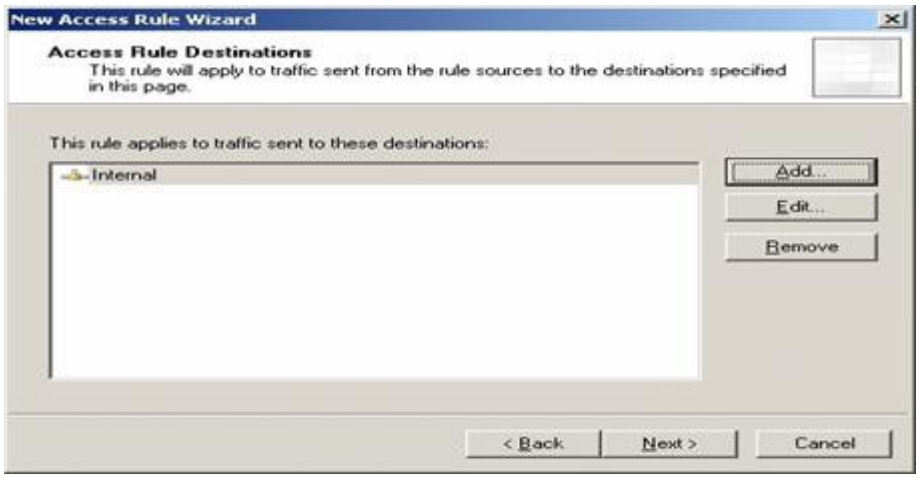
Màn hình **Add Standalone Snap-in** xuất hiện ta chọn **Certificate** rồi **Add**



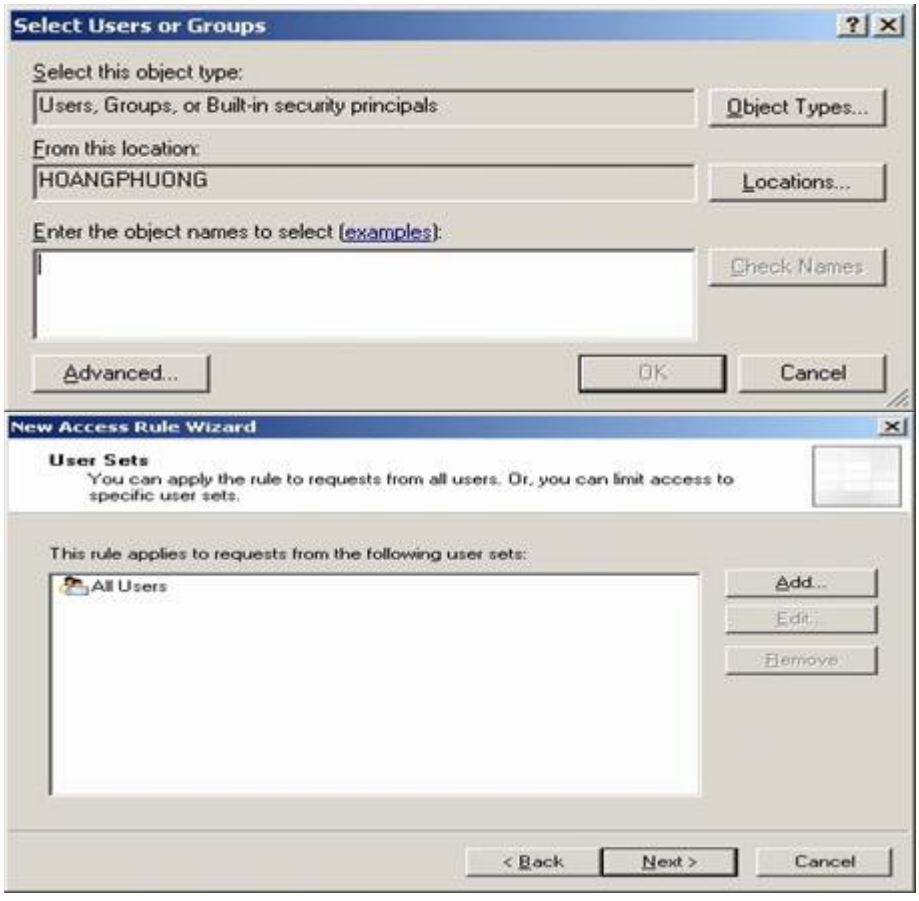
Ta chọn **My user acccount** rồi **Finish**



Ta lại tiếp tục chọn **Certificate** 1 lần nữa rồi bấm **Add**



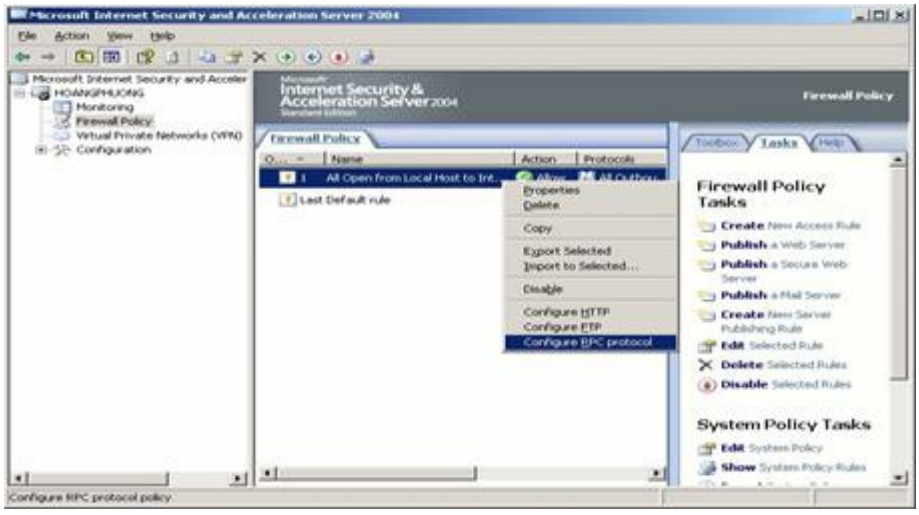
Nhưng lần này Ta chọn **Computer account**



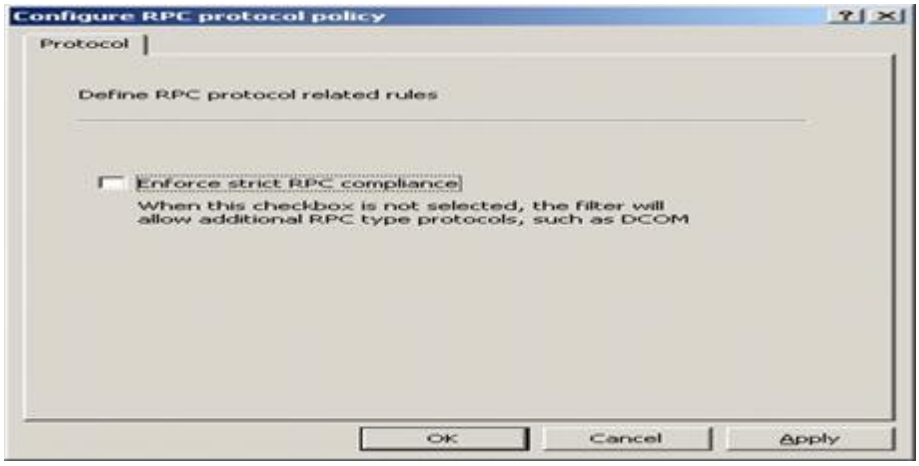
Màn hình **Select Computer:** Ta chọn **local computer** rồi **Finish**

Lúc này ta thấy màn hình **Add/Remove Snap-in** có 2 **Certificates**

Ta bấm vào **Certificate (local Computer)** rồi bấm vào **Personal** rồi **Certificate** ta **Copy Administrator**

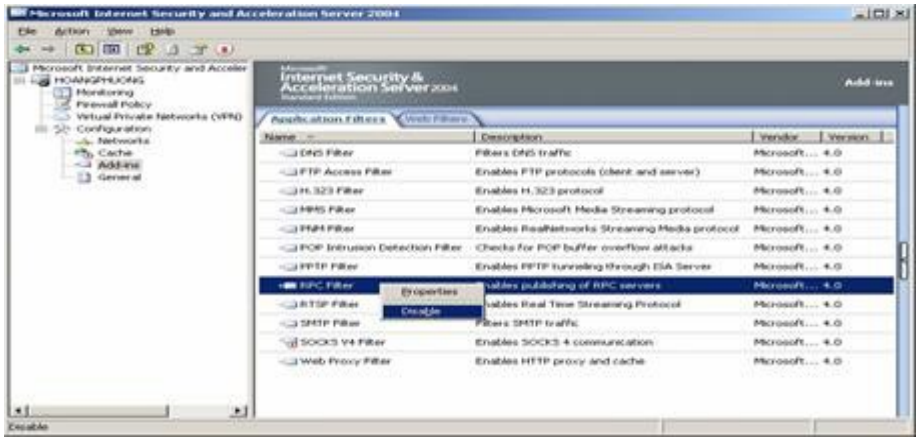


Chọn lại **Certificate –Curent User** rồi chọn **Personal** nhắp chuột phải, chọn **Paste**



Lúc này ta thấy **Certificate – Curent User**

Personal\Certificate có **Administrator** sau đó ta đóng lại tất cả

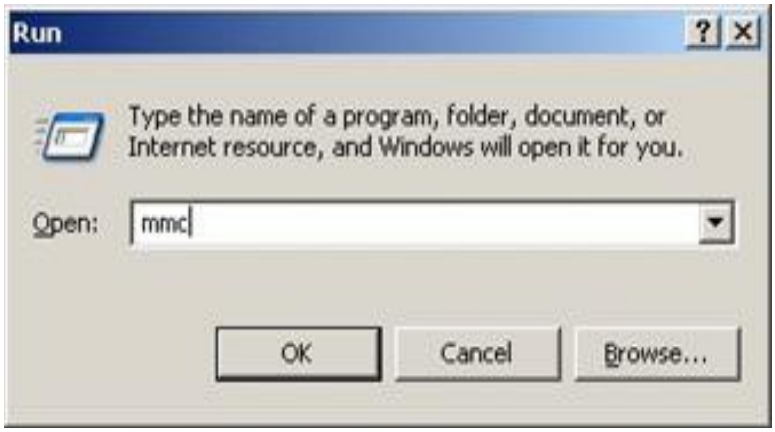


Bây giờ máy **ISA** xác lập **EAP**

Ta chọn **Virtual Private Network (VPN)** rồi ta chọn **Select Access Network**

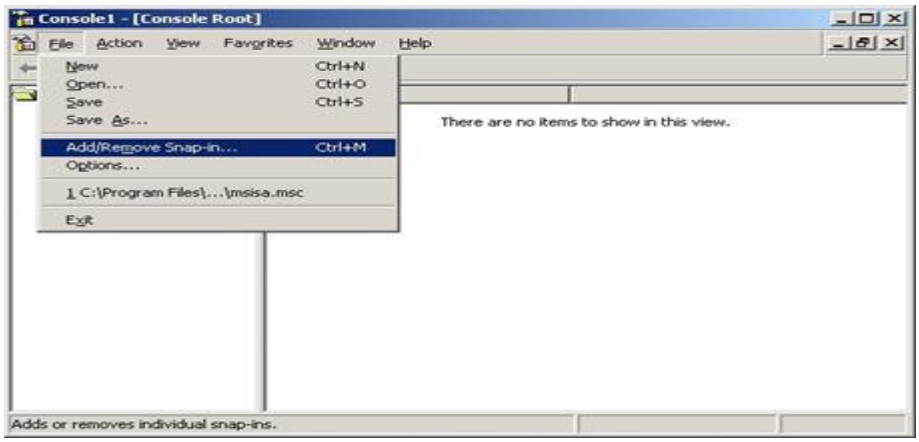
Màn hình **Virtual Private Networks (VPN) Properties** xuất hiện

Ta chọn **Tab Authentication:** Ta đánh dấuvào Extensible **authentication protocol (EAP) with smart card or other certificate** rồi OK sau đó **Apply**

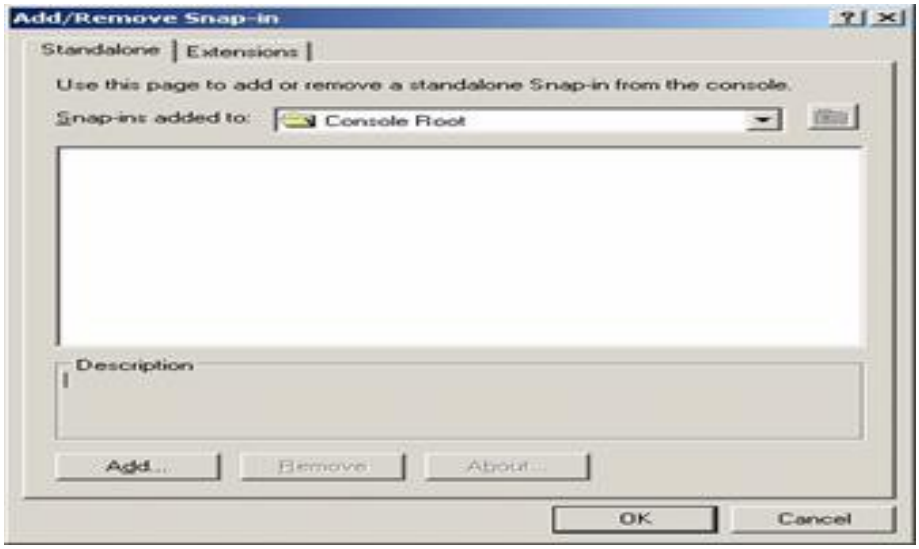


Ta chọn **Monitoring** rồi chọn tab **Service**

Rồi chọn **Remove Access Service** nhắp chuột phải và chọn **Stop**

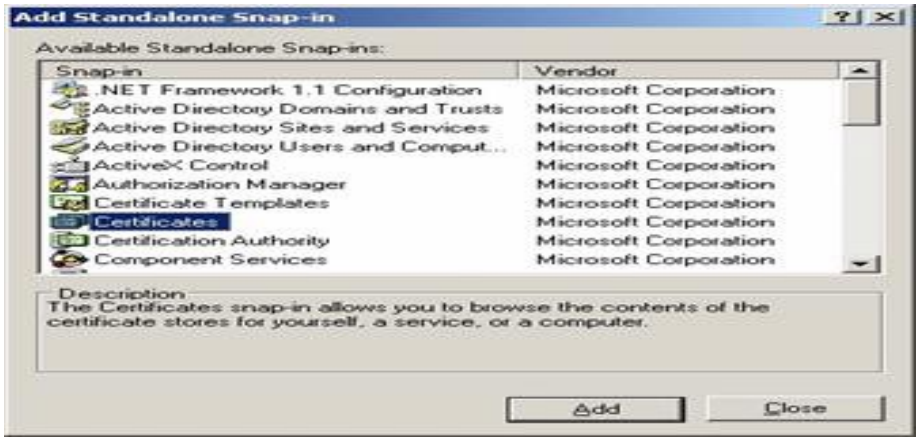


Rồi chọn lại **Remove Access Service** nhấp chuột phải chọn **Start** lại

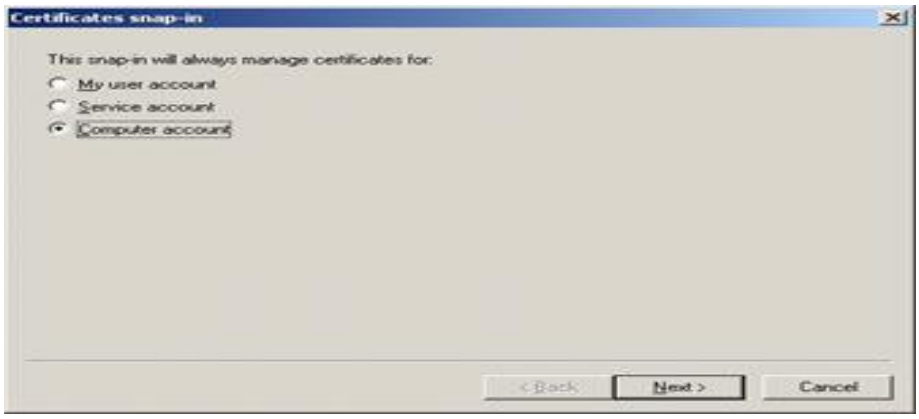


Bây giờ ta tạo kết nối **VPN** bằng **L2TP/ IP Sec**

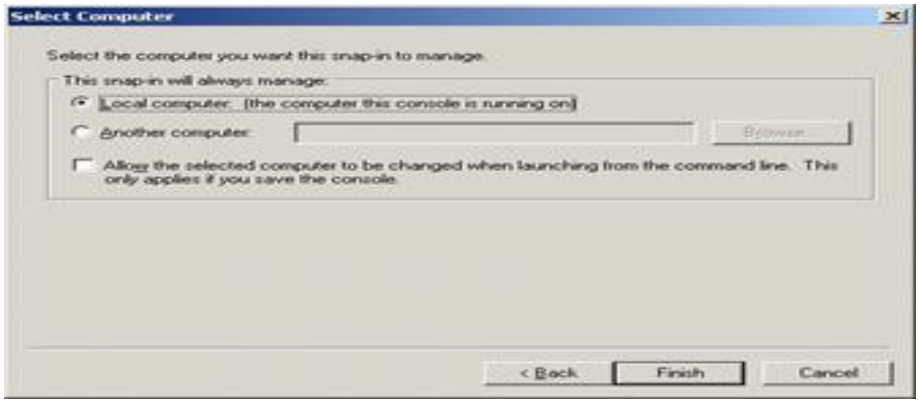
Trên "máy tính ngoài mạng", nhấp chuột phải vào **Icon My Network Places** rồi chọn **Properties**



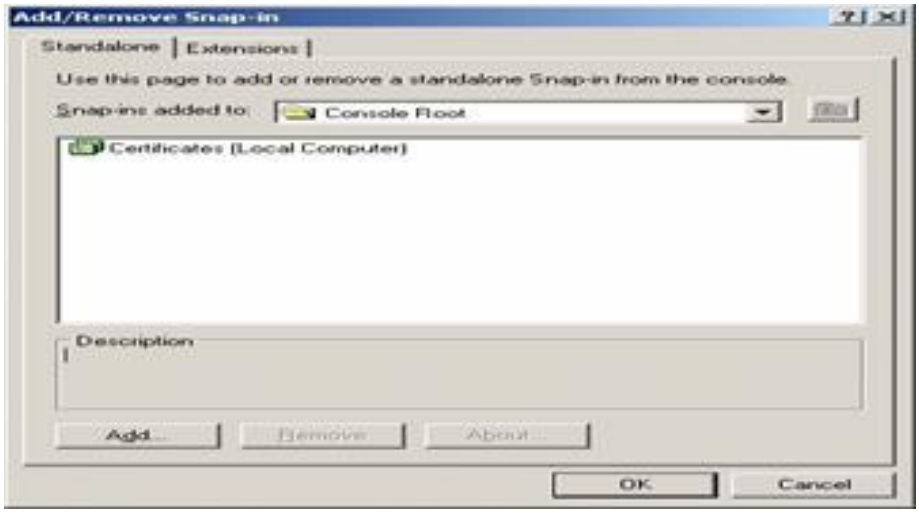
Rồi ta nhấp đúp chuột vào **New Connection Wizard**



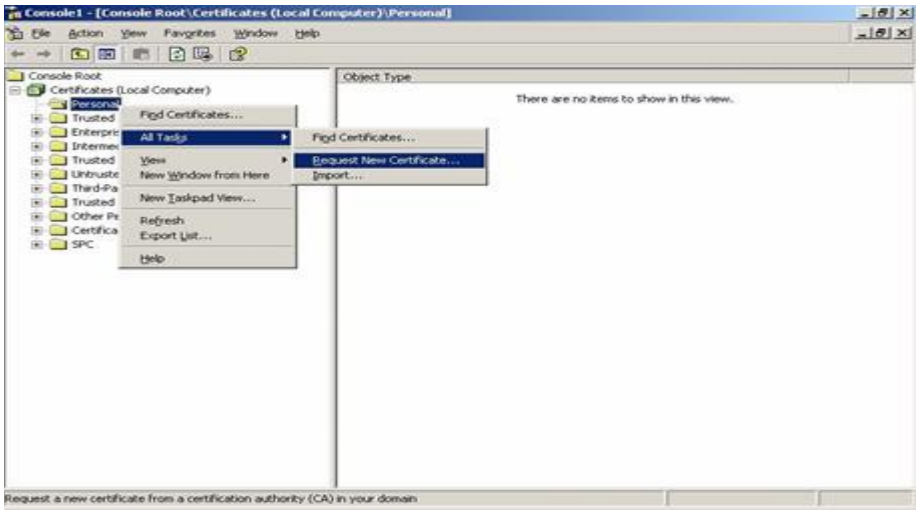
Màn hình **Welcome to the New Connection Wizard** xuất hiện ta bấm **Next**



Màn hình **Network Connection Type** xuất hiện: Ta chọn **Connect to the network at my workplace** rồi chọn **Next**



Màn hình **Network Connection** xuất hiện: Ta chọn **Virtual Private Network connection** rồi bấm **Next**

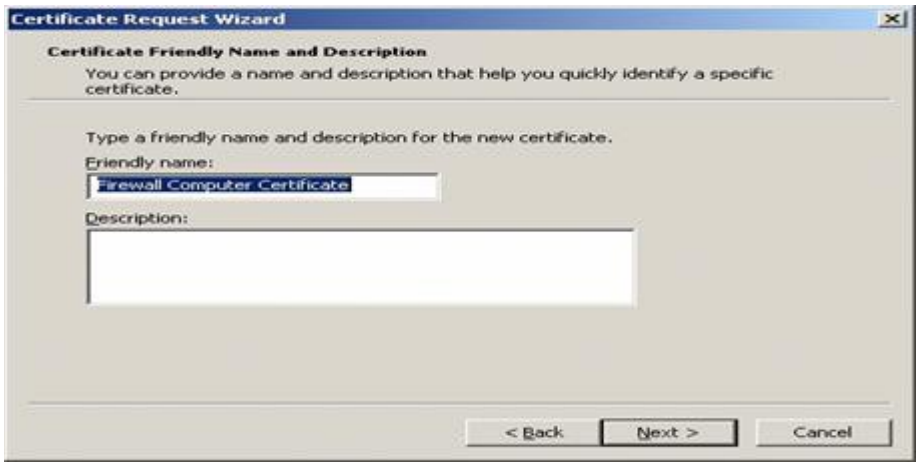


Màn hình **Connection Name** xuất hiện

Compary Name: Ta điền **L2TP** rồi bấm **Next**

Màn hình **Public Network:** Ta chọn **Do not dial the intial connection**

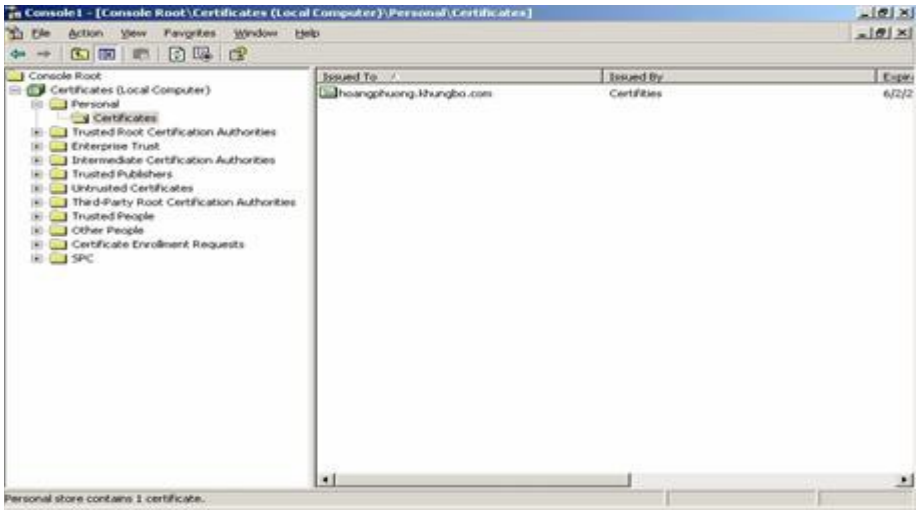
Màn hình **VPN Server Selection:** Ta điền 192.168.1.100



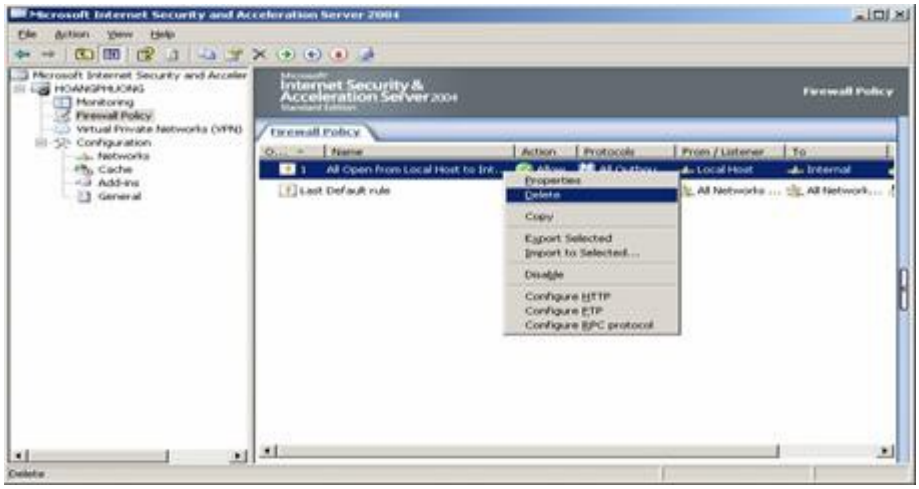
Màn hình **Connection Availabilily** xuất hiện: Ta chọn **My use only** rồi **Next**

Màn hình **Completing the New Connection Wizarrd** xuất hiện: Ta đánh dấu vào **Add shortcut to this connection to my desktop**

Ta ra màn hình **Desktop** sẽ thấy có **L2TP** được tạo ra và ta bấm nhắp đúp vào **L2TP**

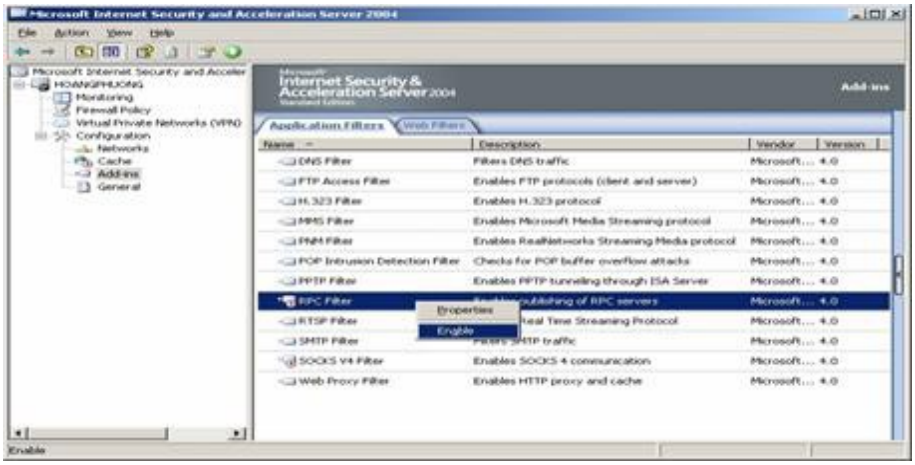


Màn hình **Connect L2TP** xuất hiện ta bấm vào **Propertiess**



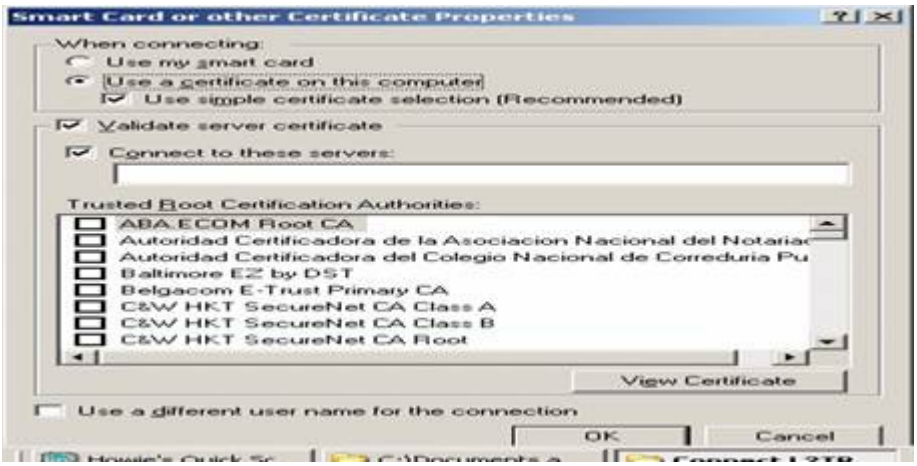
Màn hình **L2TP Properties** xuất hiện Ta chon Tab **Security**

Ta chọn **Advanced (Custom settings)** rồi bấm vào **Settings**



Màn hình **Advanced Security Setting** xuất hiện: Ta đánh dấu vào **Use Extensible Authentication Protocol (EAP)** rồi **Properties**

Màn hình **Smart Card or other Certificate Properties** xuất hiện: Ta đánh dấu vào **Use a certificate on this computer** và **Use simple certificate selection** rồi **OK**



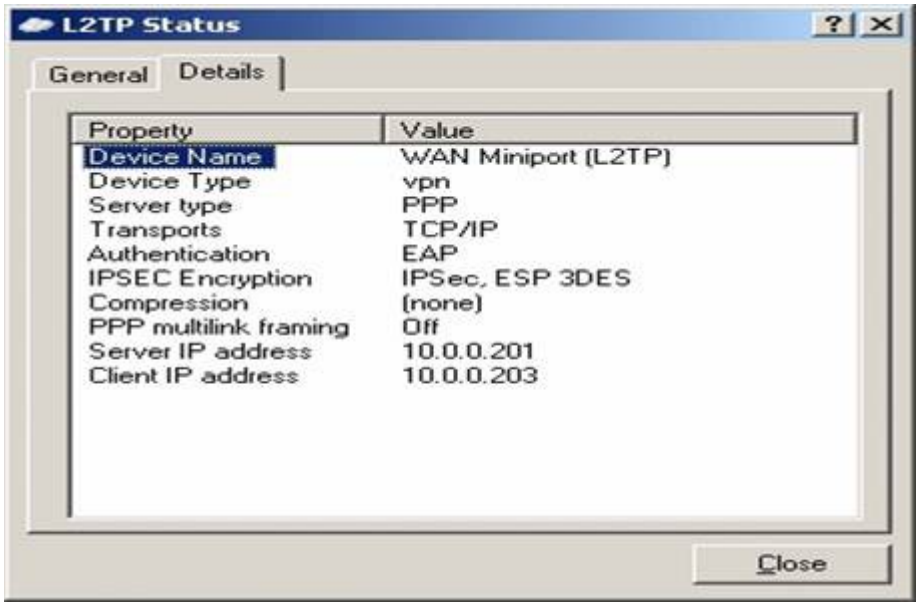
Màn hình **L2TP** xuất hiện: Rồi ta chọn **Tab Networking**

Type of VPN: Ta chọn **L2TP IP Sec VPN** rồi **OK**

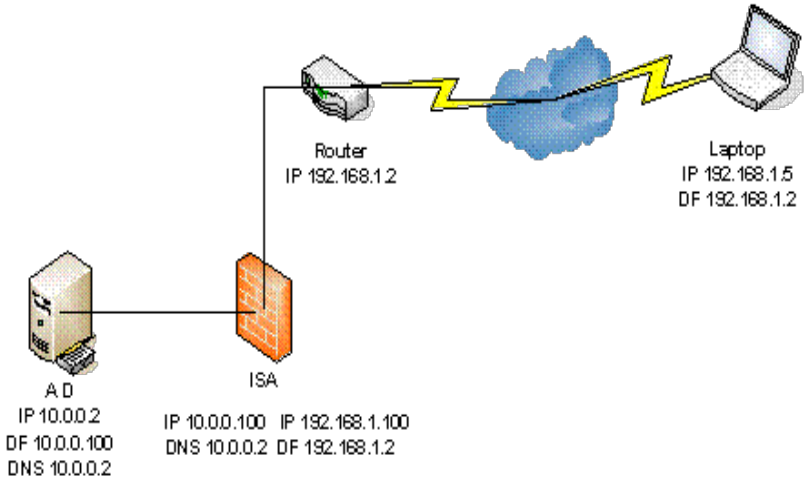
Màn hình **Connect L2TP** xuất hiện và ta bấm vào nút **Connect**

Và nó sẽ đi kiểm tra quyền chứng thực và ta bấm **OK**

Vậy là ta đã **Connect** thành công **VPN** dùng bằng **L2TP/IP Sec** dùng bằng phương thức bảo mật **EAP** thành công



4. Mô hình VPN Client to Site sử dụng chương trình No-IP



No-IP là giải pháp cho những **IP** động mà vẫn sài được những gì về tĩnh

Khi ta kết nối được **Internet** rồi mặc định **Router ADSL** sẽ có 2 IP

IP lan là của **Router 192.168.1.2** và **IP Wan** là **IP** của **Internet** khi kết nối **Internet** thành công sẽ có **IP** lúc này là **201.134.24.157**

Khi 1 người ở HàNội có nhu cầu đứng từ **Internet** có địa chỉ **IP** là **158.38.197.79** muốn **ping** vào máy **192.168.1.100** được

Thì trước tiên ta phải **NAT** trên **Router IP 201.134.24.157** về máy **192.168.1.100**

Thì 1 người ở HaNội **Ping** vào **IP 201.134.24.157** là đang **ping** vào máy **192.168.1.100**

NAT là cơ chế dẫn ta đi điểm này qua điểm kia nghĩa là ta **ping 201.134.24.157** thực chất là ta đang **ping 192.168.1.100**

Nếu **Router** bị mất điện đột ngột thì lúc này **IP** không còn là **201.134.24.157** nữa mà là **1 IP** khác **205.189.79.79**

Lúc đó 1 người ở Hà Nội ta **Ping 201.134.24.157** sẽ không được nữa Vì **Router** lúc này đã thay đổi **IP**

Muốn **Ping** được **192.168.1.100** Ta phải biết địa chỉ **IP** của **Router** lúc này là số mấy khi biết được **IP** đã đổi là **205.189.79.79** ta tiến hành **ping 205.189.79.79** là **ping** về máy **192.168.1.100**

Kết luận: Như vậy mỗi lần địa chỉ **IP** của **Router** bị đổi ta phải biết là địa chỉ lúc đó là **IP** gì thì mới **ping** được về máy **192.168.1.100**

Bây giờ tại máy có **IP 192.168.1.100** ta sử dụng chương trình có tên là **No-IP** nó cho phép tạo ra 1 tên máy ví dụ tên là **kiemthan.no-ip.info** rồi cho 1 phần mềm và ta chạy phần mềm này trên máy có **IP 192.168.1.100** thì nó sẽ tìm cách cập nhật **IP** hiện tại mà **Router** có với tên miền mà mình đã đăng kí

Như vậy ở ngoài HN thay vì mỗi lần **ping 192.168.1.100** ta phải biết **Router IP** hiện nay là gì thì bây giờ không cần biết hiện giờ **IP Router** là **IP** gì mà ta chỉ cần ping **kiemthan.no-ip.info** là đang ping vô **192.168.1.100**

Như vậy ta đã có giải pháp ta đang sử dụng **IP** động nhưng ta lại làm việc như là tĩnh, nghĩa là thay vì ta làm việc trên IP thì ta làm việc trên tên máy.

Ta sẽ cấu hình dùng **VPN** trên **ISA** thông qua **No-IP** để 1 ai khi đi công tác muốn sử dụng **VPN** mà không cần bận tâm **IP** lúc này là **IP** gì mà cần biết tên đăng kí trên **No-IP** lúc này là gì

Máy **ISA** ta cấu hình **VPN** dùng giao thức **PPTP** như bình thường (xem lại mô hình Client to Site dùng giao thức PPTP)

Sau khi cấu hình **VPN** sử dụng giao thức **PPTP** xong

Ta tiến hành đăng kí dịch vụ **No-ip**

Ta vào trang web http:// www.no-ip.com Ta bấm vào **Sign up Now** để đăng kí **No-** ip

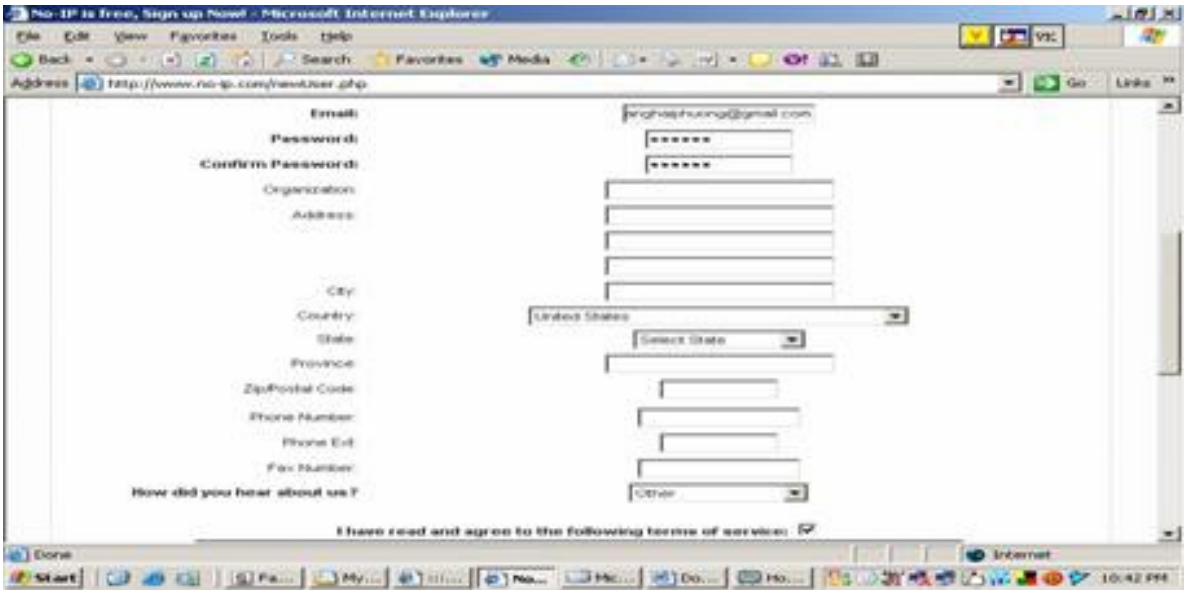
Ta bắt đầu điền các thông tin để đăng kí

First Name và **Last Name:** Ta điền phuong (ta điền gì cũng được)

Email: Ta điền hộp mail của mình hoanghaiphuong@gmail.com

Password và **Confirm Password** Ta điền pass gì cũng được ta điền123456

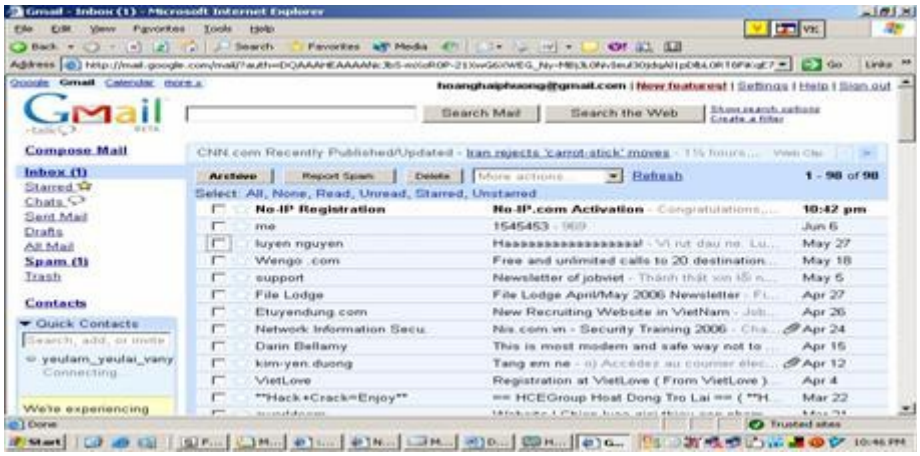
How did you hear about us: Ta chọn Other và ta đánh dấu vào **I have read and agree to the following terms of service** rồi ta bấm **SIGN UP NOW**



Khi đăng kí **No-ip** xong. **No-ip** bắt ta phải **active** thì mới cho **login** vô được giao diện của **No-ip**. Ta phải mở mail mà ta đăng kí hồi nãy cho **No-ip** ra để **active**

Ta mở mail hoanghaiphuong@gmail.com ra thì thấy **No-ip** gửi cho ta 1 lá thư để **active**

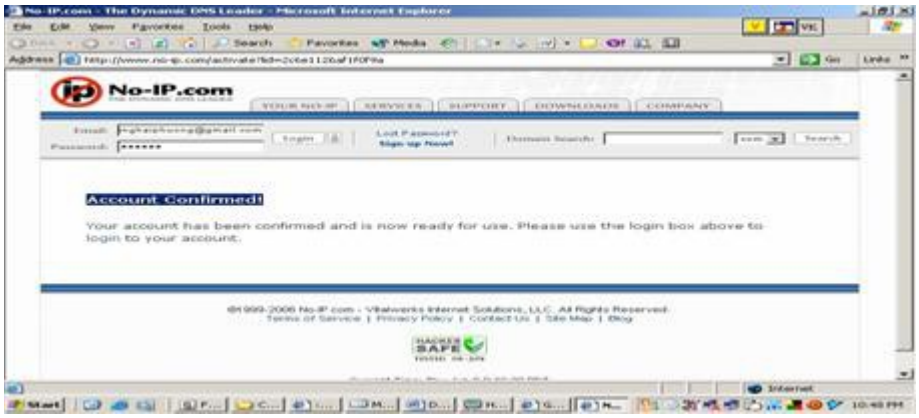
ta bấm vào lá thư **No-IP** đó



Mở lá mail của **No-IP** gửi đến, nhắp vào link để active

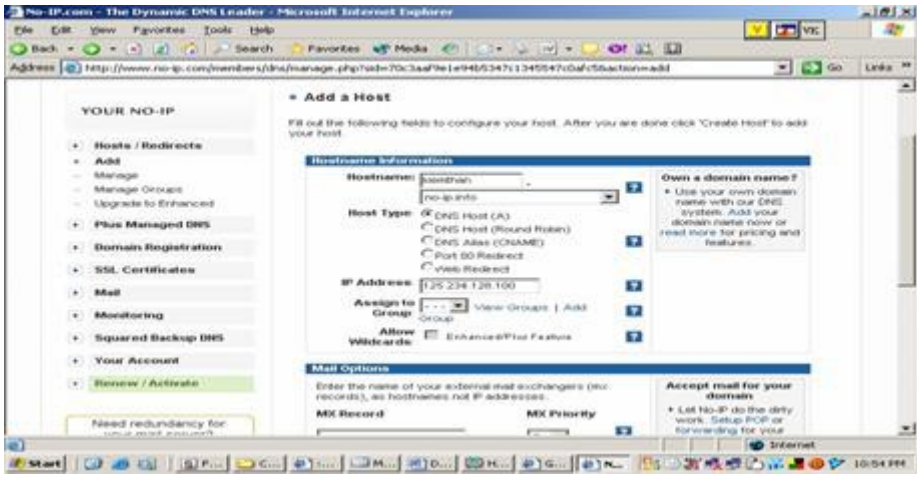
Email Ta điền địa chỉ ta đăng kí là **hoanghaiphuong@gmail**

Password Ta điền pass mà ta đã đăng kí 123456 rồi **Login**



Khi **Login** thành công ta vào được web **No-IP** Ta bấm vào **Add**

Hostname ta điền **kiemthan** rồi chọn là **No-ip. Info** rồi chọn **Create Host**

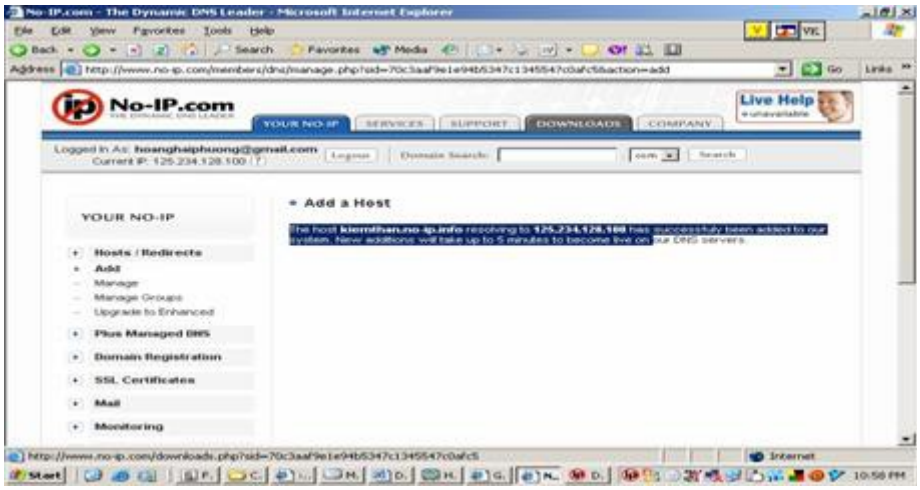


Thì màn hình báo ta đăng kí thành công **kiemthan.no-ip. Info**

The host kiemthan.no-ip. info resctving to 125.234.128.100 has successfully been addred to our systems. New addtion will take up to 5 minute to become live on our DNS servers

Khi đăng kí thành công **No-ip** rồi ta tiến hành **download** chương trình **No-ip** về máy

Ta bấm vào **Download**

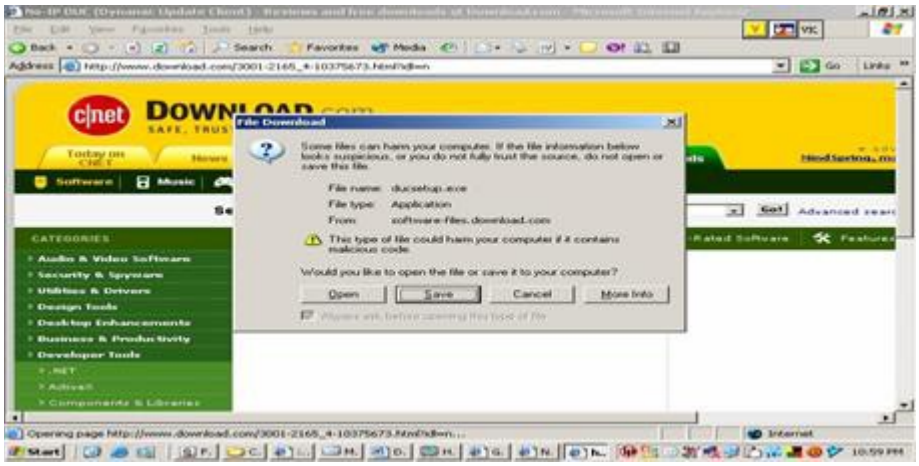


Khi được hỏi ta muốn **download No-ip** dùng cho máy nào Ta bấm vào **Windows**

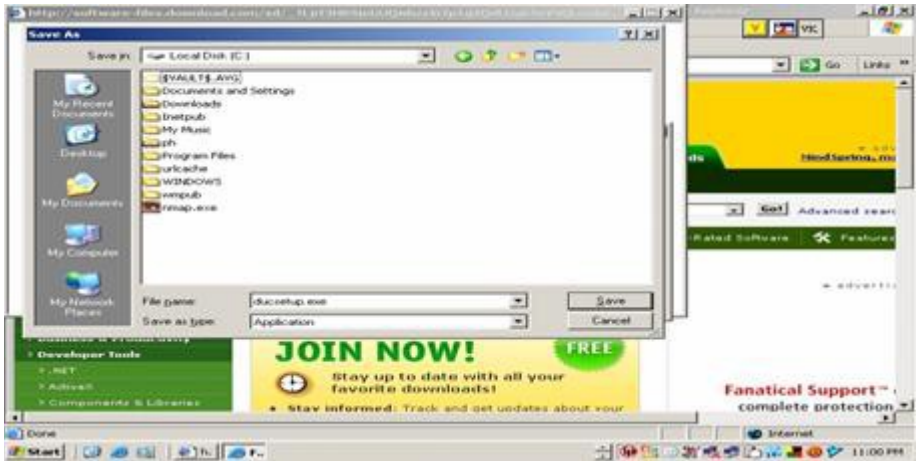
Ta tiếp tục bấm vào **Download 2.2.1**

Ta tiếp tục bấm vào **Download Now**

Nó hiện lên cái bảng cho ta **download** chương trình **No-IP** về Ta bấm vào **Save**

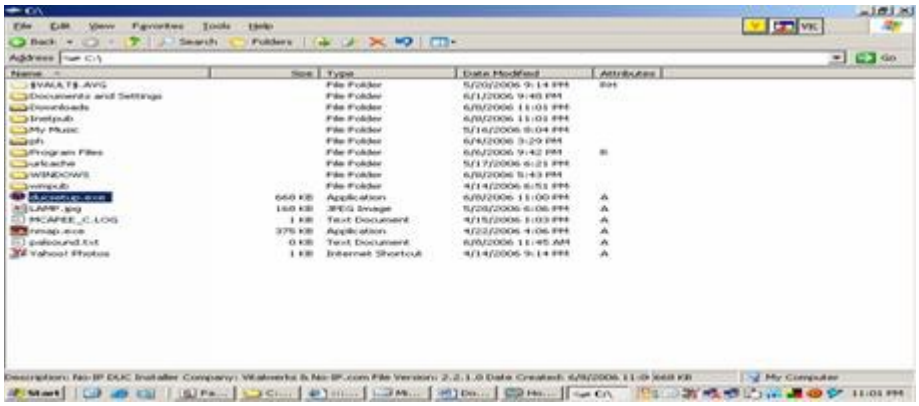


Ta lựa ổ đĩa C để lưu lại rồi bấm **save** tiếp và sẽ tự động **down** về



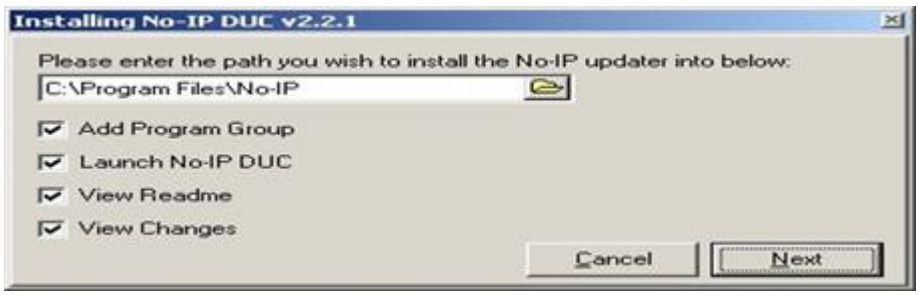
Khi **download** xong ta vào ổ đĩa C thì thấy rằng có chương trình **No-IP**

Ta bấm vào chương trình **ducsetup. Exe** để cài đặt **No-ip**



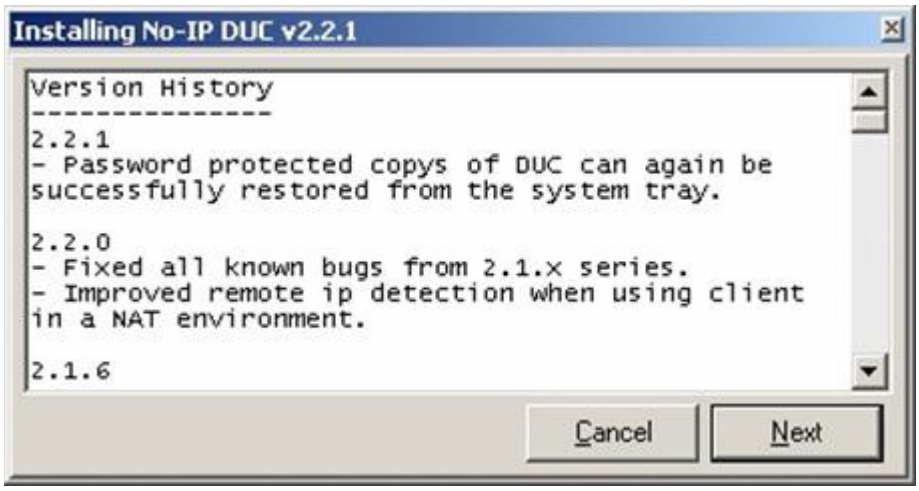
Màn hình **Installing No-IP DUC v2.2.1** xuất hiện Ta bấm **Next**

Ta tiếp tục bấm **Next**

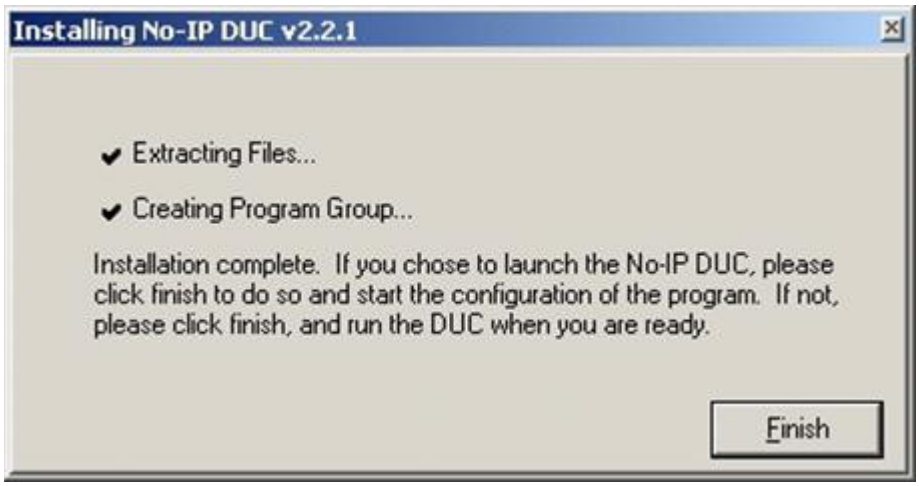


Ta bấm vào **Yes**

Ta bấm **Next** tiếp



Ta bấm vào **Finish**



Vậy là ta đã cài xong chương trình **No-ip**.

Ta mở chương trình **No-ip** lên Ta vào **Start** rồi **Programs** rồi **No-IP** rồi **No-IP DUC**

Màn hình **No-IP DUC** xuất hiện

E-MAIL Address ta điền **hoanghaiphuong@gmail**

Password 123456 rồi OK

Màn hình **No-IP DUC v2.2.1** xuất hiện Ta đánh dấu vào **kiemthan.no-ip. Info** rồi bấm vào dấu **X** để tắt chương trình đi

Ta sẽ thấy ngoài màn hình **Desktop** trên thanh **Tarbar** có mục **IP**

Cấu hình và cài đặt **No-IP** xong rồi ta tiến hành cấu hình **Router ADSL**

Ta mở **IE** lên đánh **IP** địa chỉ của **Router ADSL** để vào cấu hình

Ở đây ta cấu hình trên **Router PLANET**

Khi vào được **Router** của **PLANET** rồi ta tìm mục **Virtual Server**

Public Port Start Ta điền **3389** (**3389** là port **VPN**)

Public Port End ta điền **3389**

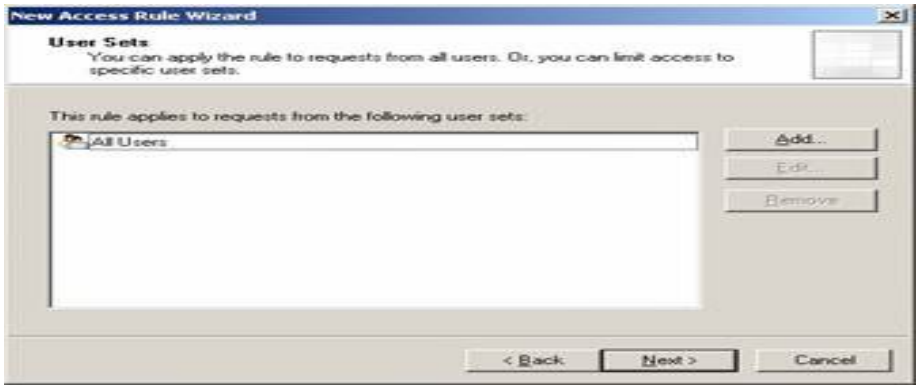
Private port ta điền **3389**

Ta chọn **TCP** với **IP** là **192.168.1.100** rồi Add

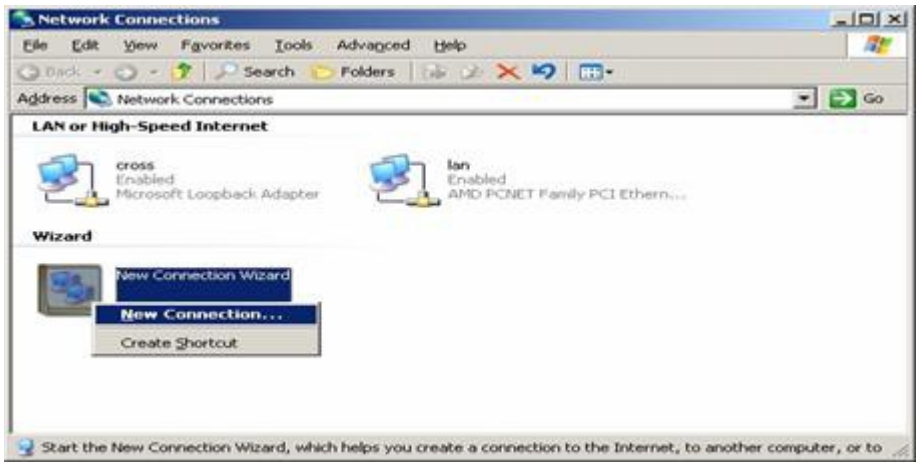
Sau khi **Add port 3389** xong rồi ta sẽ thấy xuất hiện **port 3389** rồi ta **Save setings/Restart**

Trên "máy tính ngoài mạng", ta sẽ cấu hình để sử dụng **VPN**

Ta bấm vào **My Network Places** rồi nhắp chuột phải chọn **Properties**

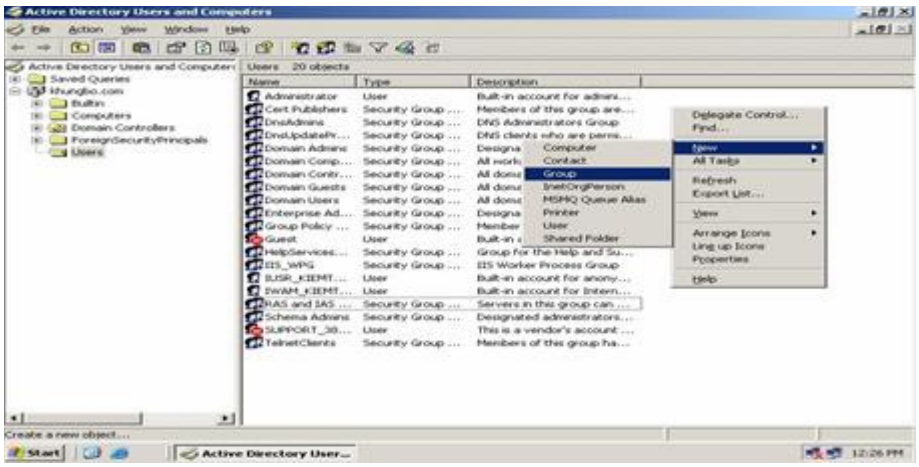


Rồi chọn **New Connection Wizrad** bấm chuột phải chọn **New Connection**.

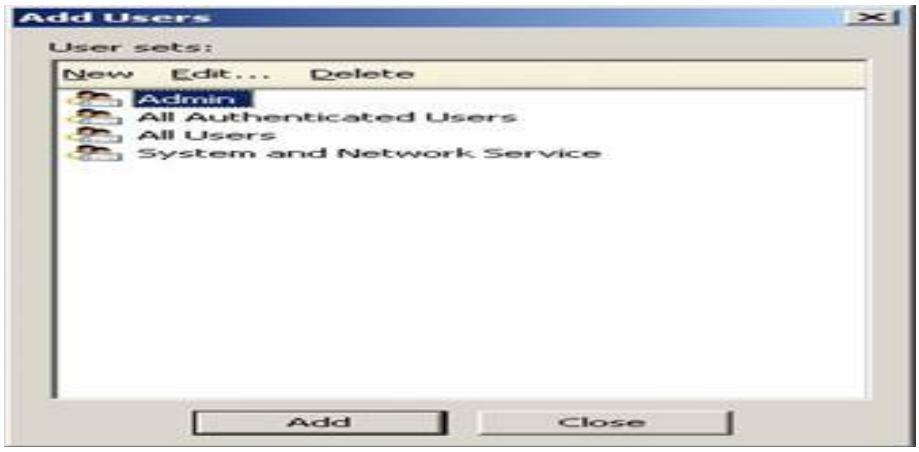


Màn hình **Wellcome to the New Connection Wizard** rồi bấm **Next**

Màn hình **Network Connection Type:** ta chọn **Connect to the network at my workplace** rồi **Next**

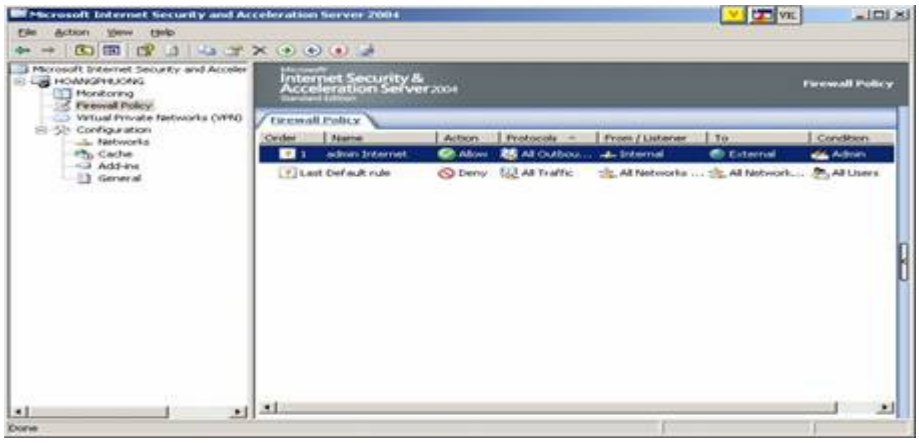


Network Connection: Ta chọn **Virtual Private Network connection** rồi **Next**



Màn hình **Connection Name:** xuất hiện

Compary Name: Ta điền **PPTP** rồi bấm **Next**



Màn hình **VPN Server Selection** xuất hiện

Host name or IP address (for example microft com or 157.54.0.1): Ta điền **kiemthan.no-ip. Info** rồi **Next**

Connection Availability: Ta chọn **My use only** rồi **Next**

Màn hình **Completing the New Connection** xuất hiện Ta đánh dấu vào mục **Add a shortcut to this connection to my desktop**

Thì lúc này ta sẽ thấy **PPTP** xuất hiện ở **Desktop**

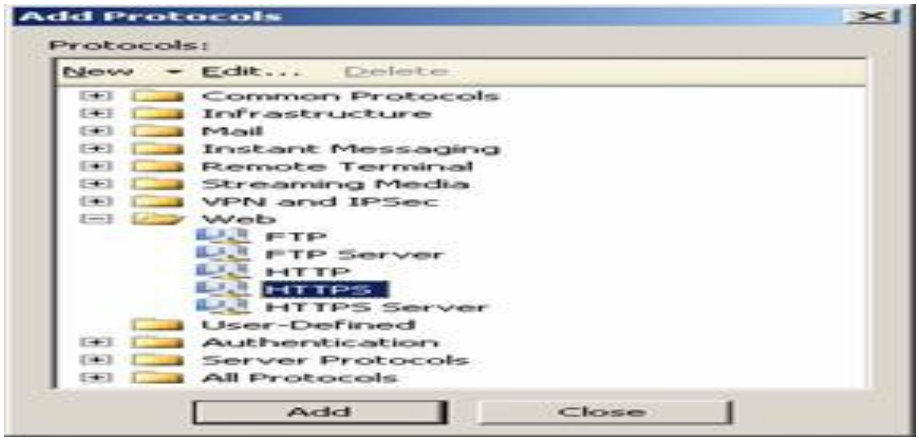
Ta nhắp đúp chuột vào **PPTP**

Thì lúc này Màn hình **Connect PPTP** xuất hiện

User name: ta điền administrator

Password: 123456 rồi bấm **Connect**

Thì ta thấy sẽ **Connect** thành công **VPN** bằng giao thức **PPTP**



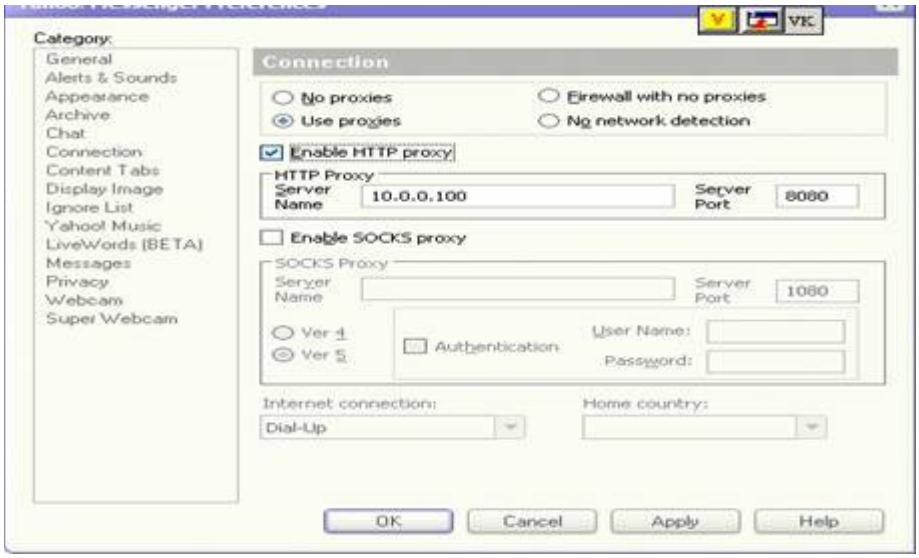
Sau đó ta bấm **Start** rồi **Run** bấm **CMD** thì ta sẽ ra được màn hình **Dos**

Khi ra được màn hình **Dos** ta bấm lệnh **ipconfig /all** ta sẽ thấy xuất hiện thêm 1 địa chỉ **IP** do ta kt nối **VPN** tời mạng cục bộ và được **ISA** cung cấp do ta cấu hình

IP được cung cấp ở đây là 10.0.0.203

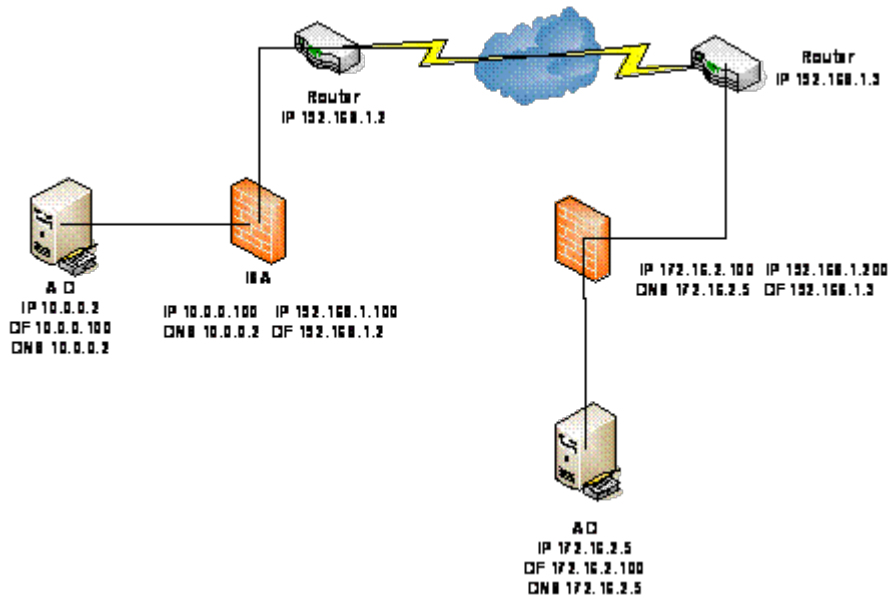
Ta tiến hành **Ping** đến mạng cục bộ thử là 10.0.0.2 thì thấy nó trả lời lại tin hiệu 127

Và kể từ lúc này ta có thể truy xuất được dữ liệu trong mạng cục bộ



5. Mô hình VPN Site to Site

Mục tiêu: Trình bày cách cấu hình và cài đặt No-IP, cấu hình Router ADSL với mô hình site to site



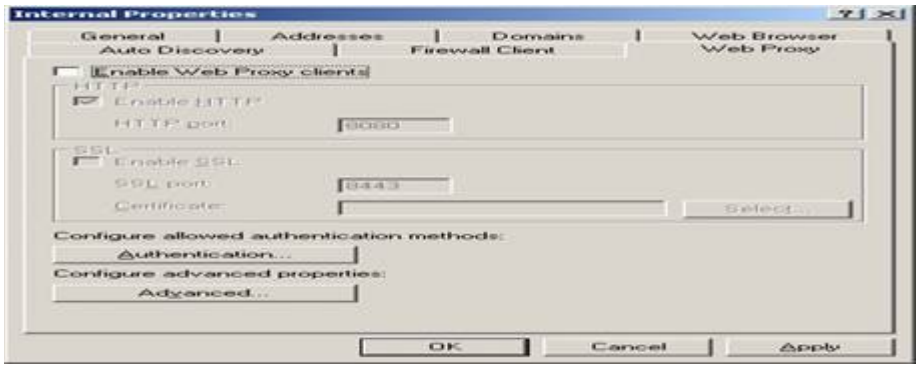
Ta sẽ làm mô hình theo site saigon và site hanoi cho dễ hiểu

Site saigon có **IP** là 192.168.1.100 và ta tạo **user** là kiem **pass** 123 và bật **Allow Access**

Site hanoi có **IP** là 192.168.1.200 và ta tạo **user** là dao **pass** 123 và bật **Allow Access**

Ta sẽ cấu hình **Site Saigon** trước

Ta bấm vào **Virtual Private Network (VPN)** rồi bấm vào **Enanle VPN Client Access** và **Apply** thì lúc này ta sẽ thấy lại là **Disable VPN Client Access**

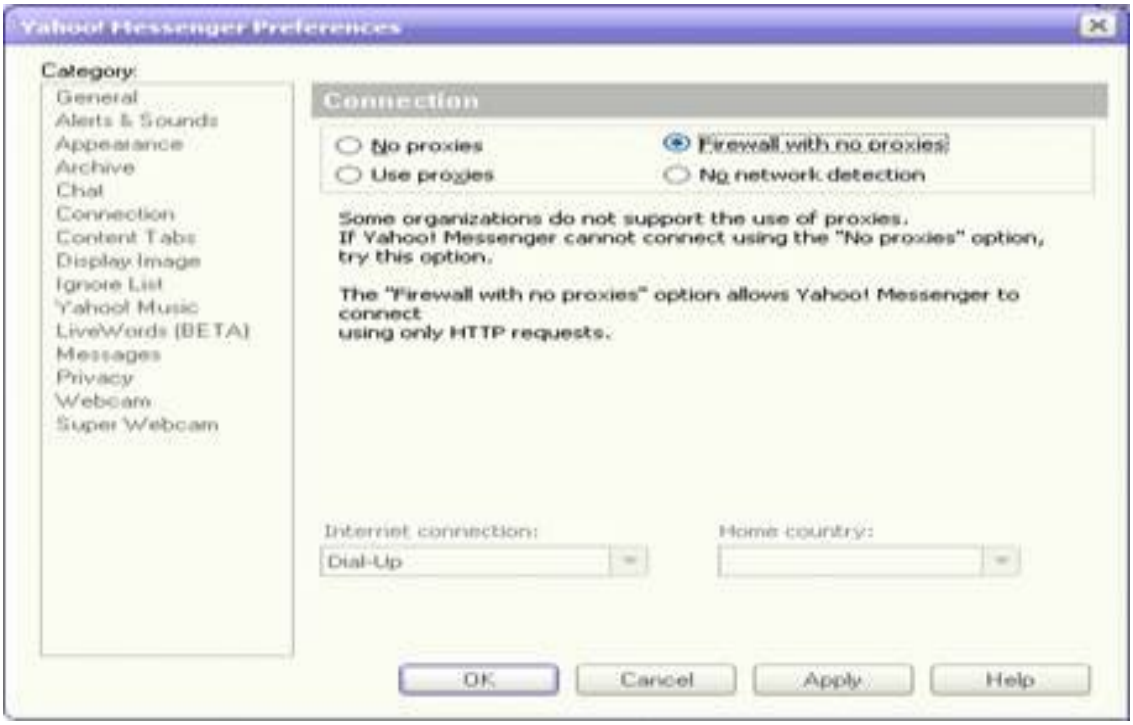


Rồi ta chọn **Configure VPN Client Access**

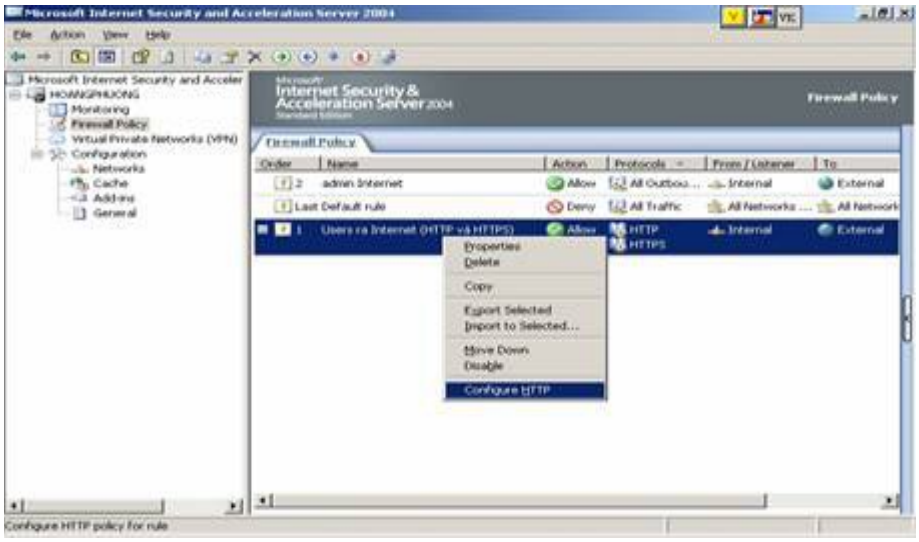
Màn hình **VPN Client Properties** xuất hiện

Ta đánh dấu vào **Enable VPN client access**

Maximu number of VPN client allowe: ta sửa lại là 10 và **OK** và **Apply**

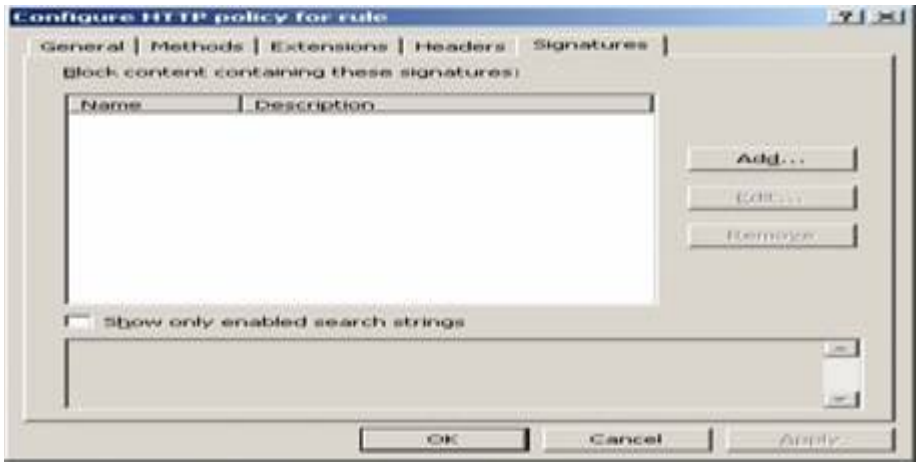


Rồi ta chọn **Tab Remote Sites:** rồi bấm vào **Add Remote Site Network**



Màn hình **Welcome to the New Network Wizard** xuất hiện

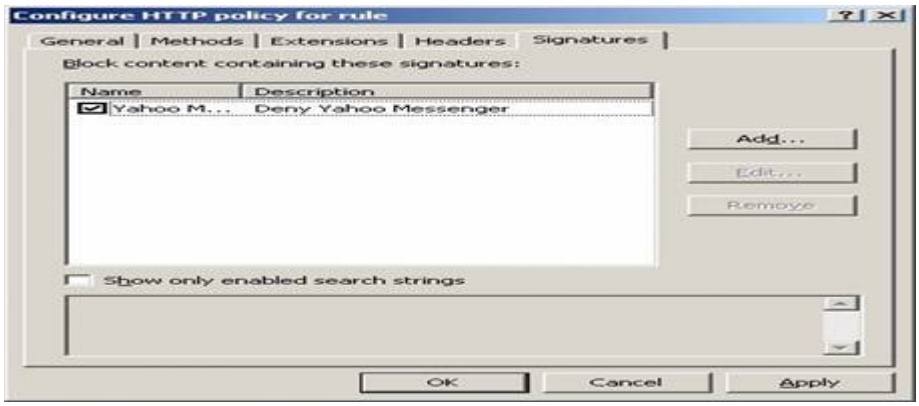
Network name: ta điền hanoi rồi **Next**



VPN Protocol: ta chọn **Point to Point Tunneling Protocol (PPTP)** rồi **Next**

Màn hình **Remote Site Gateway** xuất hiện

Remote VPN Server name or IP address: Ta điền **IP** ra net của **site hanoi** là 192.168.1.200



Màn hình **Remote Authentication** xuất hiện

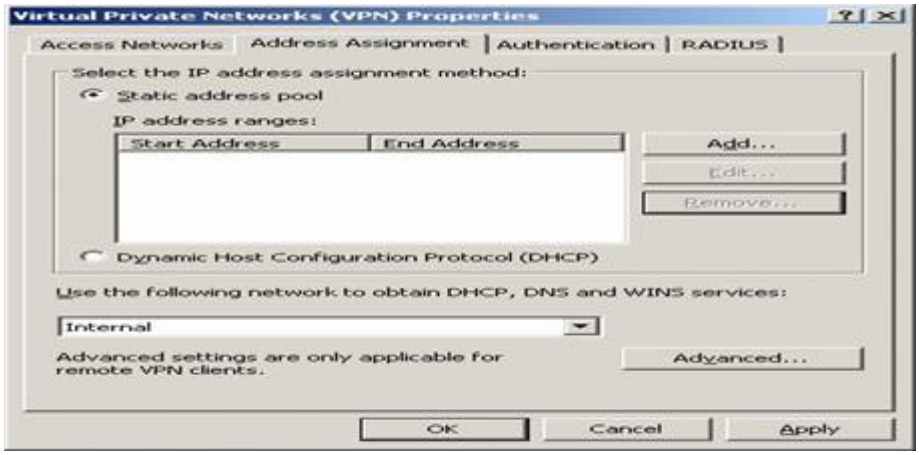
Ta đánh dấu vào **Local site can initiable connection to remote site using these credentials**

User name: ta điền user **site hanoi** là dao

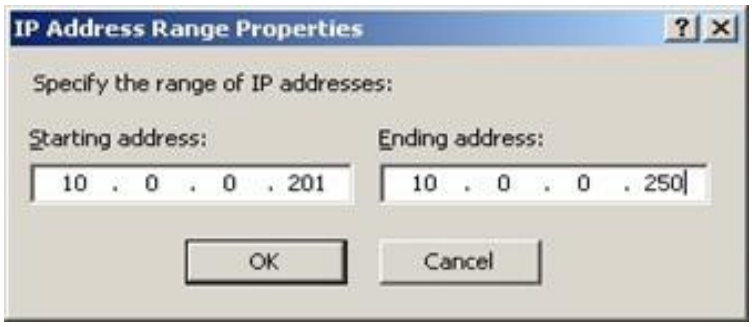
Password: 123

Confirm password: 123 rồi **Next**

Màn hình **Local Authentication** xuất hiện ta bấm **Next**

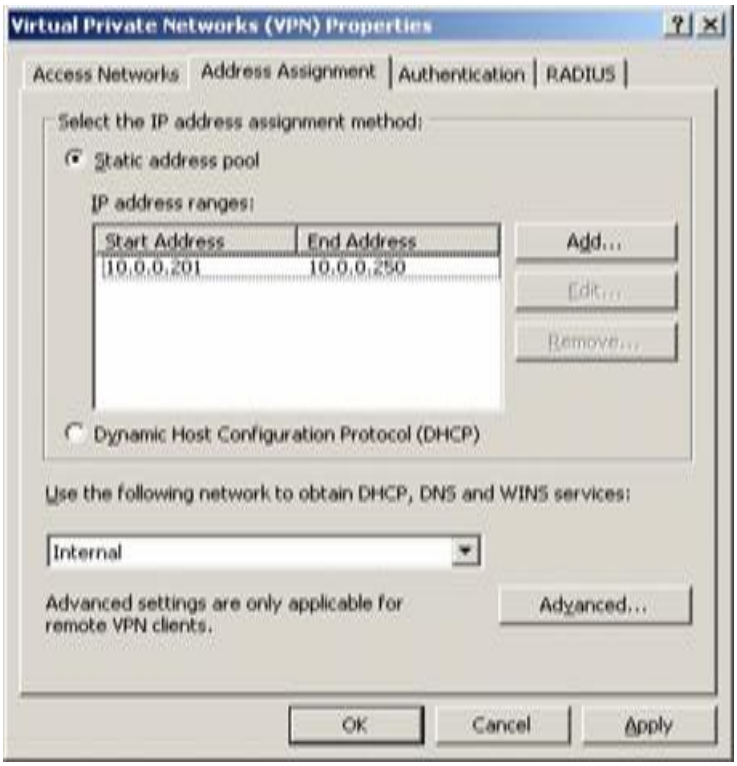


Màn hình **Network Addresses** xuất hiện Ta bấm **Add**

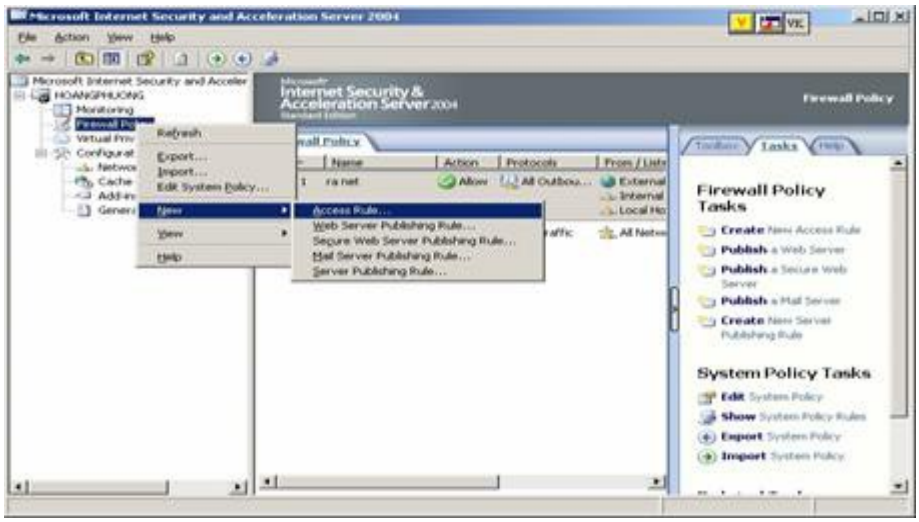


Lúc này ta sẽ nhập **IP Internal** của **ISA site hanoi** là

172.16.2.5 đến 172.16.2.100 rồi **OK**

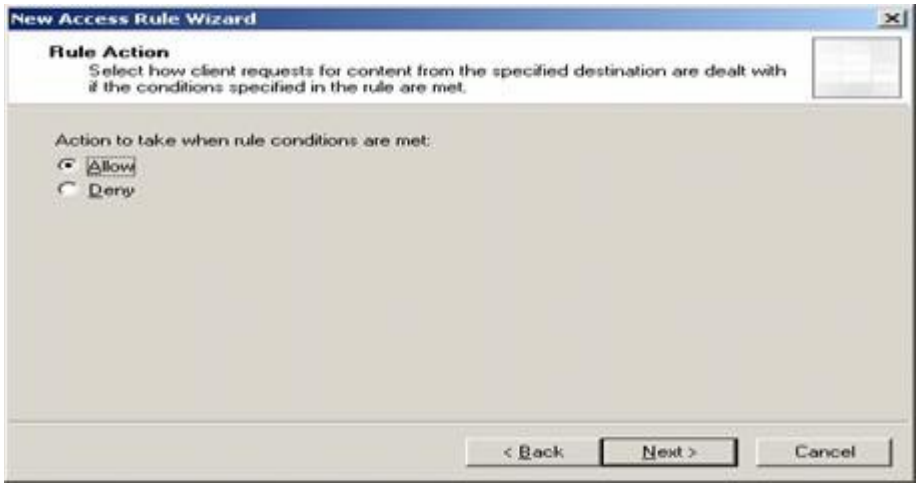


Lúc này ta sẽ thấy **Address ranges** sẽ xuất hiện **IP** rồi bấm **Next**



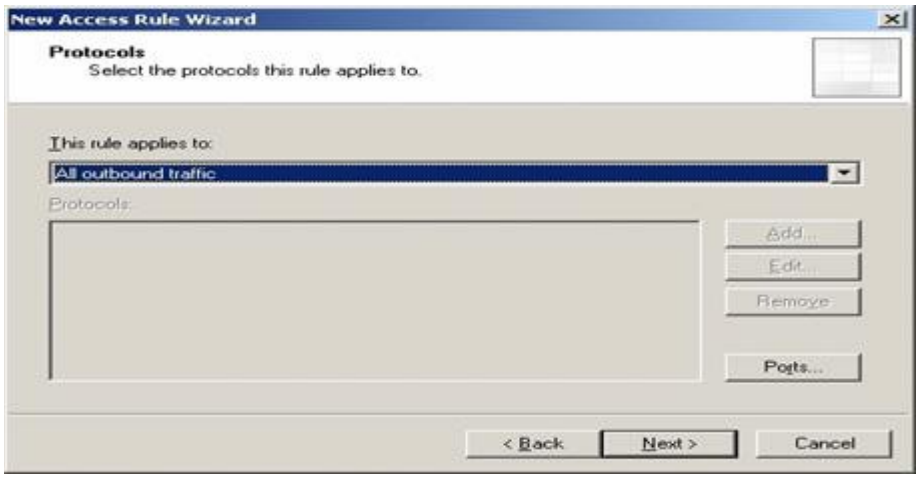
Màn hình **Completing the New Network Wizard** xuất hiện ta bấm **Finish** rồi **Apply**

Ta chọn **Vitual Pritave Network (VPN)** bấm chuột phải chọn **Properties**



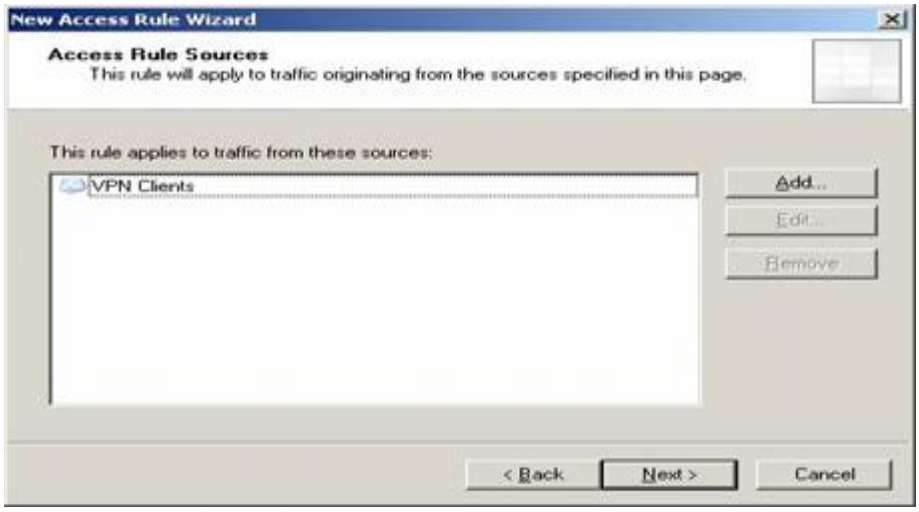
Màn hình **Virtual Private Network (VPN) Properties** xuất hiện

Ta chọn tab **Access Networks** và đánh dấu vào **External** và **hanoi**



Rồi ta chọn tab **address Assignment**

Ta đánh dấu vào **Static address pool** rồi bấm **Add**

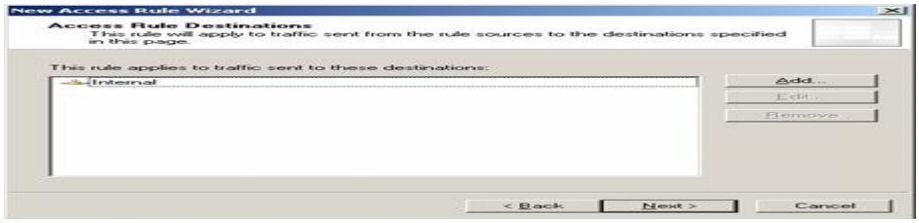


Ta cấp phát **IP** cho **site hanoi**

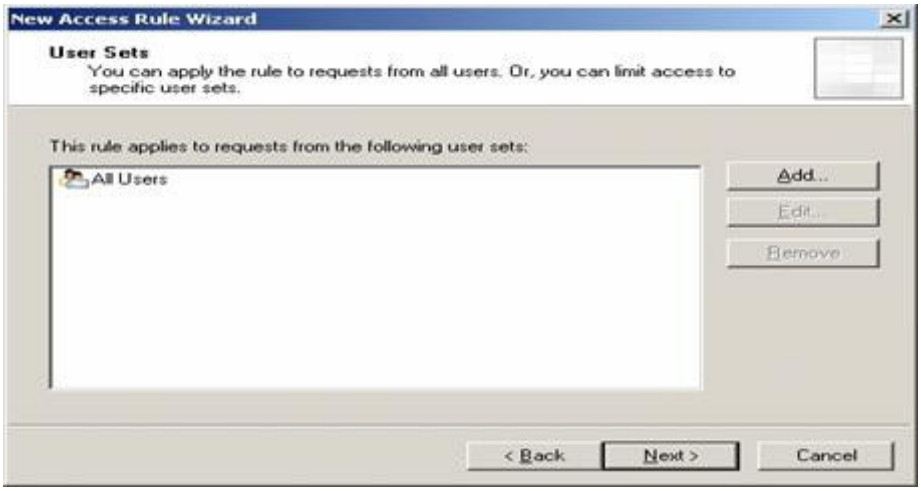
Lưu ý địa chỉ cấp phát hông được trung với **Internal** nội bộ

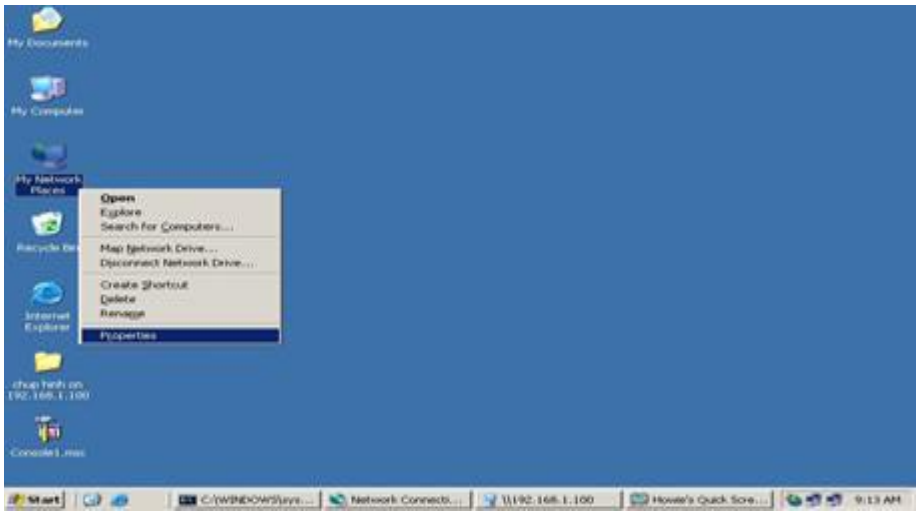
Internal của **site saigon** là 10.0.0.2 đến 10.0.0.200

nên bây giờ ta cấp 10.0.0.201 10.0.0.250 rồi **OK**



Thì lúc này IP address ranges có IP rồi ta bấm OK sau đó ta apply





Ta chọn tiếp **Configuration** rồi chọn **Network** Nhắp chuột phải chọn **New** rồi **Network Rule**

Màn hình **Welcome to the New Network Rule Wizard** xuất hiện

Network rule name: ta điền hanoi to internal rồi **Next**

Màn hình **Network Traffic Sources:** ta bấm **Add** rồi bấm vào **Network** rồi chọn **hanoi** rồi **Close.**

Câu hỏi

1. VPN là gì? Trình bày bản chất hoạt động của VPN.

2. Hãy cho biết các lợi ích của VPN?

Bài tập thực hành

1. Thiết lập VPN client to site dùng giao thức PPTP.

Máy Domain:

- Tạo group admin

- Bật **Allow access** cho Administrator

Máy ISA:

- Kích hoạt **Enable VPN Client Access**

- Thiết lập số kết nối tối đa

- Chỉ định tên miền và nhóm người dùng

- Chọn giao thức kết nối

- Cấp phát dải IP đối với người dùng khi kết nối

- Tạo rule để VPN Client truy xuất dữ liệu được

Máy tính ngoài mạng:

- Tạo kết nối PPTP

- Chỉ định địa chỉ server

- Thực hiện kết nối

2. Thiết lập VPN Client to Site dùng giao thức L2TP/IPSEC

- Cài dịch vụ **IIS** và **Enterprise CA** trên máy **AD**

- Chứng nhận **CA** cho máy **Máy ISA** (Tạo rule, cấu hình giao thức RPC, xóa rule)

- Chứng nhận cho máy **VPN Client**

3. Thiết lập VPN Client to Site sử dụng chương trình No-IP

- Máy **ISA**: cấu hình **VPN** dùng giao thức **PPTP**

- Đăng kí dịch vụ **No-ip** và active

- Khởi động và cấu hình No-IP

- Cấu hình router

- Cấu hình để sử dụng VPN cho "máy tính ngoài mạng"

4. Thiết lập VPN Site to Site

- Cấu hình **Site 1** với **IP** là 192.168.1.100, tạo **user** là user1, **pass** 123, bật **Allow Access**

- Cấu hình **Site 2** với **IP** là 192.168.1.200, tạo **user** là user2 **pass** 123, bật **Allow Access**

BÀI 9: PUBLISHING

Mã bài: MĐ 36-09

Mục tiêu của bài:
- Thiết lập được hệ thống sử dụng mail server;
- Cấu hình lọc được mail trong hệ thống;
- Thiết lập được web và FTP được chứng thực từ xa;
- Thực hiện các thao tác an toàn với máy tính.

1. Cài đặt hệ thống Mail Mdaemon và gửi mail qua lại

Mục tiêu: Trình bày các bước cài đặt hệ thống Mail Mdaemon, tạo mail POP3 cho account kiem và thử gửi mail giữa các Account.

➧ Tại **máy ISA account administrator** ta tiến hành gửi **mail** cho **account kiem**

➧ **Máy AD** cài **Mail Mdaemon**:

- Nhắp đúp chuột vào chương trình để cài đặt. Khi màn hình cài đặt mail **Mdaemon** xuất hiện, chọn nút **I Agree**;

- Màn hình **Select Destination Diretory** xuất hiện, chọn **Next**;

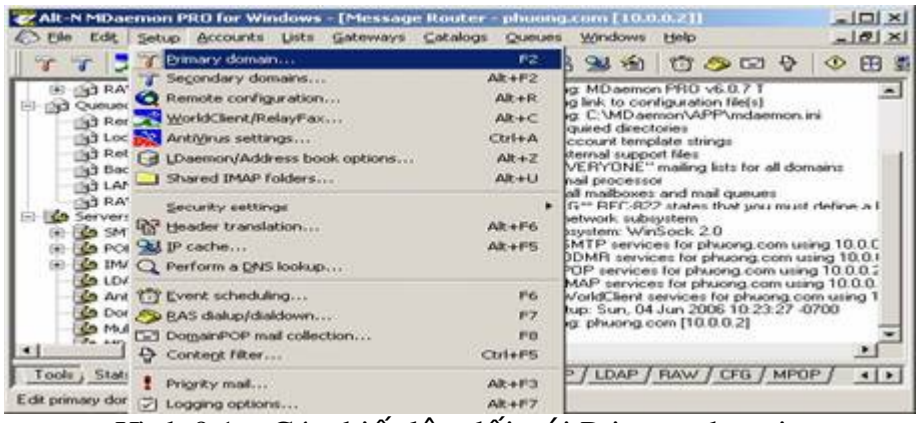
- Màn hình **Registration Infornation** xuất hiện Ta bấm **Next**;

- Trong hộp thoại **Select Components To Install**, chọn **Next**;

- Chọn **Next** trong **Ready to Install**; Lúc này ta thấy chương trình mail **Mdaemon** bắt đầu cài đặt.

Sau khi cài đặt xong, trên thanh Taskbar xuất hiện sẽ thấy hình lá thư, nhắp đúp vào lá thư đó.

Trên cửa sổ **Mail Mdaemon**, chọn tab **Setup /** chọn **Primary domain**…

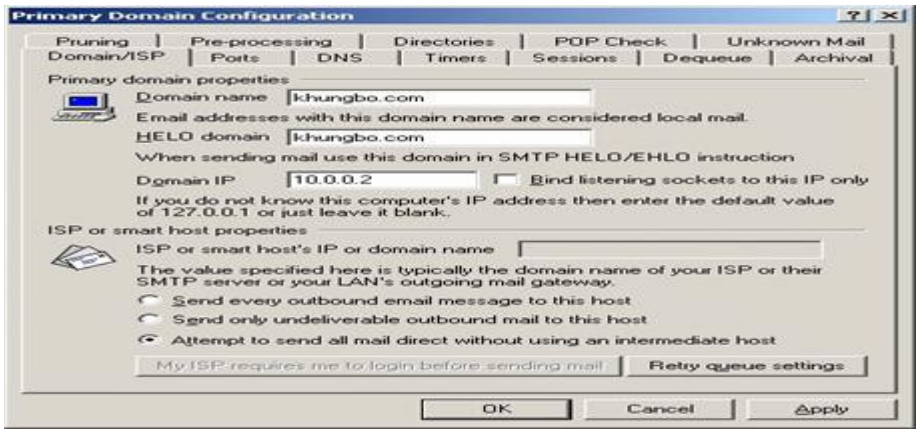


Hình 9.1 – Các thiết lập đối với Primary domain

Màn hình **Primary Domain Configuration** xuất hiện, chọn Tab **Domain/ISP**;

- **Domain name** và **HELO domain**: điền tên Domain

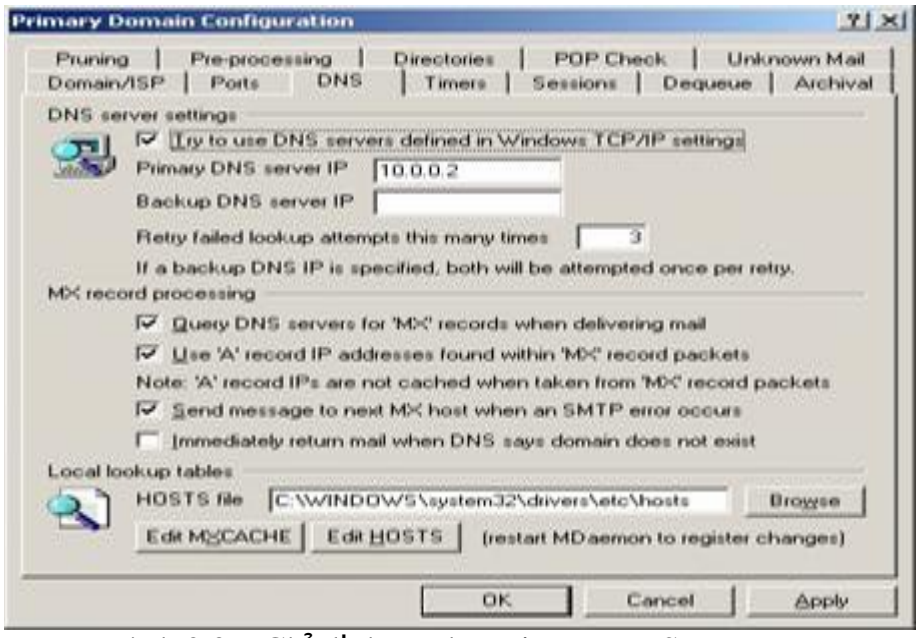
- **Domain IP**: điền **IP** của máy **Domain** là **10.0.0.2**



Hình 9.2 – Thiết lập Primary domain

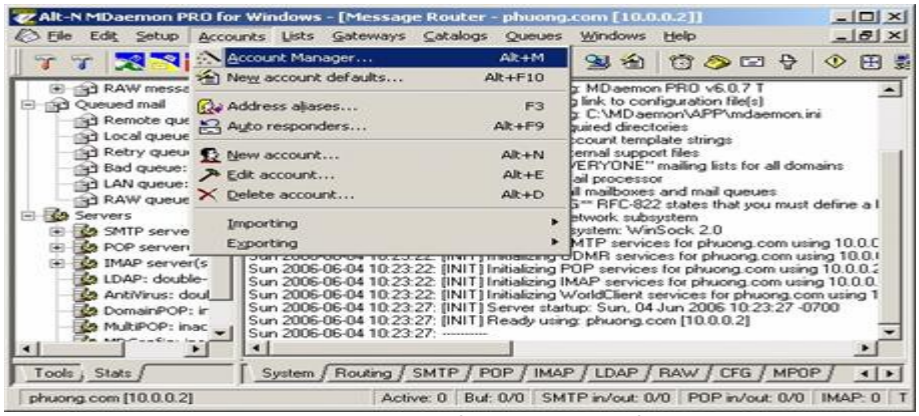
Tab **DNS**:

- **Primary DNS server IP** ta điền **10.0.0.2** rồi **OK**



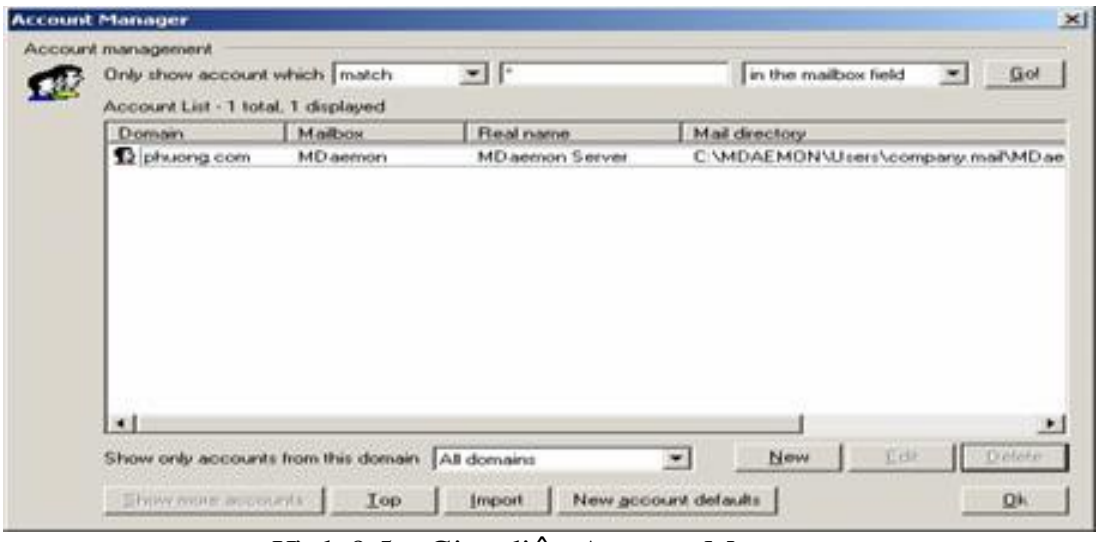
Hình 9.3 – Chỉ định IP cho Primary DNS server IP

Mở trình đơn **Accounts**, chọn **Account Manager**



Hình 9.4 – Quản lý tài khoản

Khi màn hình **Account Manager** xuất hiện, chọn nút **New;**

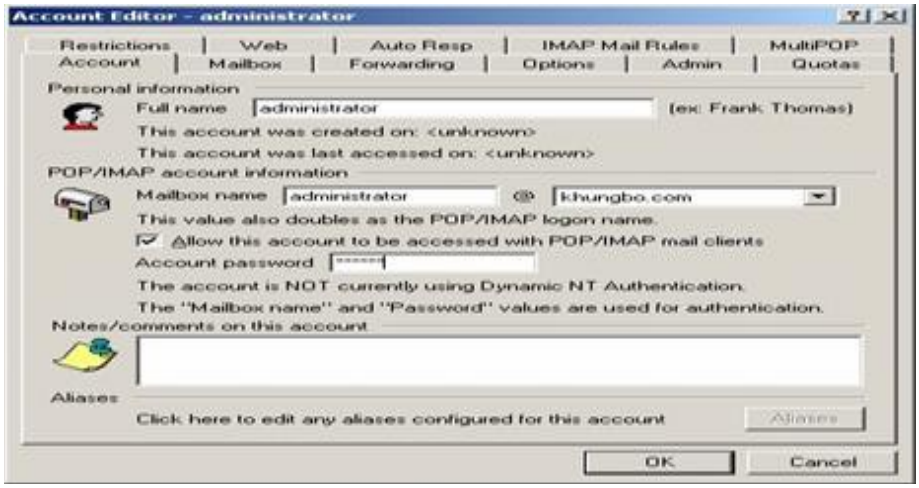


Hình 9.5 – Giao diện Account Manager

Trong cửa sổ **Account Editor**:

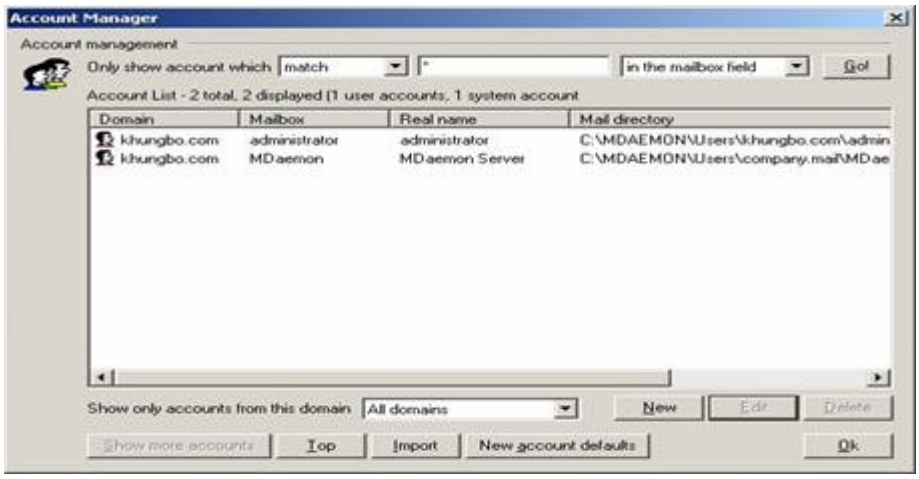
- Full name và **Mailbox name**: điền **administrator**

- **Account password**: ta điền 123456 rồi **OK**



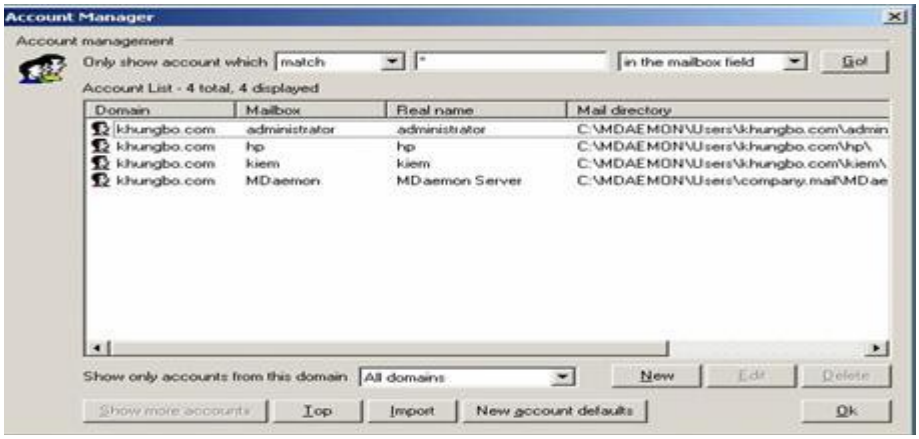
Hình 9.6 – Khai báo thông tin Account

Lúc này màn hình **Account Manager** xuất hiện **account administrator** (hình 9.7)



Hình 9.7 – Account Administrator sau khi được khai báo

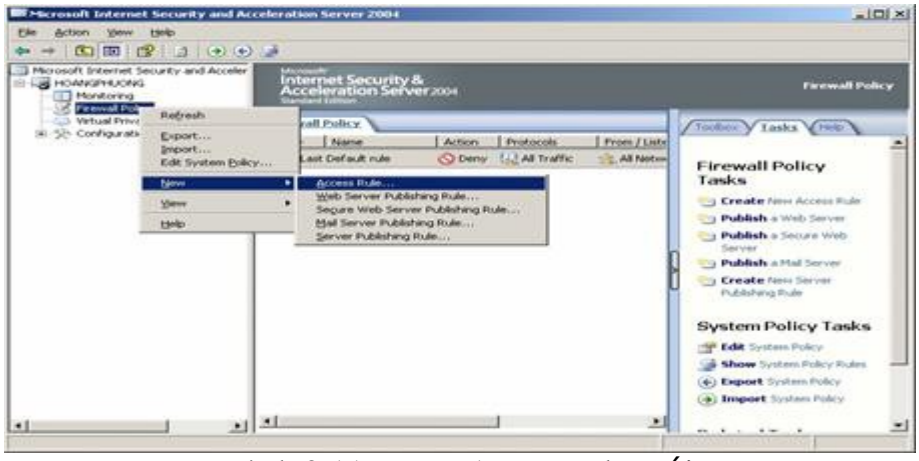
Ta tiến hành tạo thêm 2 account nữa (kiem và hp).



Hình 9.10 – Các account sau khi được khai báo

Sau khi tạo các **account** trong **MDaemon**. Tiến hành gửi mail kiểm tra hoạt động. Để gửi mail giữa **2 máy ISA** và **máy AD**, trên máy **ISA** cần tạo ra **1 rule** để cho **Internal** thông với **Local Host**.

Ta chọn **Firewall Policy** nhắp chuột phải rồi chọn **New** rồi chọn **Access rule**



Hình 9.11 – Tạo Access rule mới

Màn hình **Welcome to the New Access Rule Wizard** xuất hiện, điền **internal to local** rồi **Next**

Hình 9.12 – Chỉ định tên của Access rule

Màn hình **Rule Action** xuất hiện, chọn **Allow** rồi **Next**

Chọn **All outbound traffic** trong **This rule applies to**, chọn **Next**

Trong màn hình **Access Rule Souces**, chọn nút **Add** rồi **Network** rồi chọn **Internal** và **Local**, sau đó **Close** rồi **Next**

Màn hình Access Rule Destination: chọn Internal và Local rồi Next

Màn hình **User Sets Ta chọn All Users** rồi **Next** sau đó **Finish** rồi **Apply**.

➥ Tại máy **ISA**, mở chương trình **Outlook Epress**

Khi mở chương trình **Outlook Express**, nếu chưa tạo mail **POP3** lần nào thì **Outlook Express** yêu cầu tạo. Lúc đó màn hình **Your name** xuất hiện

- **Display name**: điền **administrator**

Trong màn hình **Internet E-mail Address**:

- **Email address**: điền **administrator@khungbo.com**

Trong màn hình **E-mail Server Name**:

- **Incoming** và **Outgoing**: điền **IP** của máy cài **mail Mdaemon** là **10.0.0.2**

Màn hình Internet Mail Logon xuất hiện, bỏ dấu chọn Remember password, chọn Next

Như vậy **mail POP3** đã được tạo trên máy ISAxong ; tắt **Outlook Express**.

➧ Máy **AD** cho **account kiem** là tạo **mail POP3** cho **account kiem** trên **máy AD**

➧ Tại **máy ISA account administrator** ta tiến hành gửi **mail** cho **account kiem**

Mở **Outlook Express** màn hình **logon** xuất hiện, đăng nhập với **User Name** (**administrator**) và **Password** (123456) tương ứng.

Màn hình **mail** xuất hiện, chọn mục **Inbox**; lúc này sẽ thấy mail do **MDaemon** gửi tới Ta bấm vào Create Mail.

Bây giờ ta sẽ gửi **mail** cho **account kiem**

- **To**: điền **kiem@khungbo.com**

- **Subject**: điền **test mail,** nội dung là **abc** rồi bấm **Send**

➧ Tại **Máy AD**, kiểm tra **account kiem** nhận được **mail** do **account admintrator** gửi đến chưa

Mở chương trình **Outlook Express** với **account kiem** sẽ nhận đươc **mail** do **administrator** gửi đến

Khi mail trong mạng chạy tốt, tiến hành Publishing Mail để người sử dụng ngoài mạng sử dụng account của mình vẫn có thể gửi mail**.**

2. Publishing Mail

Mục tiêu: …

Mở Firewall Policy, nhắp chuột phải chọn New, chọn Mail Server Publishing Rule.

Màn hình **Welcome to the New Mail Server Publishing Rule Wizard** xuất hiện, điền **Publishing Mail** rồi **Next**

Khi màn hình **Select Access Type** xuất hiện, chọn **Client access: RPC, IMAP, POP3, SMTP** rồi **Next**

Trong màn hình **Select Services**, đánh dấu vào **POP3** và **SMTP** rồi **Next**

Màn hình **Select Server** xuất hiện: điền **IP** là **10.0.0.2**

Màn hình **IP Addresses** xuất hiện: đánh dấu vào **External** rồi **Next**

Khi màn hình **Completing the New Mail Server Publishing Rule Wizard** xuất hiện, chọn **Finish.**

Trên "máy tính ngoài mạng", mở chương trình Outlook Express

Sau khi mở chương trình Outlook Express nếu ta chưa tạo mail POP3 lần nào thì Outlook Express yêu cầu tạo. Lúc đó màn hình Your name xuất hiện:

- Display name: điền hp

Màn hình **Internet E-mail Address**:

- E-mail address: điền **hp@khungbo.com** rồi chọn **Next**

Màn hình **E-mail Server Names**:

- **Incoming** và **Outgoing**, điền **IP** là **192.168.1.100** (không điền **IP** của máy cài **Mdaemon 10.0.0.2**), chọn **Next**

Khi màn hình **Internet Mail Logon** xuất hiện, bỏ chọn **Remember password**, **Next**

Vậy là ta đã tạo xong **Mail POP3** cho **account hp**.

Mở chương trình **Outlook Express** lại với **account hp**

Màn hình **Outlook Express** xuất hiện, bấm vào **Create Mail**

Thử gửi mail cho **administrator** khi đang ở ngoài mạng (kiểm tra **Publishing Mail** có thành công không)

- To: điền **administrator@khungbo.com**

- **Subject**: text mail ngoài mạng, nội dung: **admin**. Chọn nút **Send** để gửi

Tại máy ISA, kiểm tra **account hp** gửi **mail** đến cho **administrator** có nhận được không

Mở **Outlook Express** của **administrator** sẽ thấy có **mail** gửi từ **hp** gởi tới; như vậy là **Publishing mail** thành công

3. Cấu hình lọc mail

Mục tiêu: Trình bày các bước cấu hình lọc mail, cụ thể:

- Cài IIS và SMTP NNTP

- Cài đặt dịch vụ Message Screener

- Cấu hình SMTP

- Kiểm tra bộ lọc mail

Cấu hình lọc mail khi mail được gửi đến có những từ do admin lọc sẵn sẽ tự động chuyển đến cho administrator.

Muốn tiến hành lọc mail ISA phải có dịch vụ **Message Screener**

Muốn cài được **Message Screener** trong **ISA** phải cài **IIS** và **SMTP, NNTP**

➧ Tiến hành cài **IIS** và **SMTP NNTP**:

- Mở **Control Panel**, chọn **Add or Remove Programs**

- Chọn Add\Remove Windows Components

- Chọn **Application Server**, chọn nút **Details**

- Trong màn hình **Application Server,** chọn **Internet Information Service (IIS)** rồi bấm nút **Details**. Khi **m**àn hình **Internet Information Services (IIS)** xuất hiện, chọn **World Wide Web Service** rồi bấm **Details**.

- Trong màn hình **World Wide Web Service**, chọn **World Wide Web Service** rồi bấm **OK**.

- Trở về màn hình **Internet Information Services (IIS),** đánh dấu vào **SMTP** và **NNTP**, chọn **OK**.

- Trở về màn hình **Windows Components Wizard,** lúc này **Application Server** đã được đánh dấu, chọn **Next**.

Lúc này ta đã cài được **IIS**, **SMTP** và **NNTP**.

➧ Cài đặt dịch vụ **Message Screener**:

Khi cài **IIS**, **SMTP** và **NNTP** xong thì ta tiếp tục cài dịch vụ **Message Screener**

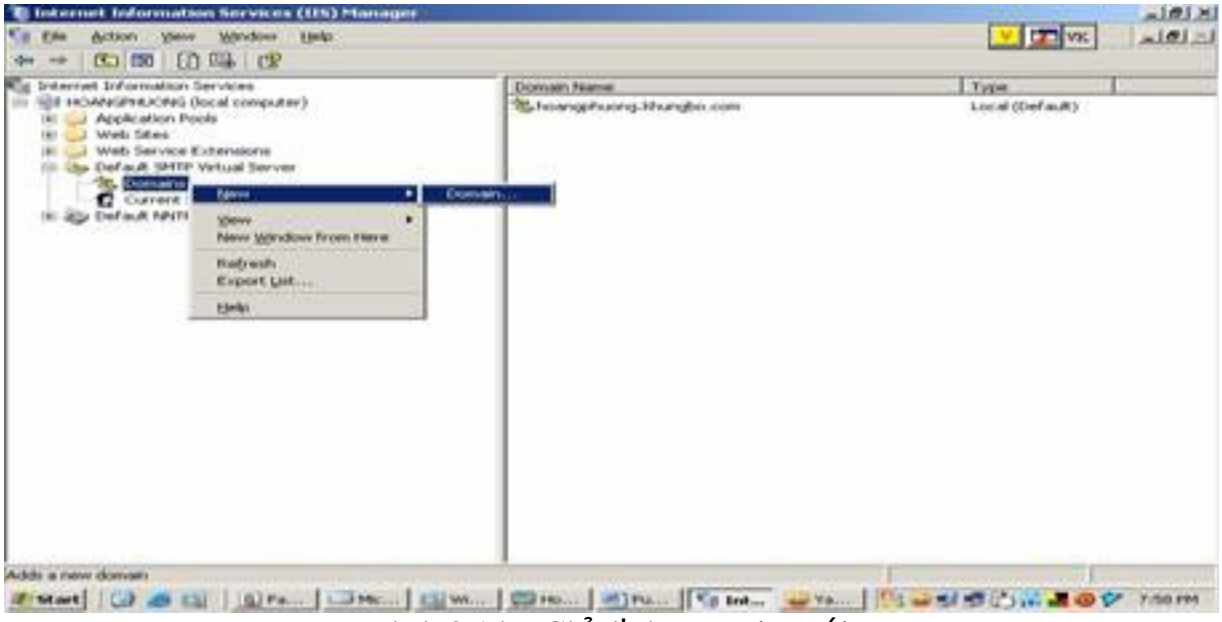
Mở chương trình cài **ISA**, chọn **Modify / Next**. Chọn cài thêm dịch vụ **Message Screener** cho ISA (hình 9.13), chọn Next.

Hình 9.13 – Cài thêm dịch vụ Message Screener

➥ Tiến hành cấu hình **SMTP** sau khi cài xong dịch vụ **Message Screener**

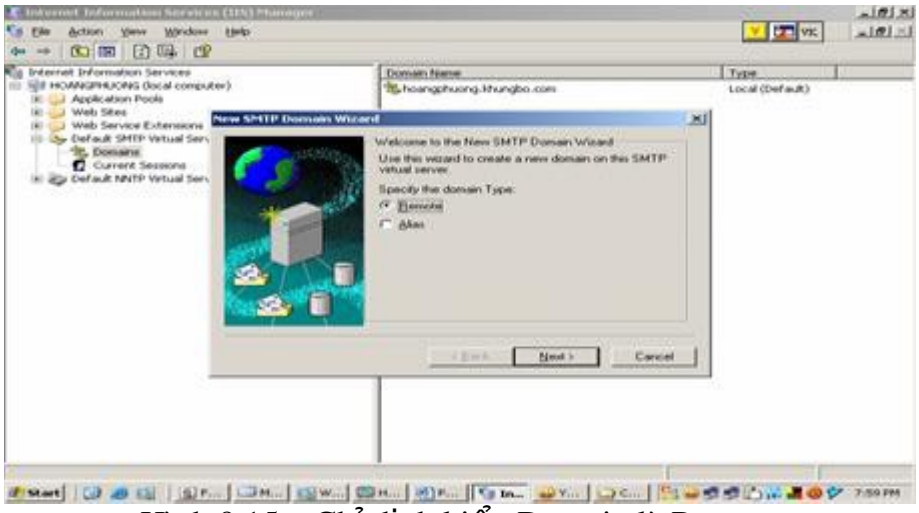
- Vào **Start / Program / Administrator Tools / Internet Information Services (IIS) Manager**

- Khi màn hình Internet **Information Service (IIS) Service** xuất hiện (hình 9.14), bấm vào dấu + của **Default SMTP Virtual Server** rồi chọn **Domain** nhắp chuột phải chọn **New** rồi **Domain**



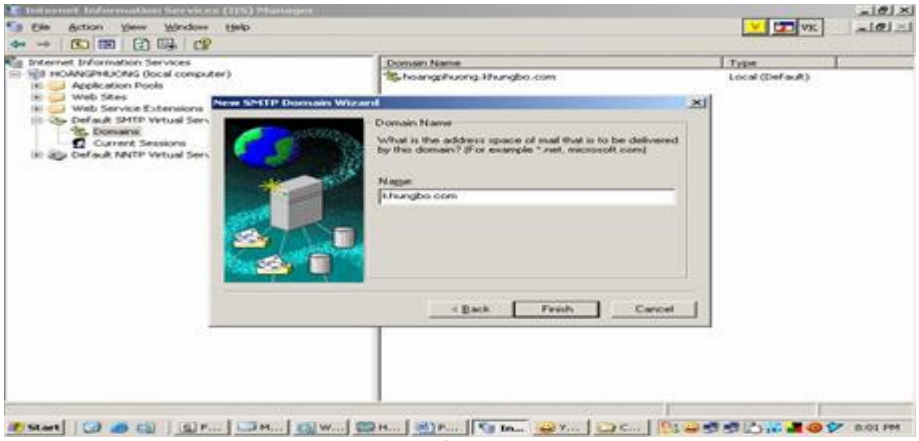
Hình 9.14 – Chỉ định Domain mới

- Trong màn hình **Welcome to the New SMTP Domain Wizard** (Hình 9.15), chọn **Remote / Next**



Hình 9.15 – Chỉ định kiểu Domain là Remote

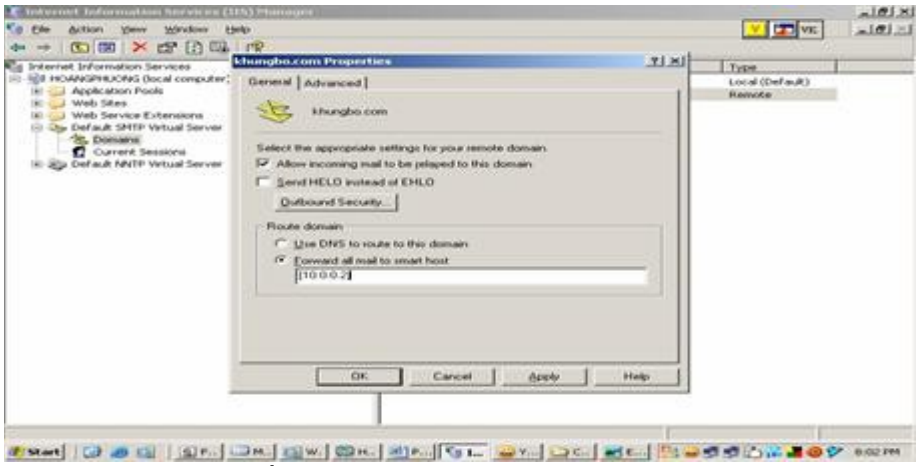
- Màn hình **Domain Name** xuất hiện, điền domain tương ứng (**khungbo.com**)



Hình 9.16 – Chỉ định tên Domain

Bây giờ trong mục **Domain** đã có tên Domain (**khungbo.com**), chọn tên Domain đó (**khungbo.com**), nhấp chuột phải chọn **Properties**

Chọn tab General trong màn hình **khungbo.com Properties**



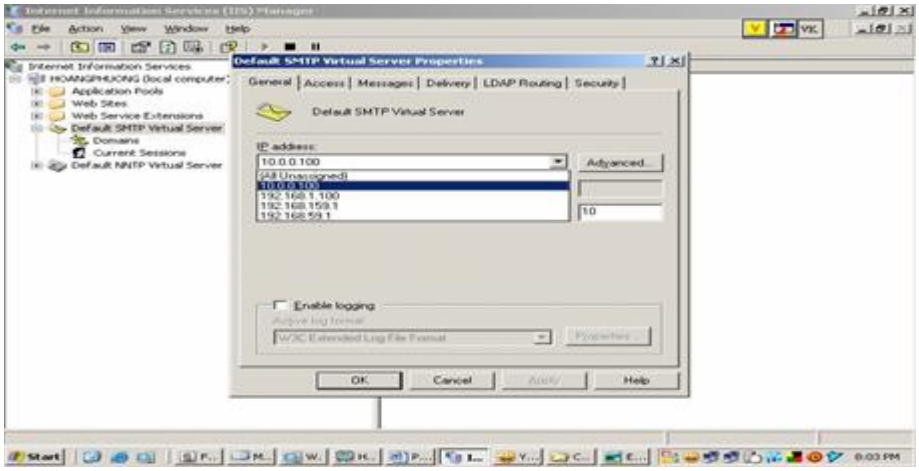
Hình 9.17 – Thiết lập các thuộc tính cho Domain tương ứng

Đánh dấu vào **Allow incoming mail to be relayed to this domain**

Chọn **Forward all mail smart to the Domain**, điền địa chỉ **10.0.0.2**, chọn **OK.**

Nhắp chuột phải vào **Default SMTP Virtual Server**, chọn **Properties**

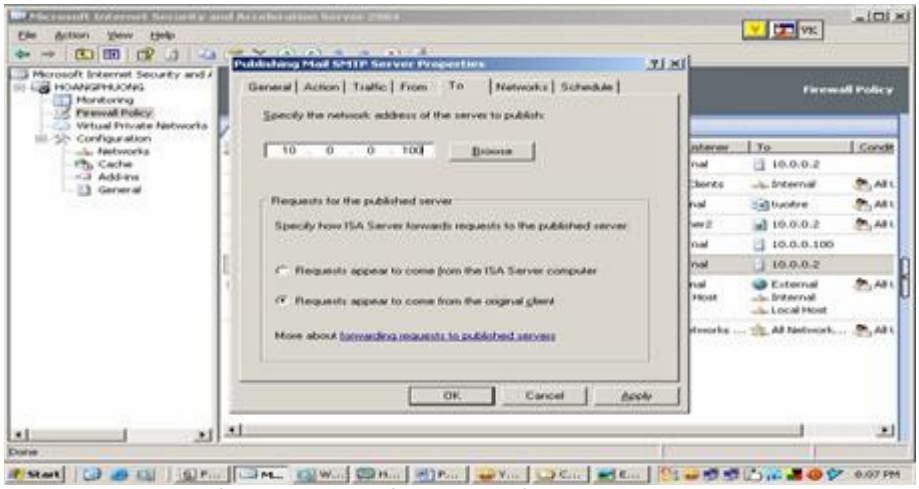
Trong hộp thoại **Default SMTP Virtual Server Properties** (hình 9.18)**,** chọn **IP** là **10.0.0.100** cho **IP address**, chọn nút **OK.**



Hình 9.18 – Thiết lập đối với **Default SMTP Virtual Server Properties**

Quay lại rule Publishing Mail SMTP Server mà ta đã Publishing Mail, nhắp chuột phải, chọn Properties

Trong màn hình **Publishing Mail SMTP Server Properties** (hình 9.20), Tab **To**: điền **IP** là **10.0.0.100**, chọn nút **Apply / OK**

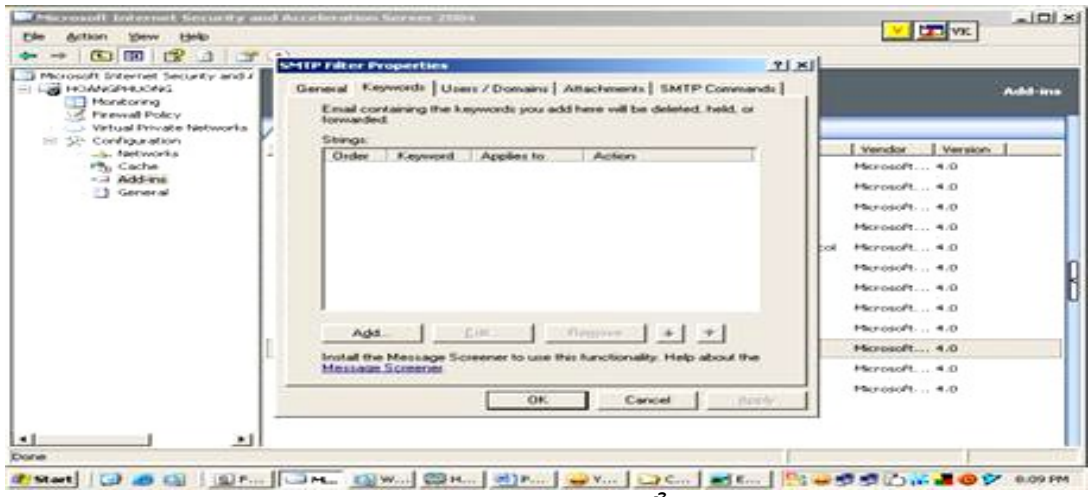


Hình 9.20 – Chỉ định địa chỉ mạng của server đã Publishing Mail

Chọn **Configuration** rồi **Add -ins**

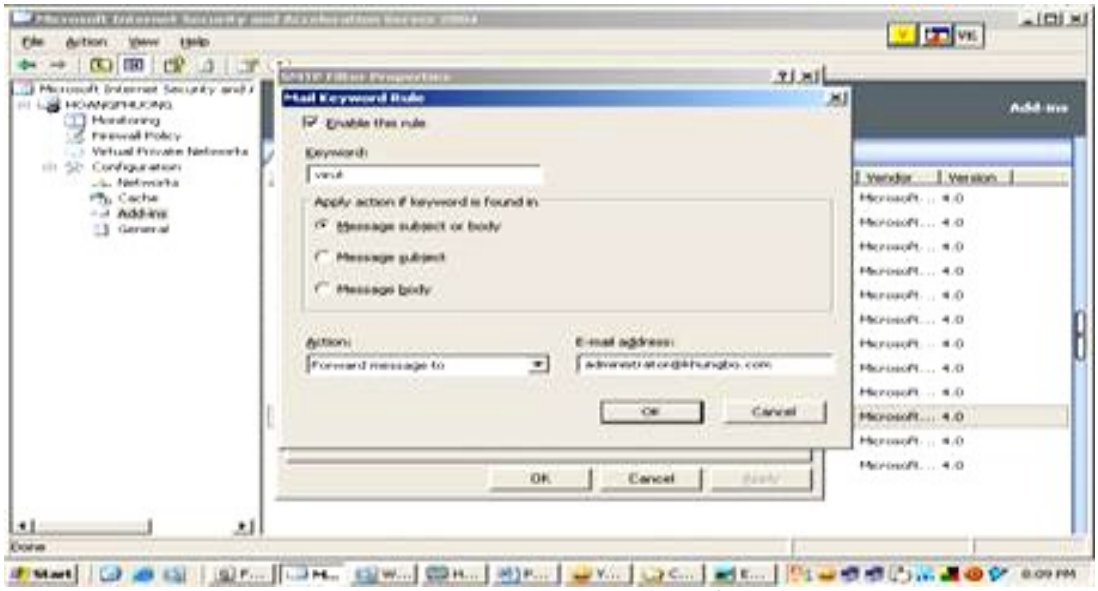
- Nhắp chuột phải lên **SMTP Fiter**, chọn **Properties**

Trong màn hình **SMTP Filter Properties**, chọn Tab **Keywords**, chọn nút **Add** (hình 9.21)



Hình 9.21 – Thêm rule để lọc mail

Trong màn hình **Mail Keyword Rule**, đánh dấu vào **Enable this rule Keyword** (hình 9.22)



Hình 9.22 – Kích hoạt rule với từ chỉ định là virut

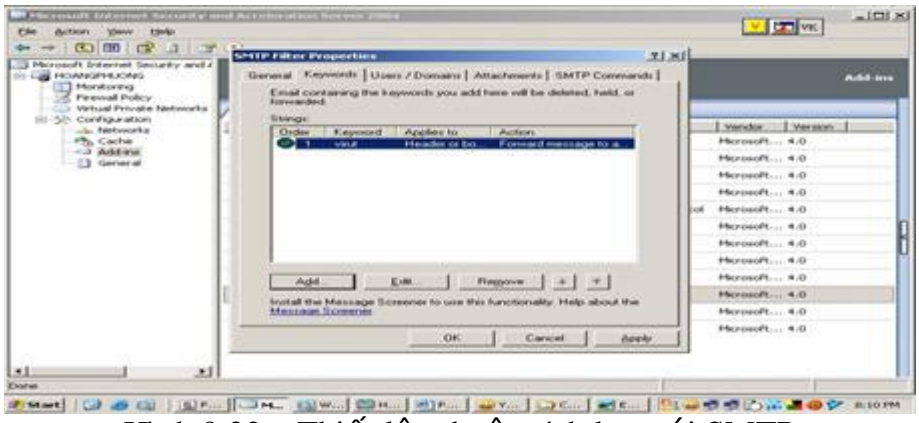
- Keyword: điền **virut**

- **Apply action if keyword is found in**: chọn **Message subject or body**

- **Action**: chọn **Forward message to**

- **E-mail address**: điền **administrator@khungbo.com / OK**

Lúc này ở hộp thoại **SMTP Filter Properties** (hình 9.23), trong **setting** có mục **virut** (được tạo trong **Keyword**), chọn **Apply,** rồi **OK**.



Hình 9.23 – Thiết lập thuộc tính lọc với SMTP

➧ Kiểm tra bộ lọc mail:

Tại "máy tính ngoài mạng", mở chương trình **Outlook Express** bằng **account hp**

Khi màn hình **Outlook Express** xuất hiện, chọn **Create Mail** để tiến hành gửi mail cho **account kiem** (nội dung là **virut**)

Tại máy **AD** ta tiến hành kiểm tra có nhận được **mail** do **hp** gửi đến **kiem** không

- Mở **Outlook Express** với account **kiem** thì thấy không có **mail** của **hp**

Tại máy **ISA** ta tiến hành kiểm tra **mail**

- Mở **Outlook Expreess** bằng account **administrator** sẽ thấy có mail của **hp**. Mail này được chuyển đến **administrator** do cấu hình lọc mail với từ khoá là **Virut** sẽ tự động chuyển đến **administrator**

4. Publishing Web

Mục tiêu: Trong các phần 4 (Publishing Web), 5 (Publishing FTP), 6 (Publishing Terminal Services) sẽ trình bày cách thức để mở các Port sao cho các máy từ External Network có thể truy cập vào mạng. Công việc này còn gọi là Server Publishing.

Muốn tạo ra trang web, máy **AD** cần phải cài chương trình **IIS**. Khi Máy **AD** đã cài **IIS** ta tiến hành tạo ra 1 trang **web**:

- Vào ổ đĩa **C:\Inetpub\wwwroot**, tạo file **Text Document**

- Sau khi tạo file **Text Document**, đổi tên thành **default.htm**

- Nhắp chuột phải vào **file default.htm** chọn **Edit**. Nhập nội dung file: **chao mung den trang web** và lưu trữ.

Sau khi tạo trang web, mở chương trình **IE** rồi nhập **http://10.0.0.2**; Nếu thấy trang web xuất hiện là đúng.

Publishing Web tại máy **ISA**:

Chọn **Firewall Policy**, nhắp chuột phải chọn **New**, rồi chọn **Web Server Publíhing Rule**. Trong màn hình **Wellcome to the New Web Publishing Rule Wizard** xuất hiện:

- **Web publishing rule name**: điền **Publish Web**, chọn **Next**

Trong hộp thoại **Select Rule Action**: chọn **Alow / Next**

Tại màn hình **Define Website to Publish**:

- Computer name or IP address: điền **10.0.0.2 / Next**

Trong **Public Name Details**: **Accept requests for:** chọn **Any domain name / Next**

Khi màn hình **Select Web Listener** xuất hiện, chọn nút **New**

Màn hình **Welcome to the New Web Listener Wizarrd** xuất hiện: **Web listener name**: điền **Listener2 / Next**

Trong màn hình **IP addresses**: đánh dấu vào **External / Next**

Khi màn hình **Port Specification** xuất hiện, đánh dấu vào **Enable HTTP** và nhập: **80**

Sau khi hoàn tất, kiểm tra thử trên "máy tính ngoài mạng": mở chương trình **IE** và nhập địa chỉ: http://192.168.1.100; Nếu trang web hiển thị là đúng.

5. Publishing FTP

Trước tiên ta phải cấu hình **FTP**.

➧ Cài đặt **FTP**: **Start / Setting / Control Panel / Add or Remove Programs**

Trong cửa sổ **Add or Remove Programs**, chọn **Add\Remove Windows Components**

Từ màn hình **Windows Components Wizard,** chọn **Application Server**, chọn nút **Detals**. Khi cửa sổ **Application Server** xuất hiện, chọn **Internet Information Service (IIS)** rồi bấm nút **Details**.

Màn hình **Internet Information Services (IIS)** xuất hiện, chọn **File Transfer Protocol (FTP) Service**, **OK.**

Trở về màn hình **Windows Components Wizard,** ta thấy **Application Server** được đánh dấu, chọn **Next**.

Chương trình bắt đầu cài **FTP**; Khi quá trình cài đặt **FTP** hoàn tất, chọn nút **Finish.**

➧ Vào **Start / Program / Administrator Tools / Internet Information Services (IIS) Manager**

Chọn **FTP Site**, nhắp chuột phải lên **Default FTP Site** chọn **Properties**. Khi màn hình **Default FTP Site Properties** xuất hiện:

- Tab **FTP Site**: **IP address** Ta chọn **IP 10.0.0.2**

- Tab **Home Directory**: đánh dấu vào ô **Write**

- Tab **Security Accounts**: chọn nút **Browse**, khi cửa sổ **Select User** xuất hiện chọn nút **Advanced**; chọn nút **Find Now** để chỉ định **administrator**, chọn **OK.**

Lúc này ta thấy **User name**: **TUANH\administrator**, **Password**: điền **123456**, **OK.** Tại **Confirm Password**, xác nhận **Password**.

Khi cấu hình **FTP** xong, chép các file hay thư mục vào **FTP** (ở đây minh họa chép các file trong **C:\Program Files\NetMeeting**).

Chép các file trong **C:\Program Files\NetMeeting** rồi dán vào **C:\Inetpub\ftproot**

➧ Kiểm tra hoạt động của **FTP**: Sau khi chép các file vào **FTP**, kiểm tra **FTP** coi có hoạt động không:

Tại máy **ISA**, mở **IE** nhập **ftp://10.0.0.2**. Khi màn hình **Log On** xuất hiện:

- **User name**: điền **administrator**

- Password: **123** (**Password 123** là **password** của **administrator**)

Khi **Log on** được vào **FTP** thì sẽ thấy được các file

➧ Sau khi truy cập thành công **FTP**, tiến hành **Publicshing FTP** để máy ngoài **Internet** cũng có thể truy cập được **FTP**:

Chọn **Firewall Policy / New / Server Publishing Rule**.

Điền **Publiching FPT / Next**; trong hộp thoại, điền **10.0.0.2 / Next**

Chọn **FTP Server / Next**

Chọn **External / Next**

Nhấn **Finish** để hoàn tất **/ Apply**.

Chọn **Configuration / Network / Network Rules /** nhắp chuột phải lên **Internet Access**, chọn **Properties**

- Tab Network Relationship: chọn Network Address Transtation (NAT) / OK

Như vậy là ta đã Publishing FTP xong

➧ Kiểm tra **Publishing FTP**: Sau khi **Publishing FTP** xong, kiểm tra **Publishing FTP** trên "máy tính ngoài mạng" có thanh công không: mở **IE** nhập **ftp://192.168.1.100**. Khi màn hình **Log On** xuất hiện:

- Users name: điền **administrator**

- Password: điền **123**

Nếu thấy được các file trong **FTP** nghĩa là đã **Publishing FTP** thành công.

Lúc này, có thể **Download** được các file trong **FTP** (copy về được nhưng không **Upload** file lên **FTP** được, nếu copy file rồi Paste vào **FTP** thì thấy bị báo lỗi)

➧ Muốn **Upload file** lên được **FTP**, tại máy **ISA** nhắp chuột phải lên **Publishing FPT** chọn **Configure FTP**

Bỏ đánh dấu **Read Only / OK / Apply**.

Lúc này, mở **IE** trên "máy tính ngoài mạng" nhập ftp://192.168.1.100, copy 1 số file rồi Paste vào **FTP** sẽ không bị lỗi.

6. Publishing Terminal Services

➧ Máy **AD**: Nhắp chuột phải **Icon Computer**, chọn **Properties**

- Tab **Remote**: đánh dấu vào **Allow users to connect remotely to this computer**, chọn **Select Remote Users / Add / Advanced**.

- Chọn **Find Now** để chỉ định **administrator / OK**

➧ Máy **ISA**:tiến hành **Publishing Terminal Services**

- Chọn **Firewall Policy / New / Server Publishing Rules.**

- Điền **Remote Desktop Connection / Next**

- Điền **IP 10.0.0.2 / Next**

- Chọn **RDP (Terminal Services) Server / Next**

- Chọn **External / Next**

- Chọn **Finish** để hoàn tất / **Apply**. Như vậy, **Publishing Terminal Services** đã được thực hiện.

➥ Tại "máy tính ngoài mạng", tiến hành kiểm tra **Publishing Terminal Server** có thành công không

Vào Start / Programs / Accessories / Communications / Remote Desktop Connection

- Computer: **IP 192.168.1.100**

- User name: **administrator**

- Password: **123**

- Chọn nút **Connect**

Hình 9.24 – Remote Desktop Connection

Màn hình **Connect** thành công và ta có thể điều khiển được

Câu hỏi

1. Mail Mdaemon là gì? Tại sao phải dùng Mail Mdaemon?

2. Cho biết mục đích và ý nghĩa của các tiến trình Publishing Mail, lọc mail, Publishing web, Publishing FTP.

Bài tập thực hành

1. Cài đặt hệ thống Mail Mdaemon và gửi mail qua lại

Máy AD cài Mail Mdaemon
Mở chương trình Outlook Epress trên máy ISA, tạo mail POP3
Tạo mail POP3 cho account trên máy AD
Từ máy ISA (account administrator), tiến hành gửi mail cho account trên máy AD
Tại Máy AD ta kiểm tra account kiem nhận được mail do account admintrator gửi đến chưa

2. Tiến hành Publishing Mail để cho 1 ai đó ở ngoài mạng sử dụng account của mình vẫn có thể gửi mail được

3. Cấu hình lọc mail:

- Cài IIS, SMTP và NNTP
- Cài đặt dịch vụ Message Screener
- Cấu hình SMTP

Kiểm tra tính năng lọc mail

4. Xuất bản web:

- Tạo một trang web
- Xuất bản web

5. Publishing FTP:

- Cài đặt FTP

- Cấu hình Internet Information Services (IIS) Manager
- Kiểm tra hoạt động của FTP
- Publicshing FTP để máy ngoài Internet có thể truy cập được FTP
- Kiểm tra Publishing FTP

BÀI 10: MONITOR ISA SERVER

Mã bài: MĐ 36-010

Mục tiêu của bài:
- Trình bày được các Tab trong Monitor;
- Phát hiện và khắc phục được các dịch vụ thông qua các tab trong Monitor;
- Thực hiện sao lưu và khôi phục lại máy ISA.
- Thực hiện các thao tác an toàn với máy tính.

1. Trình bày các tab trong Monitor

Mục tiêu: Giới thiệu chức năng của các tab trong Monitor Isa Server

1.1. Tab Session

- Cho biết đang có bao nhiêu **Session** diễn ra thông qua ISA

- Mỗi **Session** thông qua dạng nào (**SecaureNAT**, **Web Proxy**, **Firewall Client**) để biết được máy tính đang đi ra ngoài mạng thông qua **ISA** bằng dạng nào

1.2. Tab Services

- Trình bày những dịch vụ nào của **ISA** đang chạy tốt.

- Khởi động từng dịch vị khi **ISA** có trục trặc.

Ví dụ khi ta áp dụng 1 rule nào đó mà nó không chạy, thay vì khởi động lại máy tính, ta có thể restart lại dịch vụ là **Microsoft Firewall** (bằng cách chọn **Microsoft Firewall**, rồi nhắp chuột phải chọn **stop**; sau đó tiếp tục **restart** lại)

1.3. Tab Report

Tab Report dùng để tạo báo cáo thống kê, giúp thống kê lại trong khoảng thời gian nào đó máy nào trong mạng Lan đi ra web nhiều nhất chiếm nhiều băng thông nhất và lấy dung lượng nhiều nhất…

1.4. Tab Connectivity

Tab Connectivity cho phép tạo ra các kết nối phục vụ cho việc kiểm tra. Chẳng hạn, nếu trang web ngoài internet thường xuyên truy cập gặp trục trặc, thay vì phải ra ngoài CMD để ping kiểm tra nó có hoạt động không,có thể thực hiện ở đây dạng **Connectivity**. Mỗi khi muốn kiểm tra, chỉ cần kích hoạt Connectivity sẽ thấy thông báo lỗi.

1.5. Tab logging

Tab logging cho phép biết rõ từng chi tiết IP nào ra internet và chiếm dung lượng bao nhiêu, đi ra bằng Rule nào và bị Rule nào chặn lại .v.v…

2. Phát hiện các đợt tấn công gửi mail cho admin

Mục tiêu: Trình bày cách theo dõi, phát hiện các đợt tấn công bằng cách gửi mail cho admin.

Chọn **Configuration / General / Enable Intrusion Detection and DNS Attack Detection**

Khi màn hình **Intrusion Detection** xuất hiện, đánh dấu vào **Port scan**

Chọn Tab **DNS Attack**: đánh dấu vào **DNS zone trransfer / OK / Apply**

Chọn **Monitoring / Tab Alerts / Configure Alerts Defintions**

Khi cửa sổ **Alerts Properties** xuất hiện, tìm và chọn **Intrusion detected / Edit**

Trong màn hình **Intrusion detected Properties**, đánh dấu vào **Send –e-mail** (báo động khi có tấn công sẽ gửi mail thông báo cho **admin**)

- SMTP server: điền **IP 10.0.0.2**

- From và To: điền địa chỉ mail của admin (administrator@khungbo.com), chọn nút **Test** nó sẽ gửi **1 mail** đến **administrator;** nếu kiểm tra thấy có **mail** là đúng.

- Đánh dấu vào **Run a program**: dùng khi có chương trình nào được viết ra để bảo vệ máy tính, nếu khi có tấn công thì chương trình này sẽ chạy và bảo vệ)

Ở đây minh họa dùng thử bằng chương trình **notepad. exe** để xem chức năng hoạt động của nó)

Sau đó, mở **Outlook Express** sẽ thấy có 1 bức mail

"Máy tính ngoài mạng" thử tấn công bằng cách **Scan Port**.

Bật chương trình **SuperScan4** lên

Khi màn hình **SuperScan** xuất hiện, **Hostname/IP** điền **IP 192.168.1.**

Chọn **Tab Host and Service Discovery**, bỏ dấu chọn **Host dícovery**

Chọn tab **Scan**, bấm nút **Play** thì chương trình tự động thực hiện **scan port**

Lúc này, chương trình **Scan** được **10 Port**; Muốn biết rõ từng **port** đó một cách chi tiết, nhấn vào **View HTML Results** sẽ thấy trình bày chi tiết từng **Port** mà nó **Scan** được

Quay lại **Máy ISA** thì thấy **Notepad** được bật lên do có người đang tấn công

Kiểm tra **mail** thì thấy có 1 bức mail báo có 1 địa chỉ **IP 192.168.1.5** đang tiến hành tấn công.

3. Network Templates (mô hình mẫu các thông số cấu hình mạng)

Mục tiêu: Trình bày các loại Network Templates và cách sử dụng từng loại cùng với các lựa chọn chính sách Firewall.

ISA Server firewall mang đến cho chúng ta những thuận lợi to lớn, một trong những số đó là các Network Templates. Với sự hỗ trợ các Templates, chúng ta có thể cấu hình tự động các thông số Network, Network Rule và Access Rules.

Network Templates được thiết kế nhanh chóng tạo được cấu hình nền tảng cho những gì mà chúng ta có thể xây dựng.

Các loại Network Templates:

- Edge Firewall: được sử dụng khi ISA gắn 2 card Network. Có một Network interface kết nối đến Internet và một Network interface kết nối với Internal Network.

- 3-Leg Perimeter được sử dụng khi Firewall gắn 3 Card Network. Có Network interface (kết nối Internet) và Internal interface (kết nối mạng nội bộ) và DMZ interface (kết nối mạng vành đai – Perimeter Network).

- Front Firewall: Đóng vai trò một front-end firewall trong mô hình back-to-back. Back-to back là mô hình kết nối 2 Firewall làm việc với nhau theo kiểu trước (front) sau (back); Phía ngoài Front Firewall có thể là Internet giữa Front và back firewall có thể là DMZ network và phía sau back firewall là Internal network.

- Single Network Adapter: được áp dụng khi muốn loại chức năng Firewall. Được dùng trong những trường hợp khi ISA chỉ có 1 card Network đóng vai trò là hệ thống lưu giữ cache – Web caching server.

Những lựa chọn cho chính sách Firewall khi dùng Network Edge Firewall Templates (bảng 10.1)

Firewall Policy	Mô Tả
Block All (ngăn chặn tất cả)	Ngăn chặn tất cả truy cập qua ISA

Block Internet Access, allow access to ISP network services (Ngăn chặn truy cập ra Internet nhưng cho phép truy cập đến dịch vụ của ISP)	Ngăn chặn tất cả truy cập qua ISA ngoại trừ những truy cập đến các Network services như DNS services Lựa chọn này được dùng khi các ISP cung cấp những dịch vụ này Lựa chọn này sẽ xác định chính sách Firewall như 1. Allow DNS from Internet Network and VPN Client Network to External Network (Internet) - cho phép Internal Network và VPN Client Network dùng DNS của ISP để xác định Host names bên ngoài
Allow Limited Web access (cho phép truy cập web có giới hạn)	Chỉ cho phép truy cập Web dùng các giao thức HTTP, HTTPS, FTP còn lại các truy cập khác sẽ bị ngăn chặn Các Rule sau sẽ được tạo 1. Allow HTTP ,HTTPS ,FTP from Internal Network to Exterrnal Network – Cho phép các truy cập dạng HTTP, HTTPS, FTP từ Internal Network ra bên ngoài 2. Allow all protocol from VPN Client Network to Internal Network – cho phép tất cả các giao thức từ VPN Client Network (từ bên ngoài) truy cạp vào bên trong mạng nội bộ
Allow Limited Web access and access to ISP network services (cho phép truy cập Web có giới hạn và truy cập đến một số dịch vụ ISP)	Cho phép truy cập Web có giới hạn dùng HTTP,HTTPS,FTP và cho phép truy cập ISP network services như DNS còn lại ngăn chặn tất cả các truy cập network khác Các Rule sau sẽ được tạo ra: 1. Allow HTTP, HTTPS, FTP from Internal Network and VPN Client Network to External Network (Internet) – Cho phép truy cập HTTP, HTTPS, FTP từ Internal Network và VPN Client Network ra External Network (Internet) 2. Allow DNS from Internal Network and VPN Client Network to External Network (Internet) – Cho Phép Internet Network và VPN Client Network truy cập dịch vụ DNS giải quyết các Hostname bên ngoài (Internet) 3. Allow all protocol from VPN Client Network to Internal Network – cho phép tất cả các giao thức từ VPN Client Network (từ bên ngoài) truy cập vào bên trong mạng nội bộ
Allow unrestricted access (Cho phép truy cập không giới hạn)	Cho phép không hạn chế truy cập ra Internet qua ISA Server 1. Allow all Protocols from Internal Network and VPN Client Network to External Network (Internet) – Cho phép dùng tất cả giao thức từ Internal Network và VPN Client Network tới External Network (Internet) 2. Allow all protocol from VPN Client Network to Internal Network – cho phép tất cả các gaio thức từ

	VPN Client Network (từ bên ngoài) truy cập vào bên trong mạng nội bộ

Cấu hình Edge Firewall

Chọn **Configuration / Network / Templates** trong **Task Pane** rồi nhắp vào **Edge Firewall /** Next

Chọn **Allow unrestricted access /** Next / Apply

Chọn lại Firewall policy, lúc này sẽ thấy xuất hiện 2 Rule được tạo ra bởi Edge Firewall.

2 Access Rule cho phép Internal network và VPN Client truy cập ra Internet và VPN Client cũng được quyền truy cập vào Internet network

4. Backup và Restore

Mục tiêu: Trình bày cách sao lưu và phục hồi ISA nhằm khắc phục khi xuất hiện các lỗi.

Backup:

- Chọn tên máy ISA, nhắp chuột phải chọn Backup…

- Chỉ định ổ C: để lưu backup ISA với tên là backup; chọn nút Backup

- Màn hình Set Password xuất hiện: Password và Corfirm password: điền 12345678 / OK.

Vậy là quá trình Backup đã xong.

Restore: Khi ISA gặp lỗi, có thể tiến hành Restore:

- Chọn tên máy tính ISA, nhắp chuột phải chọn Restore.

- Vào ổ đĩa C sẽ thấy File Backup đã được lưu, chọn file backup rồi nhấn Restore.

- Điền password: 12345678 / OK.

Câu hỏi

1. Nêu chức năng và ý nghĩa của mỗi tab trong Monitor.
2. Trình bày mô hình mẫu các thông số cấu hình mạng.

Bài tập thực hành

1. Kiểm tra và phát hiện các đợt tấn công gửi mail cho admin.
2. Thực hiện Backup cho máy ISA; sau đó, restore lại.

CÁC THUẬT NGỮ CHUYÊN MÔN

PHƯƠNG PHÁP VÀ NỘI DUNG ĐÁNH GIÁ:

- **Về kiến thức:**

Có khả năng phát hiện các sự cố.
Thực hiện được các biện pháp sao lưu dự phòng.
Đánh giá được các thông lượng đường truyền.
Có khả năng cài đặt, cấu hình kết nối Internet.
Trình bày được các tính năng và những nét đặc trưng của ISA Server.
Trình bày được các cơ chế sao lưu, phục hồi toàn bộ máy ISA Server.
Mô tả được các loại ISA Server Client đồng thời cài đặt và cấu hình đúng qui trình cho từng loại ISA Server Clien và những tính năng riêng trên mỗi loại.

- **Về kỹ năng:**

Cài đặt, gỡ bỏ được các phần mềm yểm trợ Terminal service.
Xác định được các nguyên nhân gây ra hỏng.
Sử dụng được các biện pháp sao lưu dữ liệu.
Giải quyết được các sự cố trên mạng.
Có khả năng cài đặt, quản lý các dịch vụ RAS.
Có khả năng kết nối một mạng riêng ảo VPN.
Có khả năng tiếp nhận các cuộc gọi ở xa.
Cài đặt và cấu hình được ISA Server trên windows Server.
Thực hiện được các Rule theo yêu cầu.
Cài đặt và cấu hình được các chính sách mặc định của Firewall, thực hiện chính xác thao tác sao lưu cấu hình mặc định của Firewall.

- **Về thái độ:**

Cẩn thận, thao tác nhanh, chuẩn xác, tự giác trong học tập.

TÀI LIỆU THAM KHẢO

[1]. Fergus Strachan, *Integrating ISA Server 2006 with Microsoft Exchange 2007*, 2008.

[2]. Phạm Hoàng Dũng - Hoàng Đức Hải, *Làm chủ Windows 2003 server*, NXB Thống kê, 2005.

[3]. Tô Thanh Hải, *Triển khai Microsoft Firewall với ISA Server*, NXB Lao Động - Xã Hội, 2010.