

Cài Đặt – Cấu Hình – Quản Trị ISA Server 2004 Firewall

Trong số những sản phẩm tường lửa trên thị trường hiện nay thì ISA Server 2004 của Microsoft là firewall được nhiều người yêu thích nhất do khả năng bảo vệ hệ thống mạnh mẽ cùng với cơ chế quản lý linh hoạt.

ISA Server 2004 Firewall có hai phiên bản Standard và Enterprise phục vụ cho những môi trường khác nhau, ISA Server 2004 Standard đáp ứng như cầu bảo vệ và chia sẻ băng thông cho các công ty có quy mô trung bình. Với phiên bản này chúng ta có thể xây dựng các firewall để kiểm soát các luồng dữ liệu vào và ra trên hệ thống mạng nội bộ của công ty. Kiểm soát quá trình truy cập của người dùng theo giao thức, thời gian và nội dung của các site nhằm ngăn chặn quá trình kết nối vào những trang web có nội dung không hợp lệ. Bên cạnh đó chúng ta còn có thể triển khai các hệ thống VPN Site to Site hay Remote Access hỗ trợ cho việc truy cập từ xa của các User, hoặc trao đổi dữ liệu giữa các văn phòng chi nhánh. Đối với các công ty có những hệ thống máy chủ quan trọng như Mail, Web Server cần được bảo vệ chặt chẽ trong một môi trường riêng biệt thì ISA 2004 cho phép chúng ta triển khai các vùng DMZ (thuật ngữ chỉ vùng phi quân sự) ngăn ngừa sự tương tác trực tiếp của các Internal/External User. Ngoài các tính năng mang tính bảo mật thông tin trên thì ISA 2004 còn có hệ thống cache giúp cho người dùng kết nối Internet nhanh hơn do thông tin trang web có thể được lưu giữ sẵn trên RAM hay đĩa cứng, điều này làm cho băng thông của hệ thống được tiết kiệm đáng kể. Chính vì lý do đó mà sản phẩm tường lửa này có tên gọi là Internet Security & Acceleration (bảo mật ứng dụng và tăng tốc băng thông).

ISA Server 2004 Enterprise được sử dụng trong các mô hình mạng lớn, cần những hệ thống mạnh mẽ để đáp ứng nhiều yêu cầu truy xuất của người sử dụng (User) bên trong và ngoài hệ thống. Ngoài những tính năng đã có trên ISA Server 2004 Standard, phiên bản Enterprise còn cho phép chúng ta thiết lập các hệ thống Array (mảng) các ISA Server cùng sử dụng một chính sách, điều này giúp dễ dàng quản lý và cung cấp tính năng Load Balancing (cân bằng tải) phục vụ tốt hơn các yêu cầu của tổ chức.

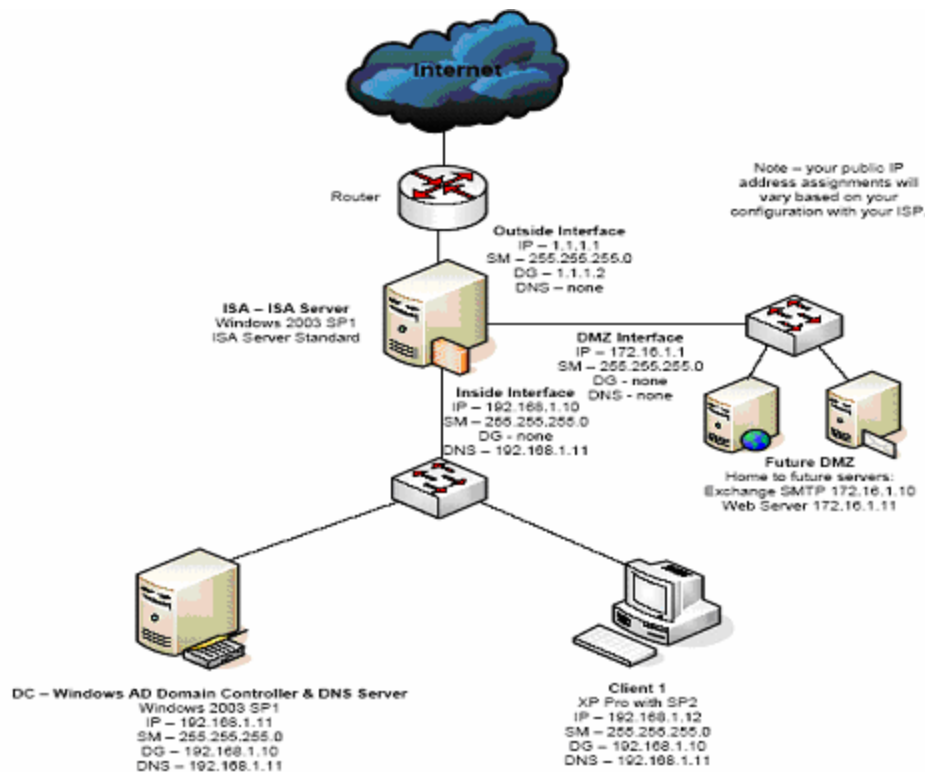
Để đáp ứng nhu cầu học tập, nghiên cứu cũng như ứng dụng hệ thống tường lửa ISA Server 2004 Firewall, tôi sẽ trình bày cách thức triển khai hệ thống ISA Server (Standar và Enterprise) cho một tổ chức thực tế với mô hình Lab như sau:

T&C Descon là một công ty xây dựng có số lượng nhân viên trên 50 người, để cung cấp dịch vụ chia sẻ Internet, công ty sử dụng một đường ADSL và hệ thống ISA Server 2004 Firewall.

Địa chỉ modem ADSL là 1.1.1.2, hệ thống có hai lớp mạng chính là Internal bao gồm các máy tính của nhân viên có dãy địa chỉ IP riêng là 192.168.1.1 – 192.168.1.255/24 và DMZ dùng để đặt các máy chủ quan trọng như Exchange Server, Web Server sử dụng địa chỉ mạng 172.16.1.0/24. Máy chủ dùng để cài đặt ISA Server chạy Windows Server 2003 SP1 có 3 NIC (network interface) với địa chỉ IP như sau:

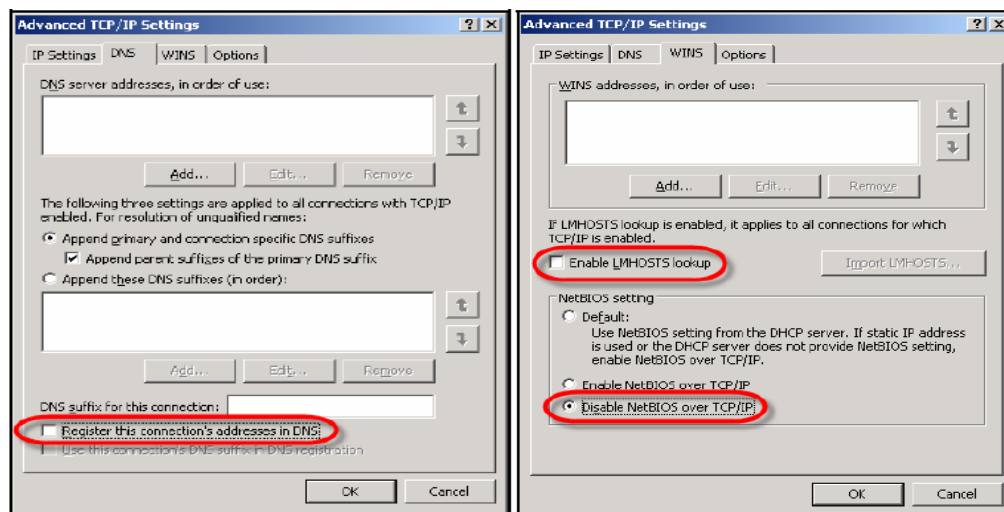
- Outside Interface : IP 1.1.1.1, Subnet Mask 255.255.255 và Default Gateway 1.1.1.2 (ADSL Modem).
- Inside Interface : IP 192.168.1.10, Subnet Mask 255.255.255.0 và DNS 192.168.1.11 (là DNS Server và Domain Controller của hệ thống)
- DMZ Interface : IP là 172.16.1.1, Subnet Mask 255.255.255.0

Mô Hình Hệ Thống



(part 2)

Nhằm bảo đảm an toàn cho hệ thống và firewall, trên giao tiếp mạng Outside hãy chọn **Disable Netbios Over TCP/IP**, bỏ chọn **Register this connection's address in DNS** và **Enable LMHOST lookup** như hình sau:

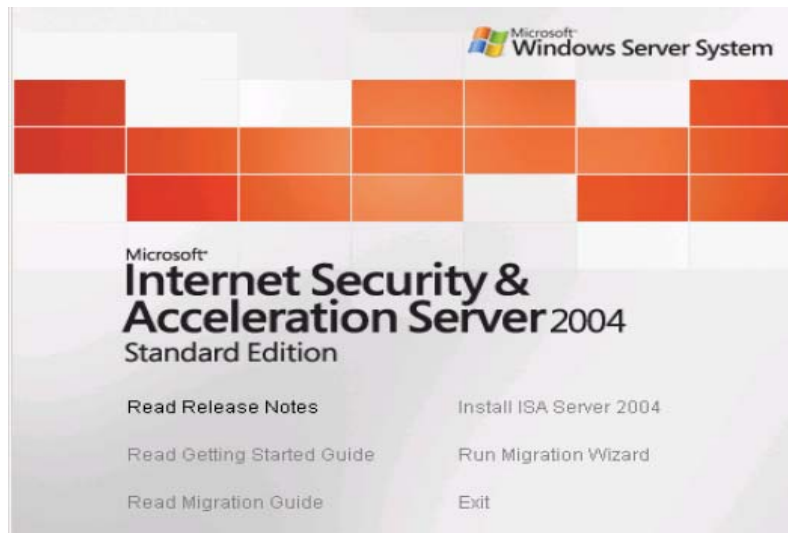


Lưu ý: Chức năng Disable NetBIOS over TCP/IP làm cho máy tính trở nên "vô hình" trên mạng, các phần mềm quét lỗi hệ thống như Retina, Nmap sẽ không tìm thấy tên của máy tính, hạn chế trường hợp dò tìm password của những tài khoản theo cơ chế brute force vì hệ thống thường tạo một số account mặc định sử dụng tên Netbios này. Do đó các máy chủ giao tiếp với Internet như firewall thường chọn chức năng này, tuy nhiên đối với các máy tính trên mạng nội bộ chúng ta không nên sử dụng vì sẽ ngăn ngừa các máy tính khác truy cập vào tài nguyên chia sẻ trên máy

của mình như Printer, Folder Share..Có một số ứng dụng bảo mật khi cài đặt sẽ *Disable NetBIOS over TCP/IP* một cách mặc định như PC Security, sẽ gây trở ngại cho quá trình hoạt động của hệ thống..

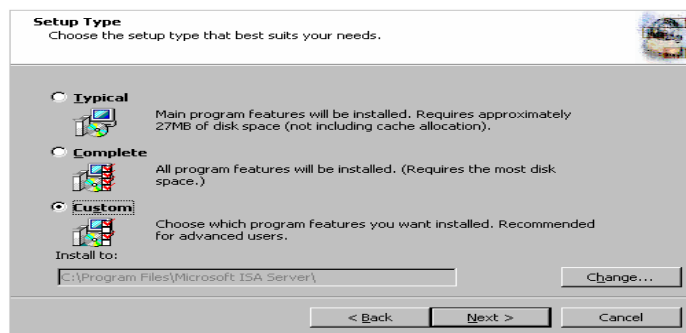
I - Tiến Hành Cài Đặt ISA Server 2004 :

Sau khi đã thiết lập đầy đủ các thông tin cần thiết hãy đưa đĩa CD ISA Server 2004 Standard vào máy dùng làm firewall, trên màn hình hiển thị hãy chọn **Install ISA Server 2004** để bắt đầu tiến trình cài đặt.

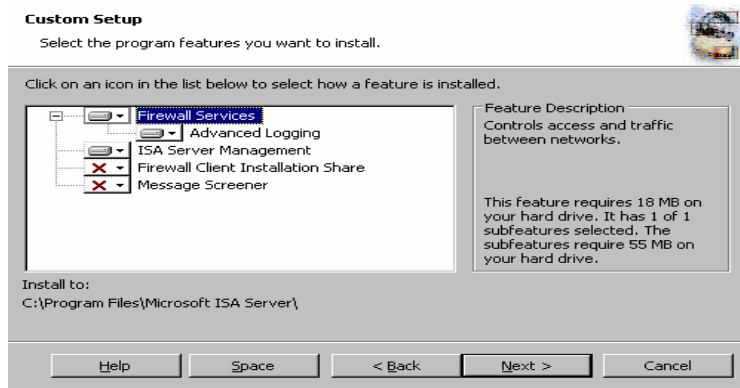


Nhấn Next trên màn hình **Welcome to the Installation Wizard for Microsoft ISA Server 2004**, chọn **I accept the terms in the license agreement** trên cửa sổ License Agreement và nhập vào các thông tin User Name / Organization, Product Serial Number trên những màn hình cài đặt tiếp theo. Chúng ta có thể chọn một trong 3 chế độ cài đặt sau:

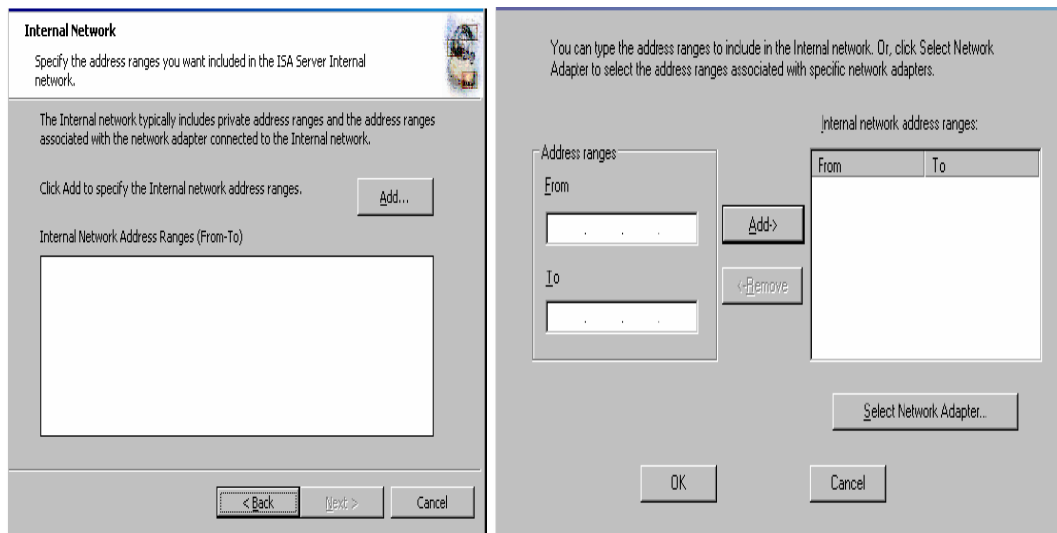
- Typical : ở chế độ này chỉ cài đặt một số dịch vụ tối thiểu, không có dịch vụ Cache.
- Complete : tất cả các dịch vụ sẽ được cài đặt như Firewall dùng để kiểm soát truy cập; Message Screener cho phép ngăn chặn spam mail và các file attachment (cần phải cài IIS 6.0 SMTP trước khi cài Message Screener; Firewall Client Installation Share.
- Custom : cho phép chọn những thành phần cần cài đặt của ISA Server 2004.



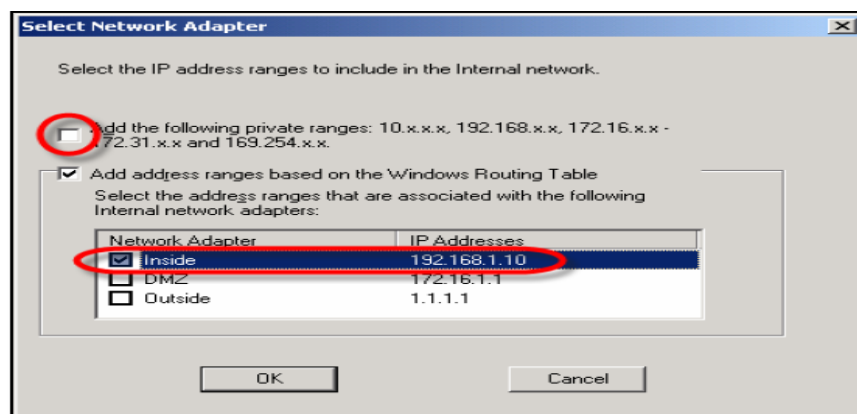
Ở đây chúng ta sẽ sử dụng chế độ cài đặt Custom và nhấn Next, mặc định chỉ có hai dịch vụ Firewall Services và ISA Server Management hãy chọn thêm Firewall Client Installation Share.



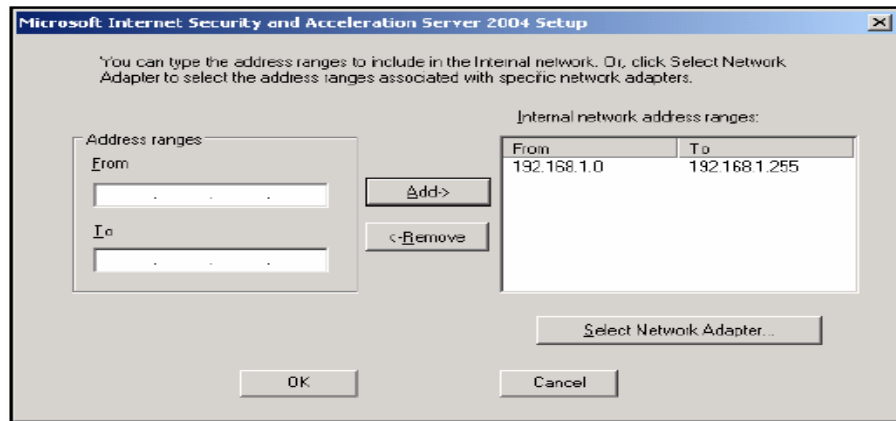
Tiếp theo tiến trình cài đặt sẽ yêu cầu bạn xác định giao tiếp mạng với hệ thống mạng nội bộ, trên cửa sổ Internal Network nhấn Add và Select Network Adapter để xác định card mạng giao tiếp với Internal Network.



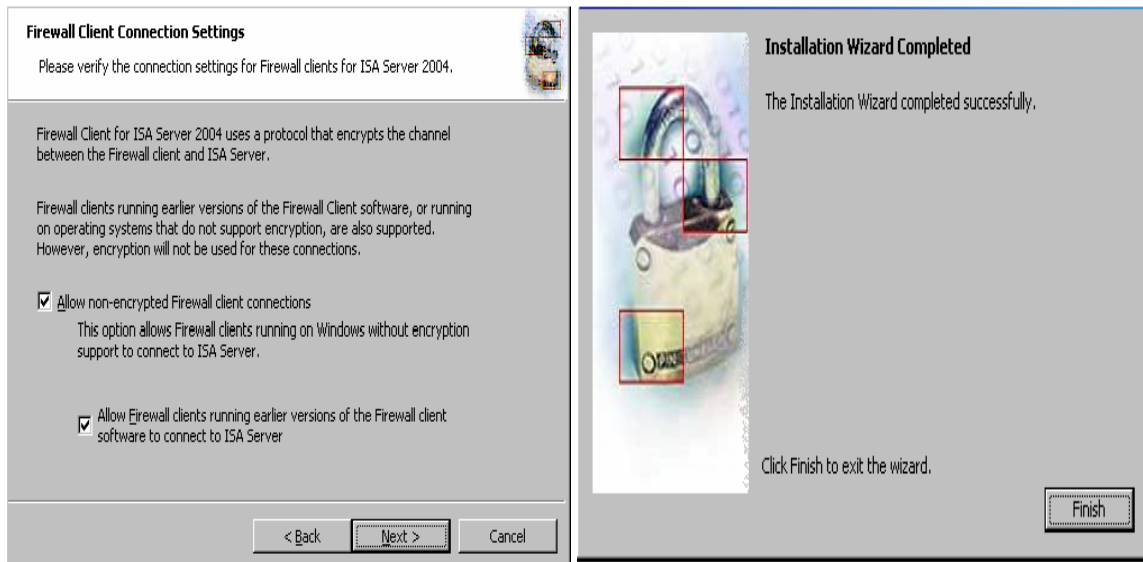
Đánh dấu vào Inside trong trang Select Network Adapter như hình sau:



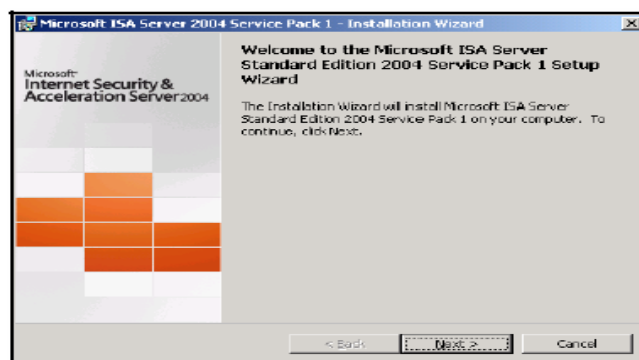
Tiếp theo chúng ta cần cung cấp dãy địa chỉ IP chứa các máy tính trên mạng nội bộ là **(From)192.168.1.0 – (To)192.168.1.255** hay tùy theo hệ thống của bạn và nhấn **Add**.
- Lưu ý dãy địa chỉ này phải chứa IP của giao tiếp mạng Inside.



Trên cửa sổ Firewall Client Connection Setting hãy đánh dấu chọn vào ô **Allow nonencrypted Firewall client connections** và **Allow Firewall clients running earlier versions of the Firewall client software to connect to ISA Server** rồi nhấn Next trong các bước tiếp theo để hoàn tất quá trình cài đặt.



Đối với phiên bản Standard chúng ta nên cài bản vá SP1 **ISA2004-KB891024-X86-ENU.msp** (có thể download từ website www.microsoft.com hay www.security365.org/downloads/software) cho ISA Server 2004 để bảo đảm quá trình hoạt động diễn ra suôn sẻ và ổn định.



II - Kết Nối ISA Server Với Internet Và Cấu Hình Các ISA Client:

Trên ISA Server 2004 Firewall có 3 dạng firewall policy là **system policy, access rule và publishing rule**.

- System policy thường ẩn và được dùng cho việc tương tác giữa firewall và các dịch vụ mạng khác như ICMP, RDP..system policy được xử lý trước khi access rule được áp dụng. Sau khi cài đặt các system policy mặc định cho phép ISA server sử dụng các dịch vụ hệ thống như DHCP, RDP, Ping..
- Access Rule : là những tập hợp các quy tắc áp dụng cho hệ thống như access rule cho phép truy cập internet hay check mail bằng POP3 client như Outlook Express.. Cần đặc biệt lưu ý đến thứ tự các Access Rule, vì luồng xử lý của firewall sẽ chấm dứt khi nó bắt gặp policy đầu tiên có những thiết lập tương ứng với giao thức truy cập. Để nắm rõ thêm cơ chế này chúng ta xem ví dụ sau:

Có 5 Access rule với thứ tự từ trên xuống dưới như sau:

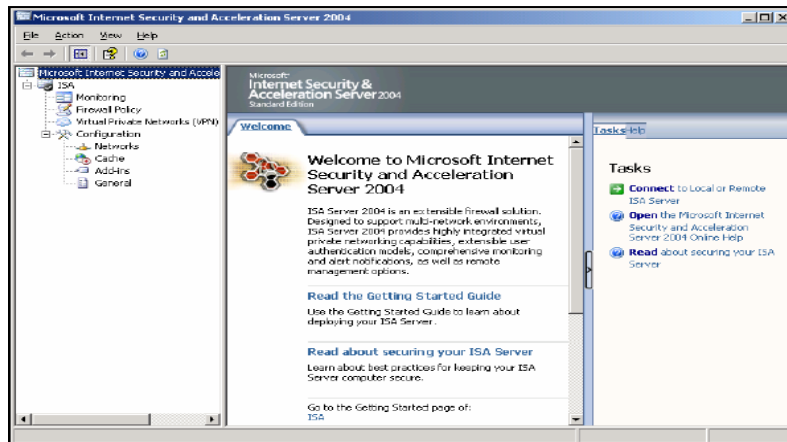
1. Deny HTTP (không cho phép sử dụng HTTP protocol)
2. Allow HTTP (cho dùng HTTP protocol)
3. Allow FTP (cho phép sử dụng FTP)
4. Deny FTP (không cho phép sử dụng FTP)
5. Deny All (default policy)

Trong trường hợp chúng ta cho rằng đối tượng sử dụng là như nhau, thì khi một user sử dụng giao thức HTTP để duyệt Web, anh ta sẽ bị từ chối truy cập vì access rule đầu tiên không cho phép sử dụng protocol này. Còn nếu user đó download tập tin thông qua FTP thì anh ta sẽ được phép vì access rule thứ 3 cho phép dùng FTP, và firewall sẽ bỏ qua các access rule còn lại.

- Publishing Rule: dùng publish các dịch vụ như Web, Mail server trên lớp mạng Internal hay DMZ cho phép các user trên Internet truy cập.

Khi quá trình cài đặt ISA Server 2004 hoàn tất chúng ta kết nối ISA Server với internet và tiếp theo là cấu hình các ISA client để có thể truy cập internet thông qua ISA Server Firewall. Mặc định ISA server chỉ có một access rule sau khi cài đặt là Deny All, từ chối mọi truy cập vào/ra thông qua ISA firewall vì vậy chúng ta cần tạo các quy tắc thích hợp với nhu cầu tổ chức hoặc áp dụng các Predefine Template cho ISA Server. Các bạn có thể cấu hình ISA Firewall Policy thông qua giao diện ISA Management Console trên chính ISA Server hoặc cài công cụ quản lý ISA Management Console trên một máy khác và kết nối đến ISA Server để thực hiện các thao tác quản trị từ xa của mình. Giao diện quản lý của ISA Server Management console có 3 phần chính:

- Khung bên trái dùng để duyệt các chức năng chính như Server name, Monitoring, Firewall Policy, Cache..
- Khung ở giữa hiển thị chi tiết các thành phần chính mà chúng ta chọn như System Policy, Access Rule..
- Khung bên phải còn được gọi là Tasks Pane chứa các tác vụ đặc biệt như Publishing Server, Enable VPN Server...

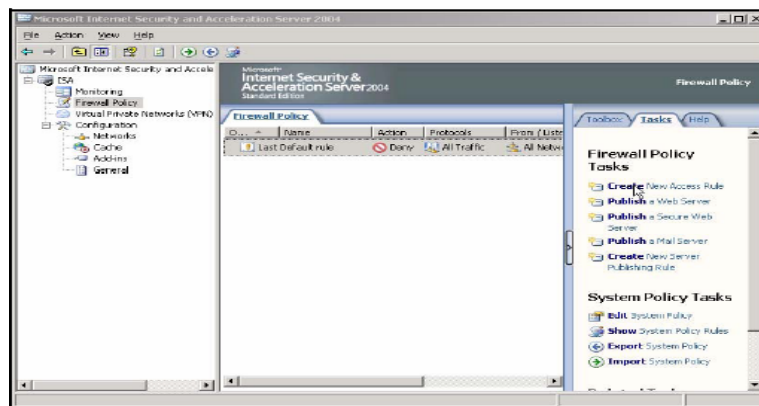


ISA Server Management console

1. Tạo Access Rule Trên ISA :

Mở giao diện quản lý ISA Management Server bằng cách chọn **Start - > All Programs - > Microsoft ISA Server - > ISA Server Management**.

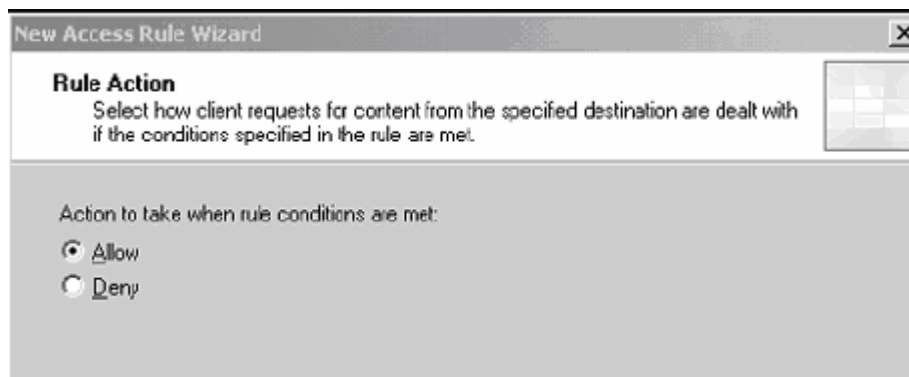
Click phải vào Firewall Policy và chọn **Create New Access Rule** hoặc chọn từ khung tác vụ (Task Pane) ở khung bên phải của màn hình quản lý như hình sau:



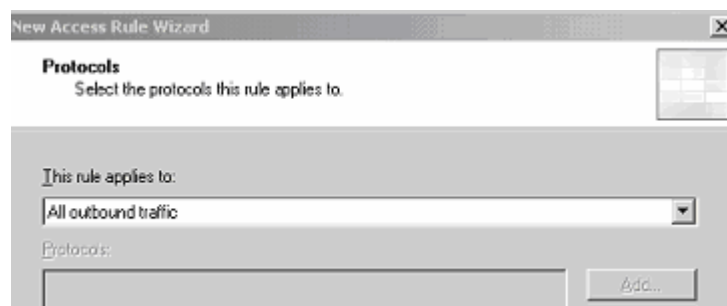
Đặt tên cho access rule cần tạo là **Permit Any traffic from internal network** hoặc tên phù hợp với hệ thống của bạn và chọn Next:



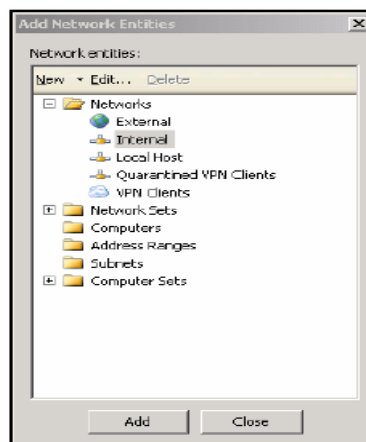
Trong phần Rule Action chúng ta chọn Allow, vì đây là access rule cho phép client sử dụng các giao thức và ứng dụng thông qua firewall.



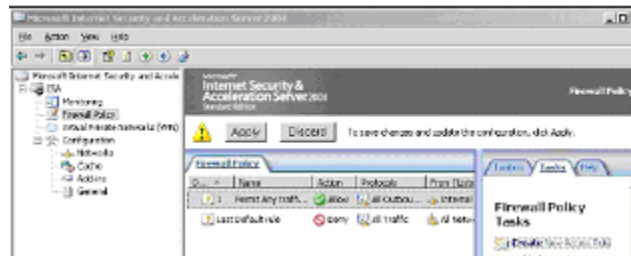
Xác định những giao thức mà User được sử dụng như HTTP hay FTP...trong cửa sổ Protocols, hãy chọn *All outbound traffic*, nếu muốn thay đổi các bạn chỉ cần bấm vào mũi tên và xác định những chức năng tương ứng như Selected Protocol để chọn một số giao thức nào đó hay *All inbound traffic* dành cho trường hợp cung cấp các kết nối từ bên ngoài vào.



Hệ thống cần biết đối tượng sử dụng các giao thức trong access rule, ở trường hợp này các client là những người sử dụng trong hệ thống mạng nội bộ cho nên chúng ta chọn **Add** trên **Access Rule Source** và chọn **Internal**. Đối với User thì chúng ta chọn **All User** (trong trường hợp cần thiết các bạn có thể xác định những Group hay User thích hợp của hệ thống như Group Domain User, Administrator..., khi Firewall không thuộc Domain thì hãy sử dụng local account của Firewall trong Local Users And Groups.)



Nhấn Apply để hiệu lực firewall policy mới tạo ra, lúc này chúng ta đã có 2 Access Rule là Default Rule (có chức năng Deny All, lưu ý default rule không thể xóa được) và *Permit Any Traffic from internal network* cho phép các user trên mạng nội bộ được phép sử dụng tất cả các giao thức trên Internet.

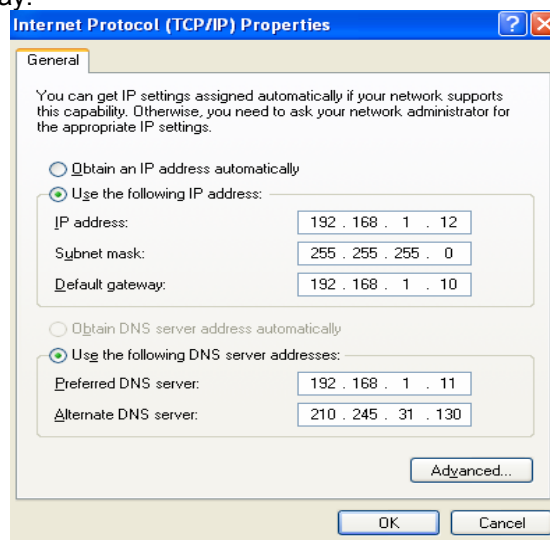


2. Cấu hình ISA Client:

Để sử dụng ISA Server thì các client trên mạng phải cấu hình một trong ba loại sau SecureNAT, Firewall Client, Web Proxy Client hoặc cả 3 dạng trên:

i. SecureNAT Client :

Đây là phương pháp đơn giản nhất, các máy tính chỉ cần cấu hình Default Gateway là địa chỉ card mạng trong của ISA Server là được (trong trường hợp này là 192.168.1.10), hoặc chúng ta có thể cấp phát thông qua DHCP server với option 006 dành cho Router. Điểm thuận lợi của phương pháp này là Client không cần cài đặt gì thêm, và có thể sử dụng các hệ điều hành không thuộc Microsoft như Linux, Unix mà vẫn sử dụng được các giao thức và ứng dụng trên internet thông qua ISA. Tuy nhiên có một bất lợi là các SecureNAT client không gửi được những thông tin chứng thực gồm Username & Password cho Firewall được, vì vậy nếu như các bạn triển khai dịch vụ kiểm soát truy cập theo domain user đòi hỏi phải có username&password thì các SecureNAT Client không ứng dụng được. Ngoài ra chúng ta không thể ghi nhật ký quá trình truy cập đối với dạng client này.



Cấu hình SecureNAT client trên Client1

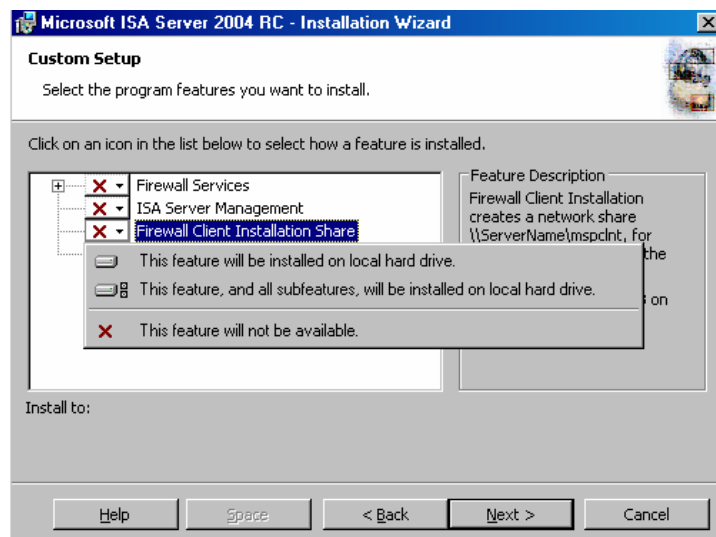
ii. Firewall Client :

Vậy nếu chúng ta muốn có một cơ chế kiểm soát chặt chẽ hơn, ví dụ User phải log-in domain mới truy cập được Internet thì phải làm như thế nào? Giải pháp đưa ra là chúng ta sẽ cài đặt Firewall Client cho các máy tính này. Thông thường khi cài đặt ISA Server các bạn sẽ cài dịch vụ Firewall Client Installation Share, sau đó trên ISA server mở system policy cho phép truy cập tài

nguyên chia sẻ và máy tính Client chỉ cần kết nối đến ISA Server theo địa chỉ IP nội bộ với tài khoản hợp lệ để tiến hành chạy tập tin cài đặt Firewall Client .

Nếu không muốn cài đặt Firewall Client Installation Share thì chúng ta có thể chọn cài dịch vụ này trên bất kỳ máy tính nào như file server hoặc domain controller như sau:

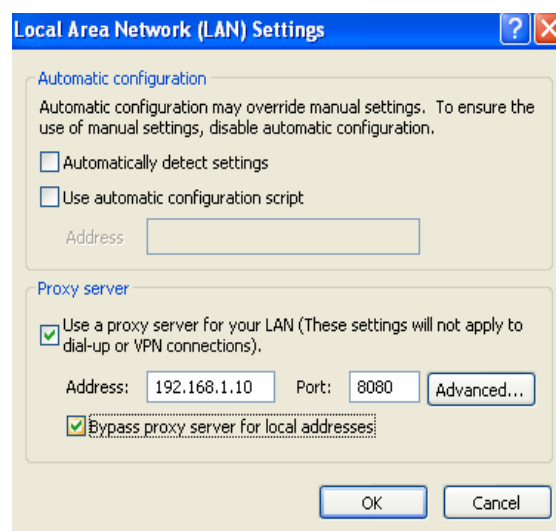
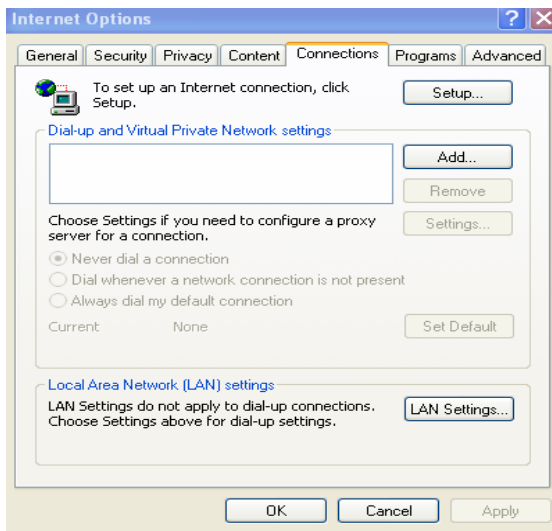
- a. Đưa ISA Server 2004 CD-ROM vào domain controller, chọn **Install ISA Server 2004**.
- b. Trên màn hình **Welcome to the Installation Wizard for Microsoft ISA Server 2004** nhấn **Next**.
- c. Tiếp theo chọn **I accept the terms in the license agreement**, nhấn **Next**.
- d. Nhập vào **User name**, **Organization** và **Product Serial Number** trên cửa sổ Customer Information. Chọn **Next**.
- e. Trong **Setup Type**, xác định tùy chọn **Custom** và enable **This feature, and all subfeatures, will be installed on the local hard drive** trong mục **Firewall Client Installation Share** như hình dưới đây và nhấn Next trong các bước tiếp theo để hoàn tất:



Sau đó trên các máy tính client tiến hành cài đặt Firewall Client bằng cách mở Start - > Run và chạy lệnh `\\192.168.1.10\mspcint\setup`

Trong trường hợp hệ thống có nhiều máy trạm, việc cài đặt trên từng máy gặp nhiều khó khăn thì giải pháp triển khai chương trình một cách tự động bằng SMS Server 2003 hoặc Assign thông qua Group Policy là hiệu quả nhất (các bạn có thể tham khảo phương pháp cài đặt tự động thông qua Group Policy trên website www.security365.org do Rõng Đông Dương thực hiện.) Với firewall client các bạn có thể tận dụng được những khả năng mạnh mẽ nhất của ISA Server như chứng thực người dùng dựa trên Domain User & Group, cho phép ghi nhật ký những lần truy cập..Tuy nhiên điểm bất lợi chính của trường hợp này là các máy tính muốn cài Firewall Client phải sử dụng hệ điều hành của Microsoft .

iii. Web Proxy Client: như chúng ta biết ngoài chức năng bảo mật thì ISA Server 2004 Firewall còn có chức năng Cache dùng để lưu trữ các trang Web thường được truy cập trên RAM hoặc trên đĩa cứng nhằm tiết kiệm băng thông. Tuy nhiên, Web Proxy Client chỉ sử dụng được các giao thức HTTP / HTTPS, FTP (upload/download), điều này có nghĩa là User sẽ không lấy mail với Outlook hay sử dụng các ứng dụng khác. Để sử dụng Web Proxy, các máy tính Client phải cấu hình trong trình duyệt Web bằng cách mở Internet Explore chọn Tools - > Internet Options chọn tab Connections - > LAN Settings và nhập vào địa chỉ của Proxy server :



Như vậy cách nhanh chóng nhất cho phép các máy tính trong tổ chức có thể truy cập Internet qua ISA Server là cấu hình SecureNAT client dựa trên hệ thống cấp phát địa chỉ IP động hoặc cấu hình IP tĩnh và trở default gateway là địa chỉ mạng nội bộ của ISA Server. Ngoài ra để quá trình phân giải địa chỉ IP diễn ra suôn sẻ thì các client cần cấu hình địa chỉ DNS server nội bộ và cả ISP DNS Server như 210.245.31.10 hay 203.162.4.191

III. Thiết Lập Các Private Policy:

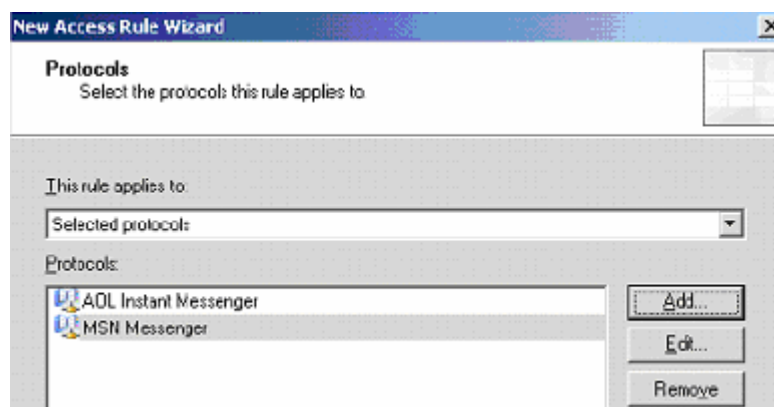
Mặc dù hệ thống đã kết nối được internet, nhưng một số công ty có những yêu cầu riêng về chính sách hệ thống như không cho phép chat bằng AOL hay MSN Messenger, cho phép download file thông qua FTP (upload và download) . Bên cạnh đó, để phục vụ nhu cầu nghiên cứu và duyệt Web giao thức HTTP được cho phép sử dụng nhưng cấm không cho download những tập tin có thể thực thi trên hệ thống Windows qua HTTP để ngăn ngừa sự lây nhiễm virus, trojan. Để thực hiện điều này các bạn hiệu chỉnh lại firewall policy của mình.

A. Tạo Access Rule Không Cho Phép Sử Dụng Aol Và Msn Messenger:

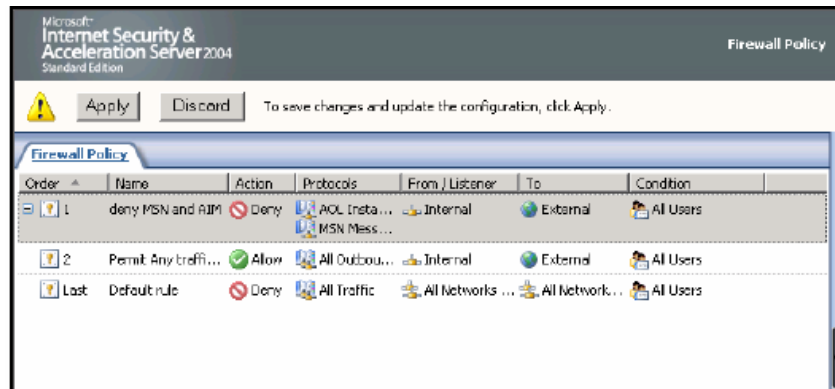
Click chuột phải vào **Firewall Policy** -> chọn **Create new Access Rule** -> đặt tên là **deny MSN and AIM** -> chọn **Next**.

Ở cửa sổ Rule Action hãy chọn **Deny** và nhấn **Next**.

Trong phần **This rule applies to** chọn **Selected Protocols**. Nhấn nút **Add**. Sau đó mở Protocols của **Instant Messaging** và double click **AOL Instant Messenger** và **MSN Messenger**. Nhấn **Close**.



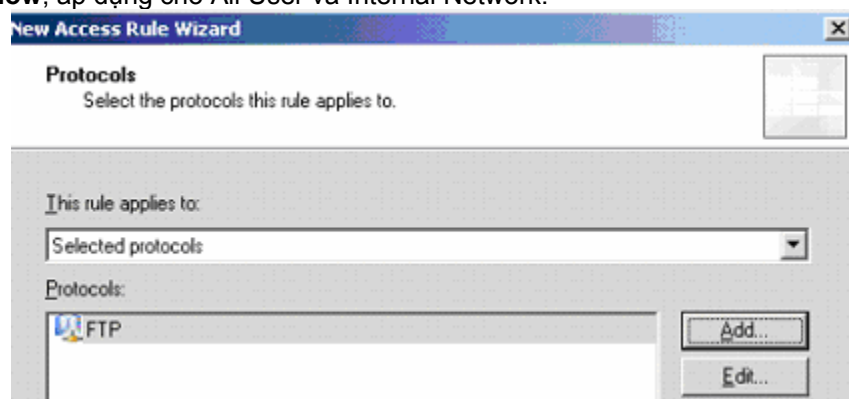
Tiếp theo chúng ta chọn Internal và External trong phần Network, áp dụng cho All user và Apply để áp dụng policy này cho hệ thống.



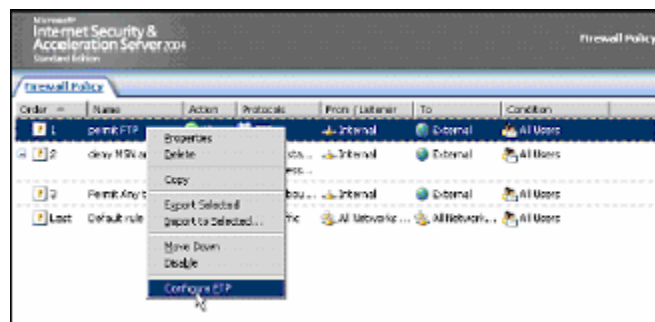
B. Tạo Access Rule Cho Phép Client Sử Dụng Ftp Download Và Upload

Trong trường hợp bạn muốn các client sử dụng FTP để download và cả upload hãy tiến hành như sau:

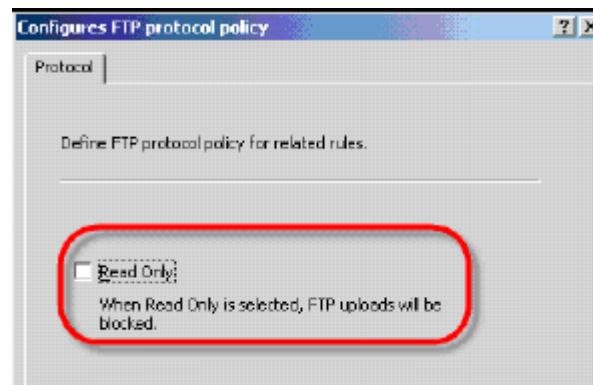
Tạo access rule mới thông qua **Create a New Access Rule** đặt tên là **permit FTP** với Rule Action là **Allow**, áp dụng cho All User và Internal Network.



Sau khi click vào nút Apply thì User trên hệ thống mạng nội bộ đã có thể download thông qua FTP bằng các chương trình FTP Client như FileZilla, tuy nhiên để họ có thể upload lên các FTP server thì chúng ta cần bổ thiết lập Read Only cho FTP access rule bằng cách click phải chuột vào Access Rule **permit FTP** và chọn **Configure FTP**

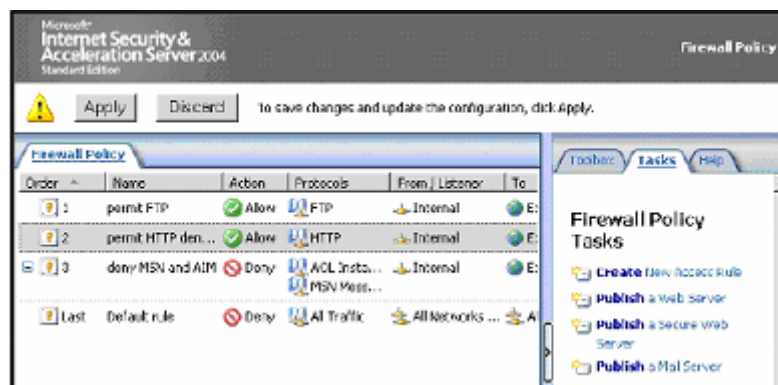


Trên cửa sổ hiện thị Configure FTP protocol policy bỏ chọn Read Only sẽ cho phép upload lên Ftp server.

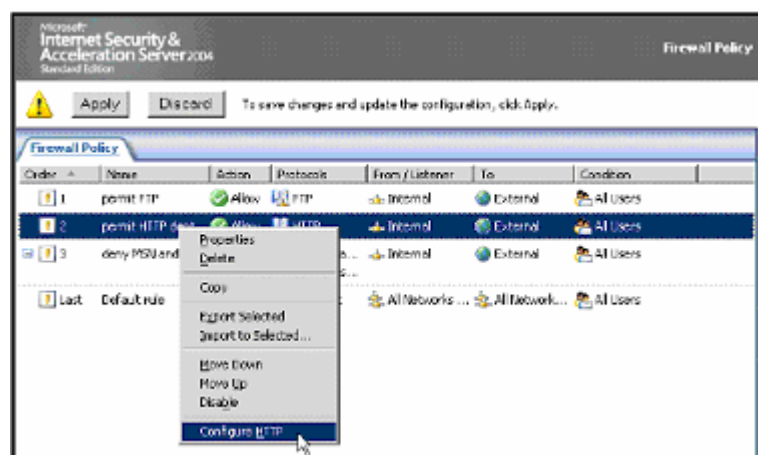


c. Tạo Access Rule Cho Phép Sử Dụng HTTP Nhưng Không Cho Phép Download Những File Có Khả Năng Thực Thi Trên Hệ Thống Windows.

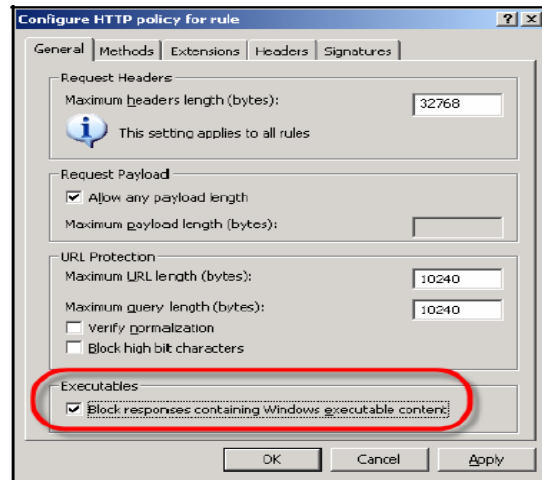
Tạo access rule mới tên là **permit HTTP deny executables** cho phép các user trên lớp mạng Internal sử dụng HTTP protocol



Click phải chuột vào **permit HTTP deny executables** và chọn configure HTTP



Đánh dấu chọn vào ô **Block responses containing Windows executable content** như hình sau:

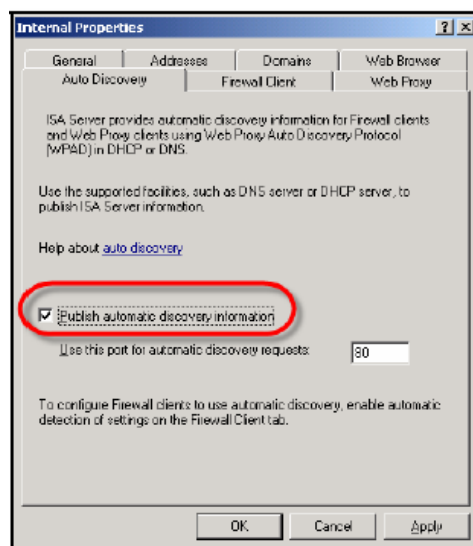


IV. Sử Dụng WPAD Hỗ Trợ ISA Client Tự Động Dò Tìm Firewall Và Web Proxy

Khi hệ thống sử dụng DHCP cấp phát địa chỉ IP động, chúng ta cần phải hỗ trợ các client tự động dò tìm Web Proxy Server và Firewall thông qua CNAME WPAD record trên DNS Server hoặc cấu hình option Predefine là wpad trên DHCP server (tham khảo file demo ở www.security365.org/downloads/demo/ISA2004).

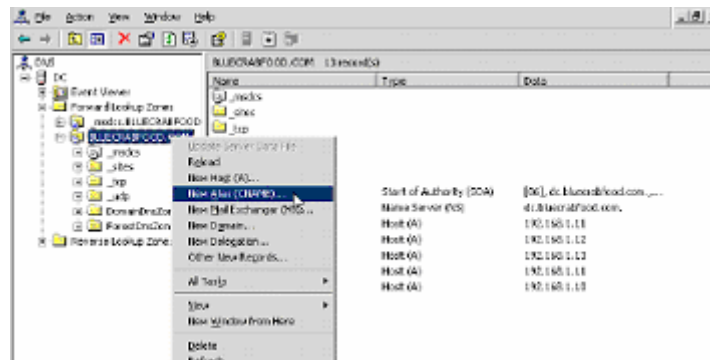
Lưu ý: Việc cấu hình WPAD trên DHCP chỉ sử dụng được nếu DHCP Server là dịch vụ của hệ điều hành Windows, còn khi các bạn sử dụng DHCP Server của các hãng khác thì chúng ta phải sử dụng DNS để làm điều này.

- i. Trước tiên chúng ta cần phải bật chức năng hỗ trợ Auto Discovery trên ISA Server. Hãy mở ISA Management Console, trong phần Network hãy double click vào Internal Network chọn tab AutoDiscovery và check vào mục **Publish automatic discovery information**, trong ô **Use this port for automatic discovery request** hãy nhập vào số 80.

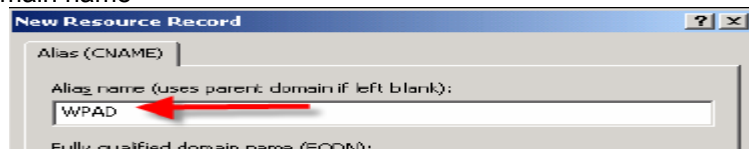


ii. Tạo CNAME record trong DNS server đặt tên là WPAD

Mở cửa sổ DNS Management Console, nhấn chuột phải lên Domain Zone và chọn New Alias (CNAME)



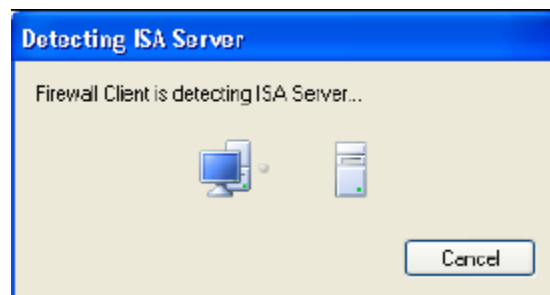
Nhập vào WPAD trong phần Alias name và tên đầy đủ ví dụ WPAD.SECURITY365.ORG trong ô Full qualified domain name



Nhấn OK để hoàn tất. Hãy sử dụng bất kỳ Firewall Client hay Web Proxy Client nào kiểm tra lại. Chọn Automatically detect ISA Server trong firewall client và bỏ chọn Use proxy server thay vào đó là Automatically detect settings trong trình duyệt Web để tự động dò tìm Web Proxy.

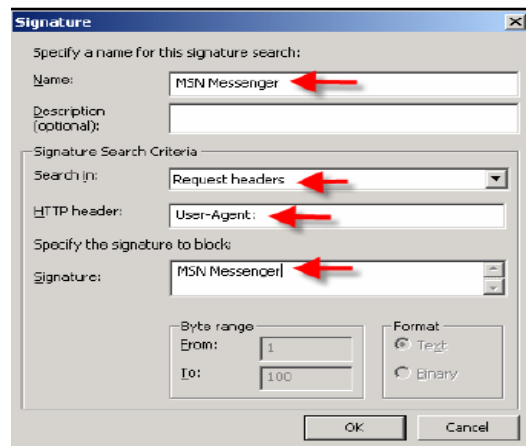


Chọn Detect Now, sau khoảng thời gian ngắn tên ISA Server trên hệ thống của bạn sẽ xuất hiện



Như vậy, chúng ta đã cài đặt và cấu hình ISA Server để hỗ trợ quá trình truy cập Internet, download và upload tài liệu thông qua FTP, hỗ trợ tự động dò tìm Firewall và Web Proxy đối với Client với record WPAD trong DNS Server. Tuy nhiên, bạn nhận thấy rằng một số client vẫn chat được bằng MSN Messenger hay sử dụng các chương trình P2P để tìm kiếm tài liệu. Đó là do những ứng dụng này có thể sử dụng HTTP, port 80 để truyền thông qua web proxy server. Các bạn có thể ngăn chặn điều này bằng cách hiệu chỉnh permit HTTP policy như sau:

Click chuột phải permit HTTP Access Rule và chọn Configure HTTP. Trong tab Signature nhập vào các tham số như hình dưới đây và nhấn OK, sau đó chọn Apply để áp dụng cho hệ thống:



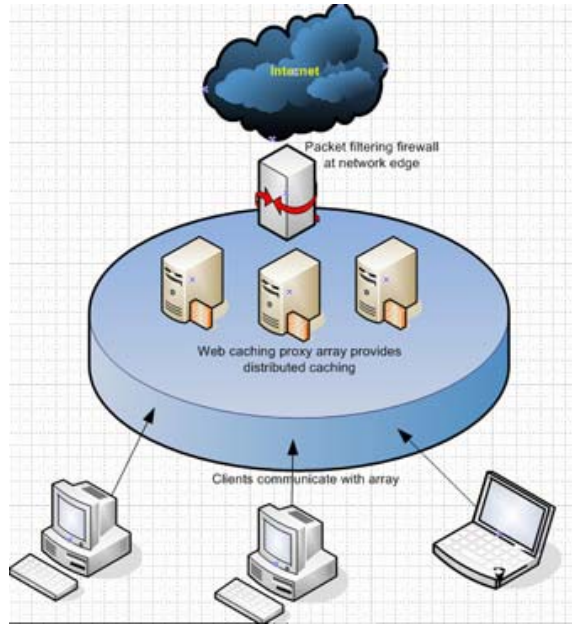
V - Tiết Kiệm Băng Thông Với Tính Năng Cache Và Content Download Job:

Có một đặc tính rất hữu ích của ISA Server tuy nhiên bị disable một cách mặc định đó chính là web caching đối với http và ftp request. Với ISA chúng ta có thể thực hiện cả hai cơ chế caching đó là:

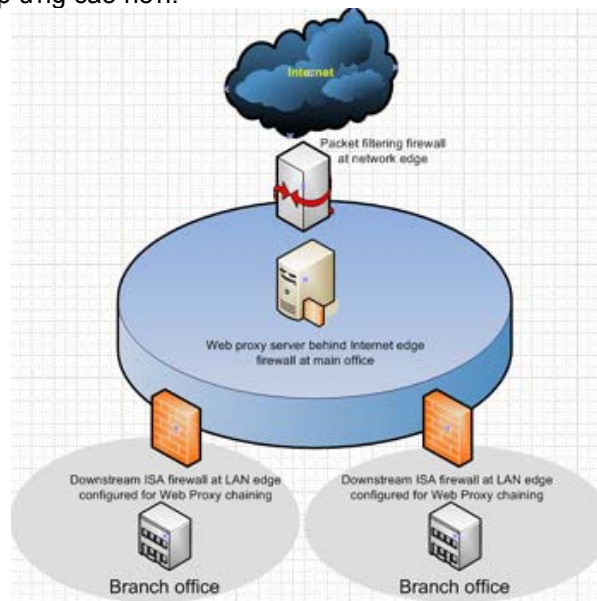
- Forward Caching : với cơ chế này nội dung các trang web thường xuyên được truy cập như www.pcworld.com.vn sẽ được tải về trước và lưu trữ trong phần Cache của Isa server, vì vậy khi người dùng mở lại những trang web này sẽ được trả nội dung trên Cache thay vì phải kết nối trực tiếp với web server trên Internet.
- Reverse Caching : ngược lại với forward caching, khi doanh nghiệp hay tổ chức có những web server cho phép người dùng bên ngoài truy cập reserver caching tiết kiệm băng thông bằng cách lưu trữ nội dung trang web trên các proxy server (đặt tại các đường biên mạng - network edge) để đáp ứng cho internet user, giảm tải cho web server. Vì vậy trên một số tài liệu reverse cache còn được gọi là gateway cache hay surrogate cache.

Về mặt tổ chức thì chúng ta có thể xây dựng hệ thống cache trên ISA theo các mô hình khác nhau tùy thuộc vào số lượng user và kiến trúc mạng của mỗi doanh nghiệp:

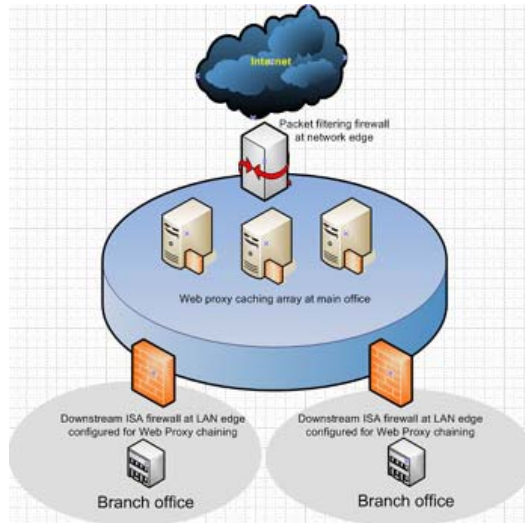
- Distributed Caching : các ISA server sẽ được phân bố đều trên mạng, nâng cao khả năng đáp ứng cho người dùng.



- Hierarchical caching: khác với mô hình trên, trong trường hợp này ISA server sẽ được phân bố theo từng cấp, các yêu cầu sẽ được xử lý bởi những ISA server nội bộ trước, vì vậy thời gian đáp ứng cao hơn.



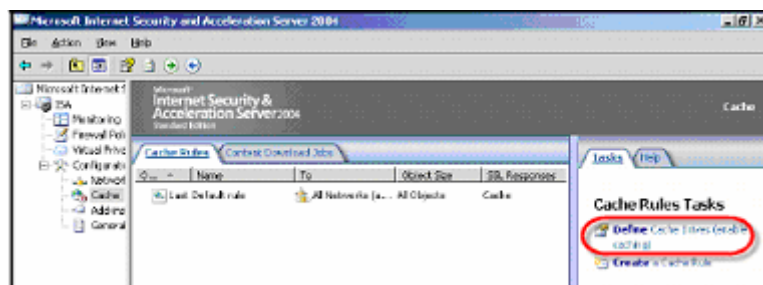
- Hybrid caching : là sự kết hợp cả hai mô hình trên.



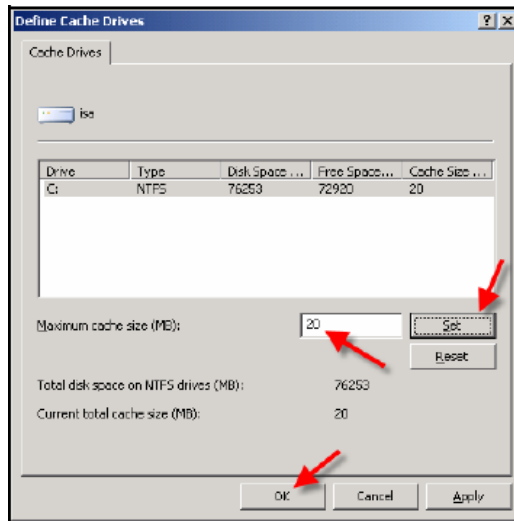
Vậy, khi chức năng Web Cache được bật, những trang web thường xuyên truy cập sẽ tự động tải về có thể được lưu giữ trên RAM hay đĩa cứng của ISA Server (cache), và những User khi truy cập vào lại trang web này sẽ được trả về nội dung từ cache chứ không phải download trên Internet. Tuy nhiên một số trang web tìm kiếm thì không nên lưu trữ nội dung trên cache vì sẽ cho ra những kết quả tìm kiếm không được cập nhật..., vì vậy khi thiết lập Web Caching các bạn nên đặt Caching Rule để không lưu giữ những trang Web như www.google.com. Ngoài ra một số trang web thường xuyên được người dùng truy cập để đọc tin, tham khảo giá cả thị trường, tin tức về bảo mật... chúng ta có thể lập lịch để dịch vụ Web Proxy Server tải về trước ngoài giờ làm việc thông qua chức năng **Content Download Job**.

i. Enable Web Caching:

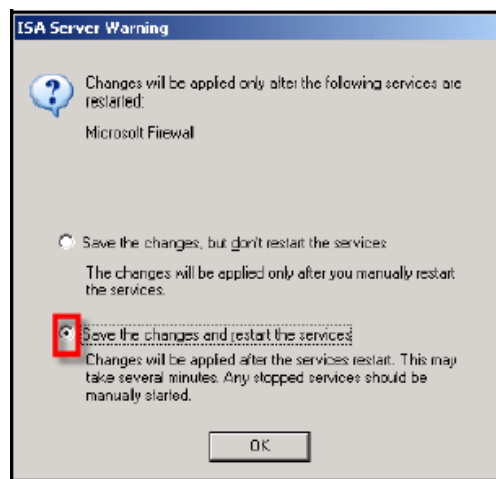
Mở ISA Management Console, chọn mục Cache trong phần Configuration và click chuột vào **Define Cache Drivers (enable caching)**:



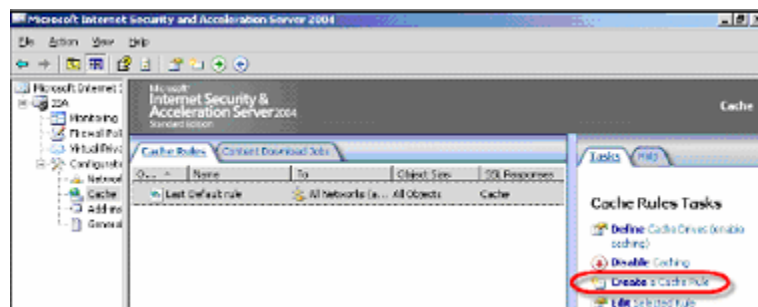
Xác định phân chia NTFS dành cho việc lưu trữ nội dung các trang Web (cache size), ví dụ 20 MB, nhấn Set để thiết lập và click OK:



Sau khi click Apply để áp dụng chức năng Web Cache sẽ có một hộp thoại thông báo Restart lại Firewall Services hay chỉ lưu lại và không Restart, hãy chọn **Save the changes and restart the services** và click OK.



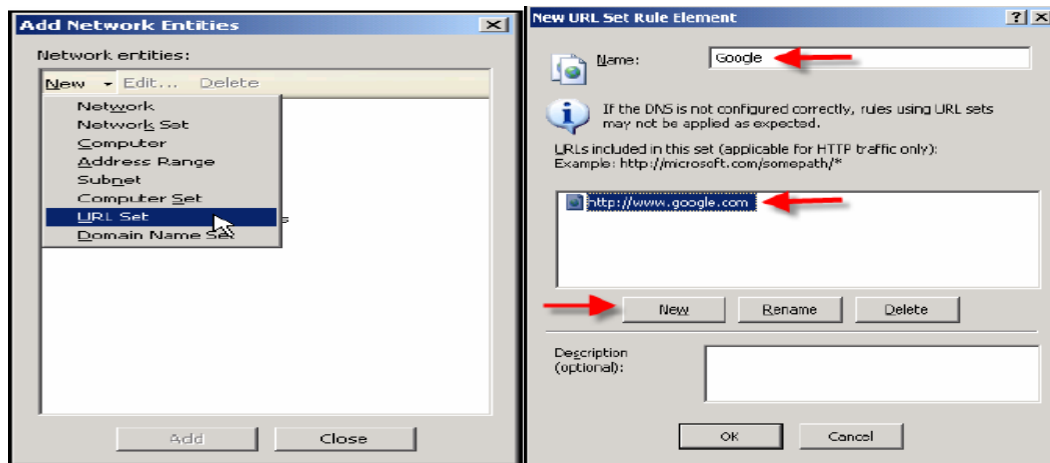
ii. Tạo Cache Rule không lưu trữ nội dung các trang Web từ www.google.com:
Trên khung Task Pane chọn Create a Cache Rule:



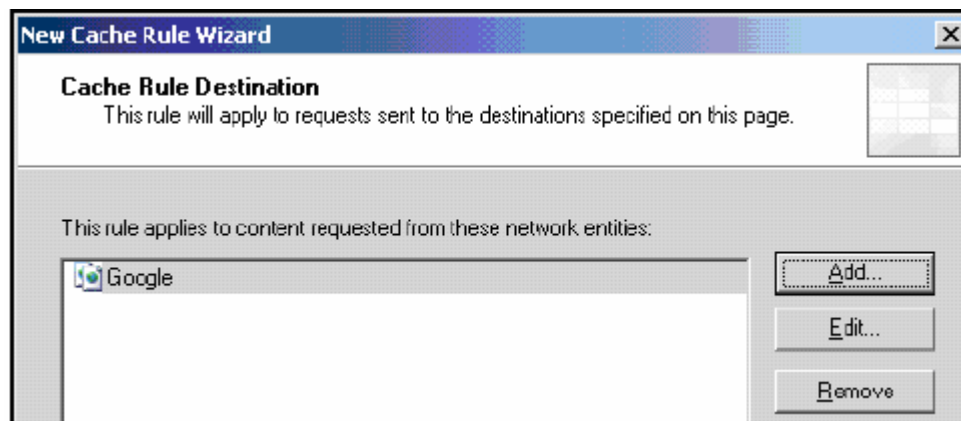
Đặt tên là No Google Cache trong khung New Cache Rule Wizard:



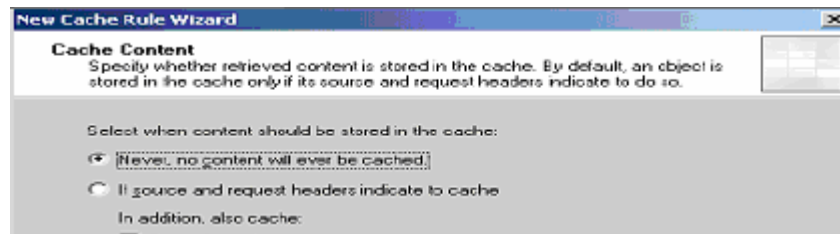
Trong cache rule destination, chúng ta cần xác định trang web không cần lưu trữ bằng cách chọn Add, click New và trên menu hiển thị hãy chọn URL Set, nhập tên là Google sau đó chọn New và đưa vào địa chỉ <http://www.google.com> như hình dưới đây:



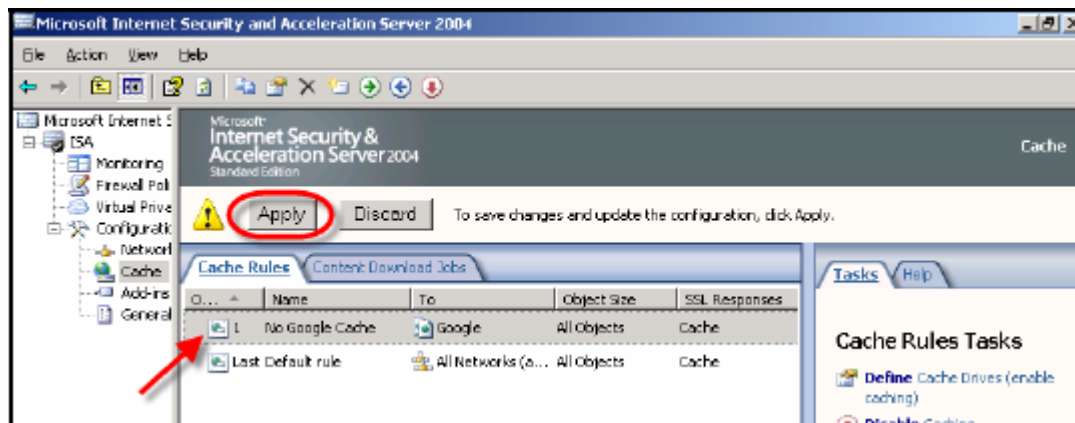
Nhấn OK để quay trở lại cửa sổ Add New Network Entities, mở mục URL Sets và chọn Google:



Next để tiếp tục, trên màn hình tiếp theo hãy chấp nhận giá trị mặc định, sau đó nhấn Next và chọn **Never, no content will ever be cached**. Cuối cùng nhấn Finish để kết thúc quá trình thiết lập.



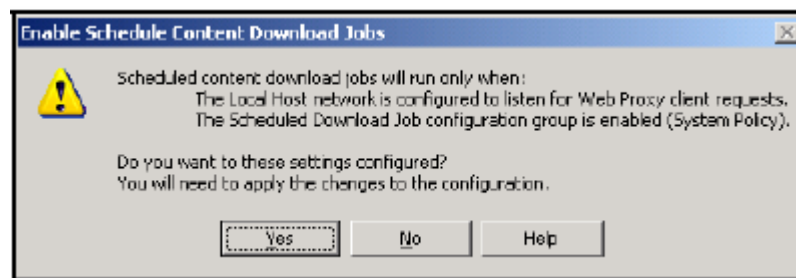
Như vậy ISA Server 2004 của chúng ta đã được bật chức năng Web Caching để tiết kiệm băng thông, đồng thời ngăn ngừa việc lưu trữ nội dung của trang web tìm kiếm như Google để hạn chế các thông tin không cần thiết. Lúc này chúng ta có thể kiểm tra lại policy mới được tạo ra trên giao diện quản lý và nhấn Apply để áp dụng.



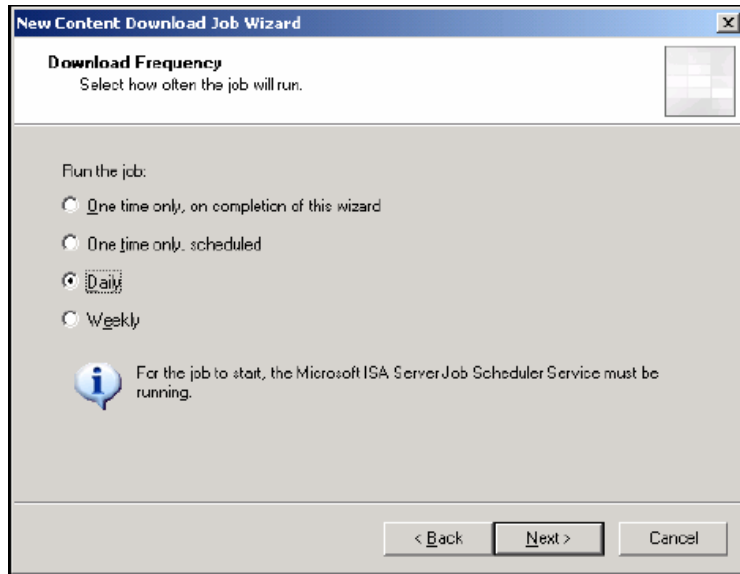
iii. Cấu hình Content Download Job:

Giả sử User trên hệ thống thường truy cập vào trang web www.security365.org để xem các thông tin mới về virus/trojan hay các lỗi bảo mật, do đó chúng ta cấu hình ISA server tự động download trang web này về trước vào ngày giờ xác định nào đó trong tuần để nâng cao hiệu quả hoạt động.

Click **Content Download Job**, trên khung **Tasks Pane**, chọn **Schedule a Content Download Job**. Chúng ta sẽ thấy thông báo như dưới đây



Chọn Yes và sau đó đặt tên cho Content Download Job là SecureSolution, nhấn Next để tiếp tục xác định ngày giờ là chạy tiến trình này một ngày một lần (Daily), một tuần một lần (Weekly)...

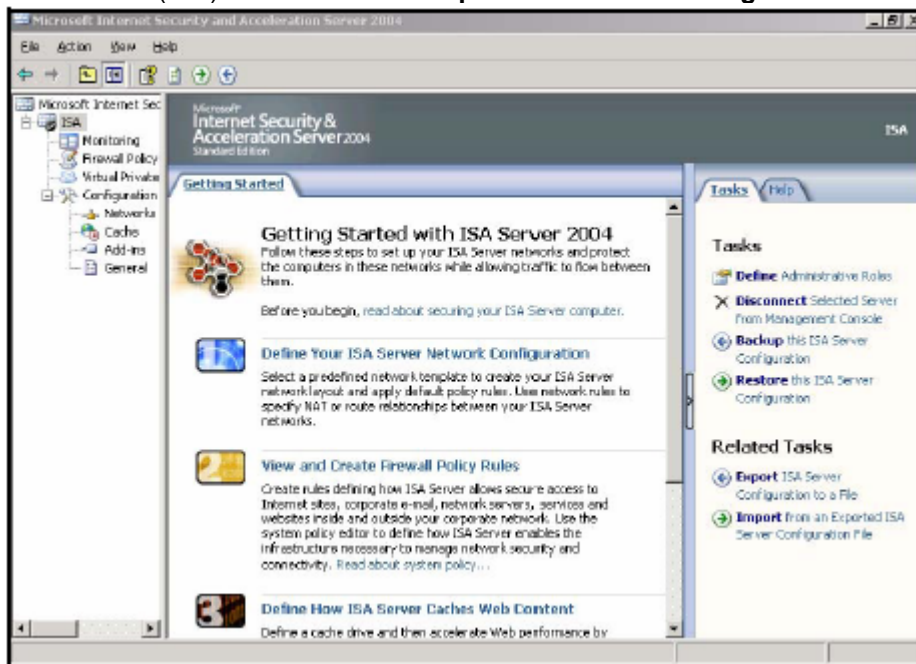


Nhấn Next và nhập vào địa chỉ trang web cần tải về trong ô Download content from this URL, trong trường hợp này chúng ta nhập vào www.security365.org Hãy chọn giá trị mặc định trong các bước tiếp theo để hoàn tất.

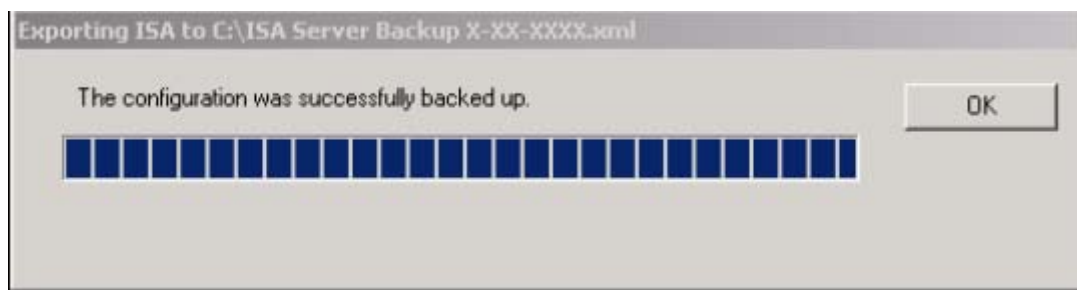
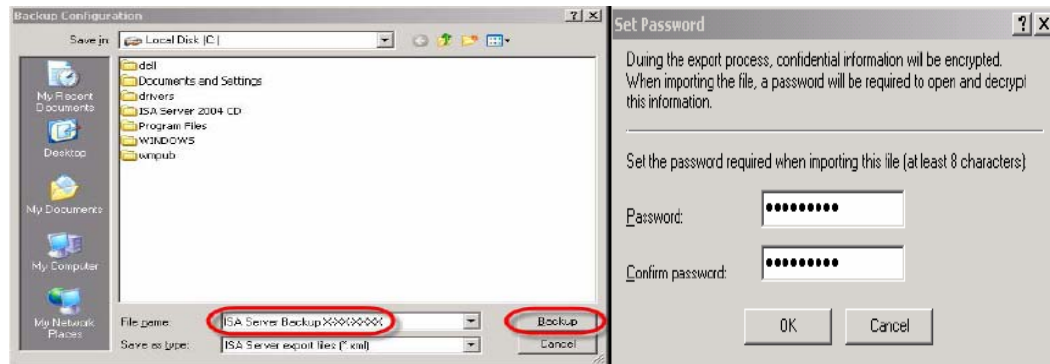
VI – Backup Và Restore Các Thông Tin Cấu Hình Của ISA Server 2004 Firewall:

Đối với các hệ thống lớn với nhiều phòng ban và nhân viên, trong mỗi bộ phận lại yêu cầu những chính sách truy cập riêng làm cho số lượng policy rất nhiều và khó quản lí. Vì vậy để bảo đảm hệ thống luôn hoạt động ổn định chúng ta cần phải tiến hành sao lưu (backup) các policy một cách đầy đủ để có thể phục hồi (restore) khi có sự cố xảy ra. Chúng ta có thể backup toàn bộ ISA Server hay chỉ một số các firewall policy nào đó.

Thao tác sau đây sẽ tiến hành backup toàn bộ ISA Server, mở ISA Management Console, chọn server name (ISA) và click vào **Backup the ISA Server Configuration** trên khung Tasks Pane

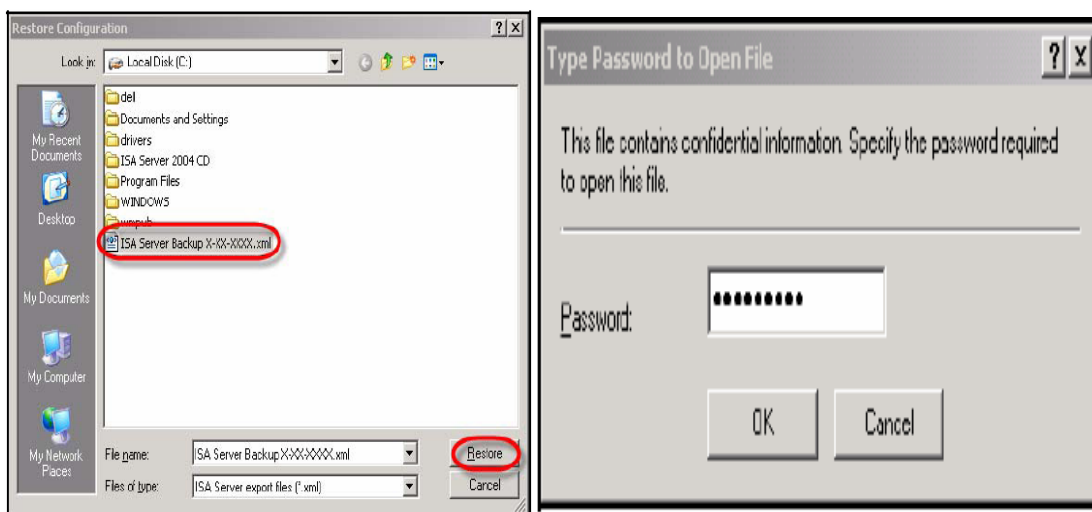


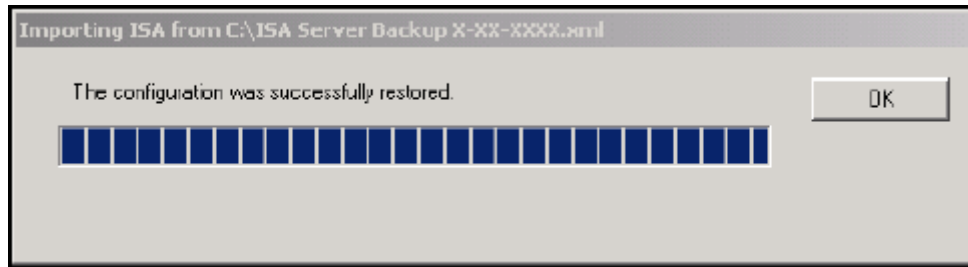
Tiếp theo chúng ta đặt tên của tập tin backup (nên đặt theo dạng X-XX-XXXX là ngày-tháng-năm tiến hành backup để dễ dàng phân biệt khi tiến hành phục hồi), chọn nơi lưu trữ và nhấn nút Backup một hộp thoại yêu cầu đặt password cho tập tin backup hiện ra, hãy nhập password vào và chọn OK tiến trình backup sẽ diễn ra như hình sau:



Hình ảnh hiển thị tiến trình backup hoàn tất

Để thử nghiệm, các bạn có thể xóa một vài hay toàn bộ firewall policy trên hệ thống của mình, sau đó chọn **Restore this ISA Server Configuration** trên khung Tasks Pane, xác định tập tin backup chọn Restore và nhập vào password được thiết lập cho tập tin này. Sau khi tiến trình phục hồi hoàn tất chúng ta có thể kiểm tra lại các policy trước đây của hệ thống đã được phục hồi đầy đủ.





Hình hiển thị tiến trình phục hồi thành công

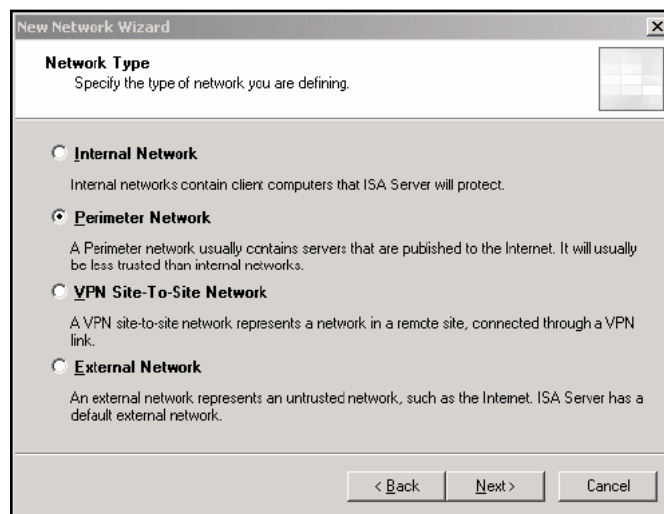
Qua thao tác backup và restore trên chúng ta thấy việc sao lưu và phục hồi các firewall policy hay toàn bộ hệ thống được tiến hành khá đơn giản và dễ dàng. Trong trường hợp chỉ backup một firewall policy nào đó chúng ta cũng tiến hành tương tự với chức năng **Export Firewall Policy** trên khung Task Pane.

VII - Thiết Lập Vùng DMZ Và Publish Server Thông Qua ISA

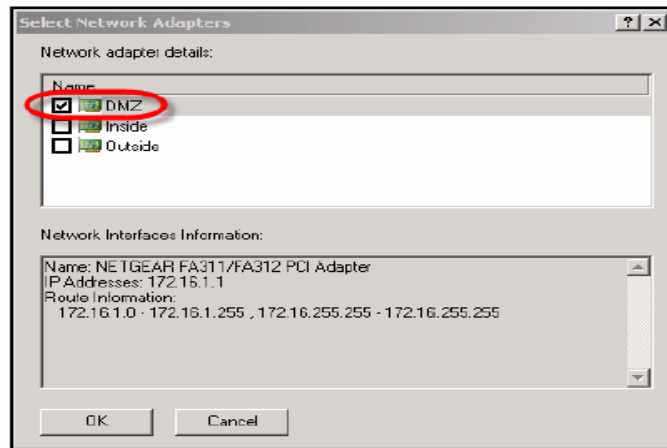
Một trong những thuật ngữ bảo mật được nhiều người quan tâm đó là DMZ (Demilitarized Zone), đây là từ chỉ vùng “Phi Quân Sự” trong thế giới thực, còn trong môi trường máy tính thì DMZ là nơi đặt những Server được publish ra ngoài internet để các người dùng bên ngoài (internet user) có thể truy cập đến Web Server với mục đích gia tăng tính năng an toàn cho hệ thống mạng. Bởi vì DMZ được tách biệt hoàn toàn với hệ thống Internal, cho nên khi internet user truy cập vào các máy chủ này sẽ không ảnh hưởng và gây nguy hiểm đối với các máy tính và dữ liệu nội bộ. Ngoài ra, khi các Server đặt trong DMZ còn ngăn ngừa được sự tương tác trực tiếp của internal user với chúng. Theo đúng nghĩa truyền thống của DMZ, các request (yêu cầu truy cập) của internet user đến các publish server phải qua DMZ trước rồi mới đến Firewall nội bộ, tuy nhiên ngày nay DMZ bao luôn cả tình huống internet user kết nối đến Firewall/Router và sau đó yêu cầu sẽ được chuyển để các server trong DMZ dựa trên Firewall Policy như trường hợp mà chúng ta áp dụng sau đây trên ISA Server để xây dựng 1 DMZ chứa mail và web server.

i. Tạo DMZ:

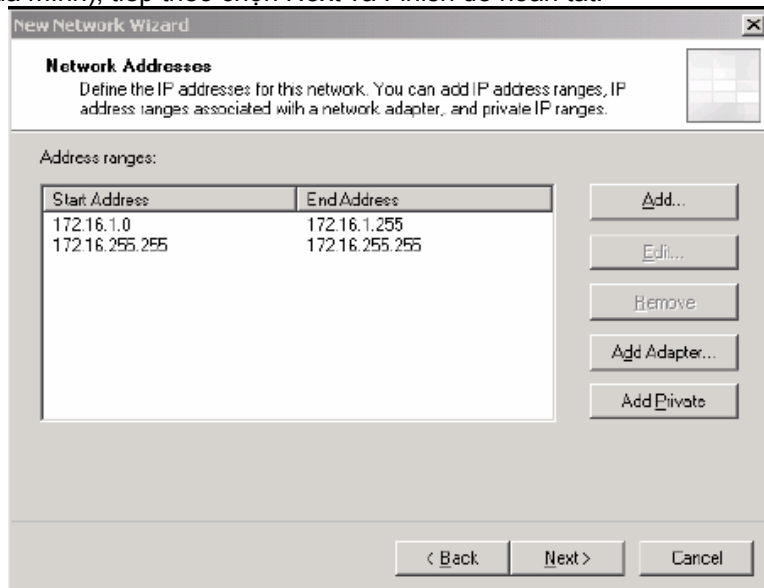
Trong phần Network hãy chọn Create a New Network, đặt tên là DMZ và chọn Next, chọn Perimeter Network (chúng ta có thể tạo bao nhiêu lớp mạng tùy ý không như trên ISA 2000 chỉ có 3 lớp, đây là một cải tiến của ISA Server 2004):



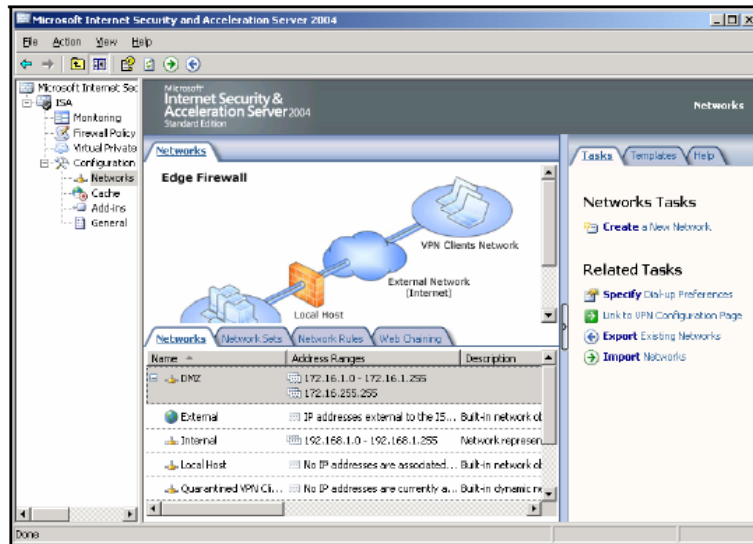
Sau khi click Next của sổ Network Address xuất hiện, hãy chọn Add Adapter để lựa chọn card mạng cho vùng DMZ:



Nhấn OK, và địa chỉ mạng cho vùng DMZ sẽ như hình dưới (các bạn có thể thay đổi theo yêu cầu hệ thống của mình), tiếp theo chọn Next và Finish để hoàn tất.

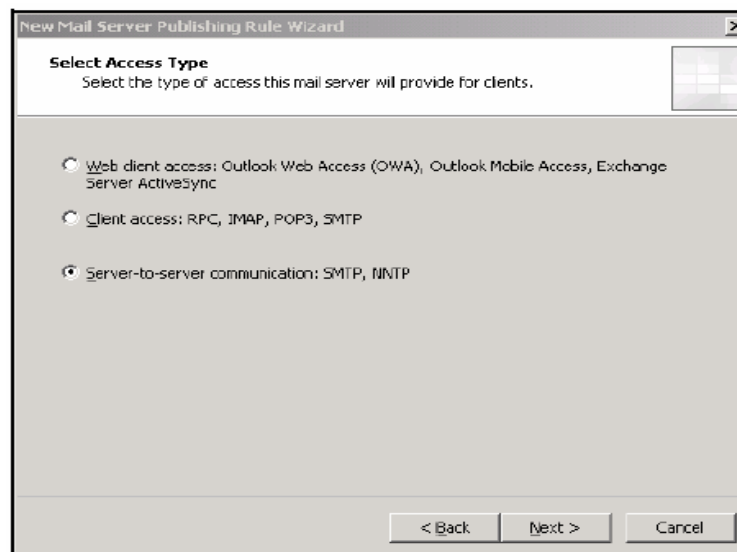


Sau khi click Apply để áp dụng cho hệ thống, trong phần Network chúng ta sẽ thấy một lớp mạng là DMZ tách biệt với hệ thống Internal, các bạn có thể đặt các Exchange Mail Server hay Apache Web Server với trong lớp mạng này.

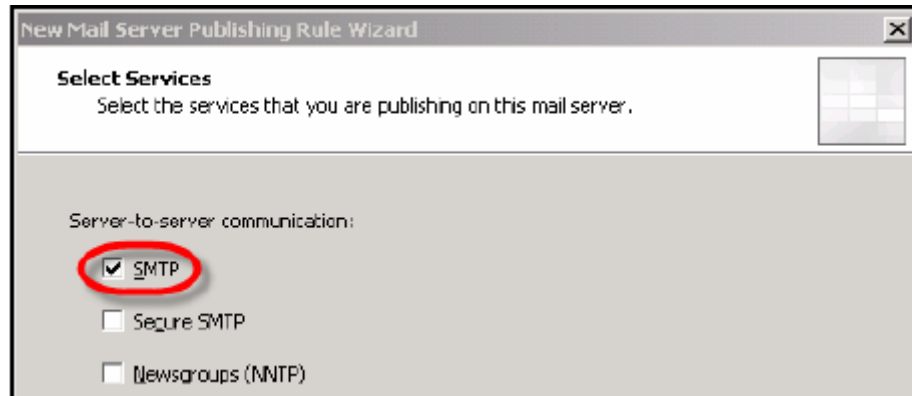


ii. Publish Exchange Server trong DMZ:

Lấy ví dụ, công ty T&C Descon có một Exchange Server có địa chỉ là 172.16.1.10 đặt trong DMZ. Để các User bên ngoài Internet có thể truy cập đến mail server để gửi và nhận mail chúng ta cần phải publish chúng thông qua ISA Firewall của mình. Mở ISA Management Console, chọn Firewall Policy, trên khung Task Pane hãy click vào Publish a Mail Server để hiển thị New Mail Server Publishing Rule Wizard. Đặt tên cho Publishing Rule này và chọn Next. Trong cửa sổ Select Server Type chúng ta chọn **Server-to-server Communications: SMTP, NNTP**



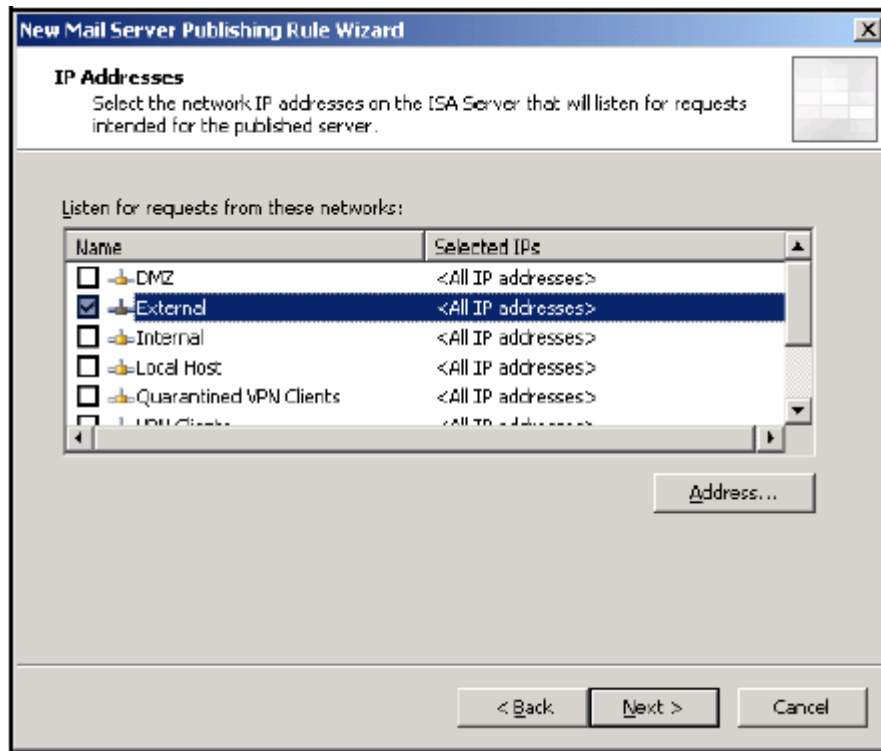
Chọn Next, trên khung Select Services hãy check vào ô SMTP



Trên cửa sổ tiếp theo chúng ta nhập vào địa chỉ của Mail Server trong DMZ, ở đây là 172.16.1.10



Cuối cùng là xác định lớp mạng được phép kết nối với Mail Server, trong trường hợp này User ở bên ngoài Internet nên chúng ta chọn lớp mạng là External và click Next, sau đó chọn Finish để hoàn tất quá trình publish mail server.



Cần lưu ý là để có thể check mail thì phải có thêm những protocol khác như DNS, POP hay RPC. Vì vậy có thể chúng ta cần cho phép các yêu cầu về DNS từ Mail Server với Domain Controller (có cài tích hợp DNS) trong lớp mạng Internal hay với các ISP DNS.

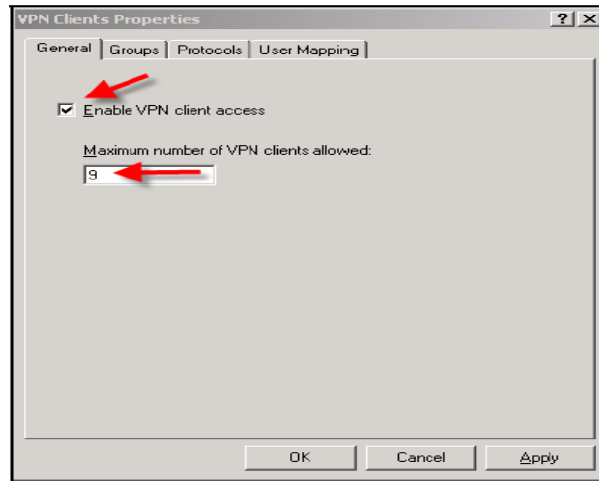
VIII – Cấu Hình Remote Access VPN Trên ISA Server 2004:

Ngoài chức năng quản lý truy cập Internet, Publish Web/Mail server và Caching, chúng ta có thể dùng ISA Server 2004 làm VPN Server cung cấp các kết nối remote access cho internet user để có thể truy cập tài nguyên trên mạng nội bộ. Ví dụ công ty có một số nhân viên kinh doanh sử dụng Laptop và họ cần truy cập vào hệ thống mạng LAN thông qua VPN Server để check mail, chạy những chương trình quản lý khách hàng CRM hay cập nhật các báo cáo..Sau đây là các bước cấu hình Remote Access VPN trên ISA 2004.

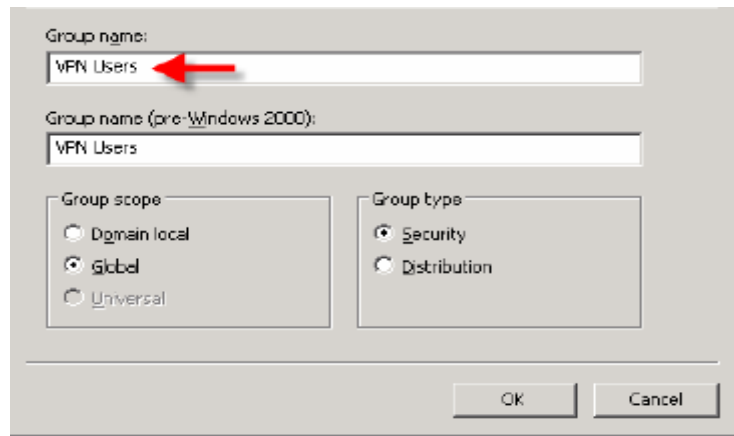
Mở ISA Management Console chọn mục Virtual Private Network (VPN), sau đó chọn **Verify that VPN Client Access is Enable**



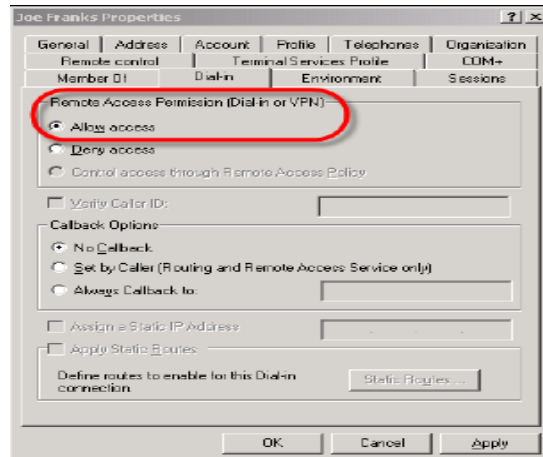
Đánh dấu vào Enable VPN Client access và đặt giá trị Maximum number of VPN clients allowed bằng 9 (số lượng VPN client tối đa có thể kết nối cùng lúc) rồi nhấn OK và Apply chính sách mới cho firewall.



Để các VPN client có thể kết nối thành công hãy tạo group VPN trên domain controller DC và gán quyền Allow access cho thuộc tính Dial-in đối với những user thuộc group VPN. Hãy log in vào Domain Controller (DC) của hệ thống và chọn **Start - > Administrative Tools - > Active Directory Users and Computers**. Nhấn chuột phải trên User container chọn **New - > Group** như hình sau:



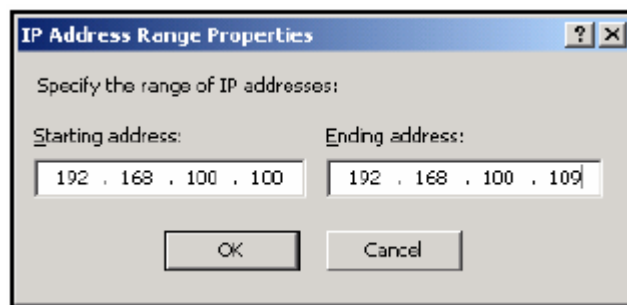
Add những user thuộc bộ phận kinh doanh (những người cần truy cập qua VPN) vào VPN Group, ví dụ Joe Franks. Trên thanh thuộc tính của Joe Franks chọn tab Dial-in và check Allow access



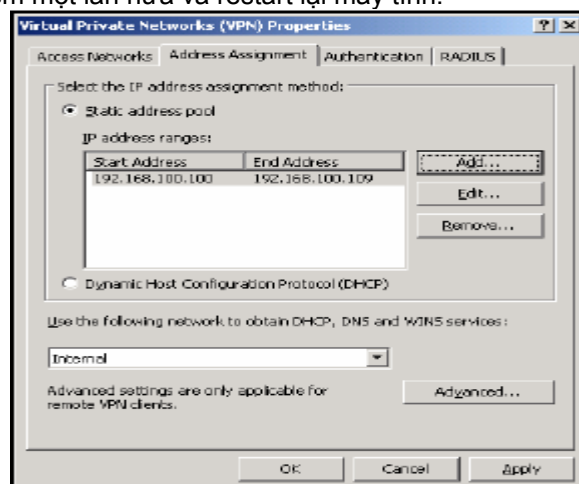
Hãy trở lại màn hình quản lý ISA server trên ISA1 mà chúng ta đang mở và chọn Specify Windows Users trên danh sách VPN Client, nhấn Add và chọn group VPN User chúng ta đã tạo.

Việc tiếp theo cần làm để cho phép VPN client kết nối là cấu hình địa chỉ IP cho các VPN client, có hai cách là sử dụng DHCP để cấp phát IP động cho các client hoặc dùng một static pool để gán IP cho chúng như sau:

Trên khung Tasks Pane nhấn vào mục Define Address Assignment, chọn Static address pool và nhập vào dãy địa chỉ sau:



Nhấn OK, xác nhận thêm một lần nữa và restart lại máy tính.



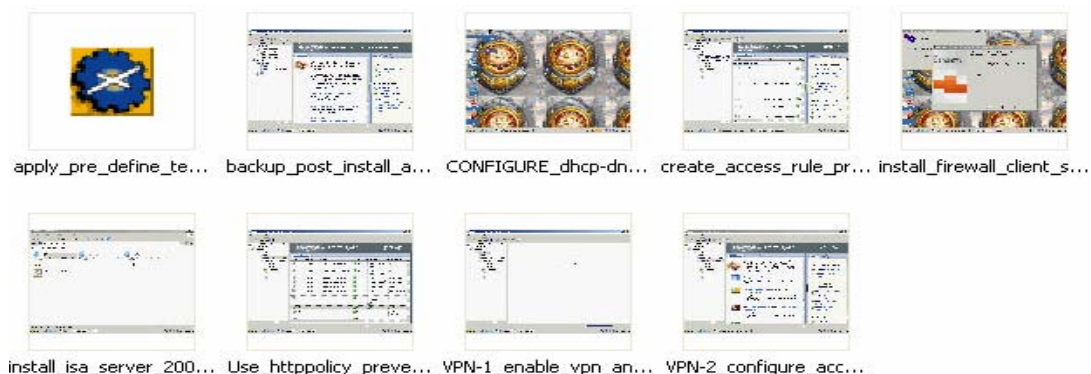
Cuối cùng, hãy tạo access rule cho phép các VPN client có thể truy cập đến các tài nguyên nội bộ sau khi kết nối thành công đến VPN server. Hãy chọn Firewall Policy và chọn Create New Access Rule đặt tên là **VPN Client full access to Internal**.



Nhấn Next và chọn Allow, trên cửa sổ tiếp theo chọn All outbound traffic. Do access rule cho phép VPN client truy cập tài nguyên nội bộ nên hãy xác định source traffic là VPN Clients trong phần Network. Ngược lại ở khung destination hãy chọn Internal trong phần Network, và chọn các giá trị mặc định cho những bước tiếp theo để hoàn tất.

Bây giờ ISA Server đã sẵn sàng cho các kết nối VPN, các bạn chỉ cần tạo các VPN Connection đến địa chỉ Outside của firewall và thực hiện kết nối và truy cập vào tài nguyên hệ thống nội bộ. Để nắm thêm chi tiết các bạn có thể tham khảo các file demo tại địa chỉ sau:

<http://www.security365.org/downloads/demo/ISA2004.rar>



Các Tập Tin Minh Họa Tiến Trình Cài Đặt Và Triển Khai ISA Server 2004

Nguyễn Trần Tường Vinh
MCSA/MCSE Security, Comptia SECURITY+, SCNP
Giám Đốc Công Ty Giải Pháp An Toàn
Leader@Security365.Org
www.security365.org