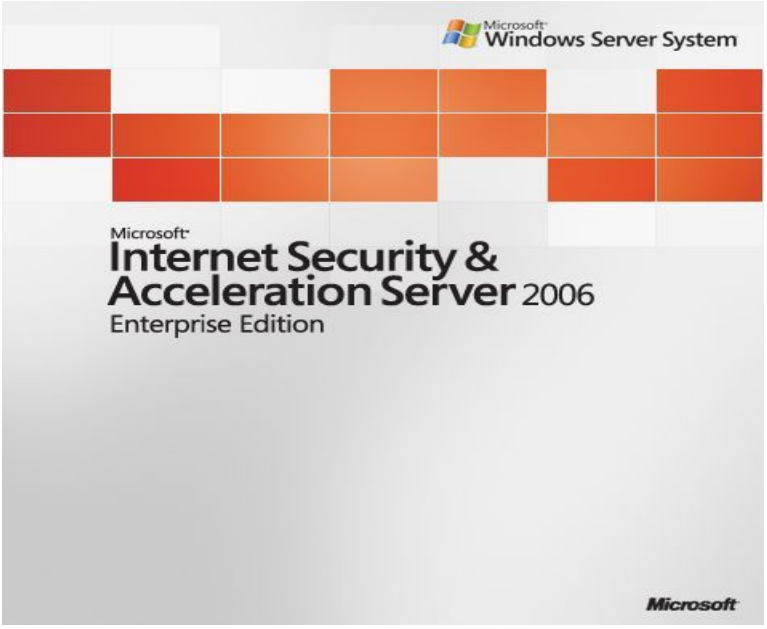
ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
Chi nhánh Trung Tâm Phát Triển Công Nghệ Thông Tin Tại
CẦN THƠ

ĐỒ ÁN TỐT NGHIỆP

KỸ THUẬT VIÊN

Đề tài: Thiết kế và xây dựng giải pháp quản trị an ninh mạng với phần mềm Firewall ISA Server 2006 cho mô hình doanh nghiệp vừa và nhỏ



GV hướng dẫn: **NGUYỄN DUY**
nguyenduy0606@gmail.com

Sinh viên thực hiện:

LÊ THÁI GIANG	**MSSV : 09720020**
ĐẶNG QUỐC QUÂN	**MSSV : 09720070**
NGUYỄN ANH DŨNG	**MSSV : 09720016**
NGUYỄN TRIỀU TIÊN	**MSSV : 09720102**

Lớp: **CỬ NHÂN 1 – KHÓA 2**

Cần Thơ, ngày 05 tháng 11 năm 2011

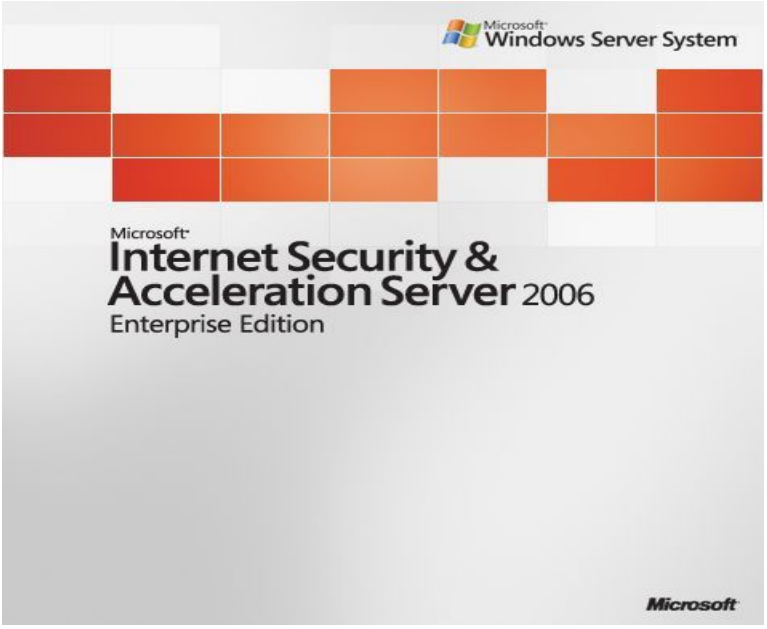
2011

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
Chi nhánh Trung Tâm Phát Triển Công Nghệ Thông Tin Tại
CẦN THƠ

ĐỒ ÁN TỐT NGHIỆP

KỸ THUẬT VIÊN

Đề tài: Thiết kế và xây dựng giải pháp quản trị an ninh mạng với phần mềm Firewall ISA Server 2006 cho mô hình doanh nghiệp vừa và nhỏ



GV hướng dẫn: **NGUYỄN DUY**
nguyenduy0606@gmail.com

Sinh viên thực hiện:

LÊ THÁI GIANG	**MSSV : 09720020**
ĐẶNG QUỐC QUÂN	**MSSV : 09720070**
NGUYỄN ANH DŨNG	**MSSV : 09720016**
NGUYỄN TRIỀU TIÊN	**MSSV : 09720102**

Lớp: **CỬ NHÂN 1 – KHÓA 2**

Cần Thơ, ngày 05 tháng 11 năm 2011

2011

LỜI MỞ ĐẦU

Ngày nay, việc duy trì hệ thống mạng nội bộ hoạt động ổn định , nhanh chóng, an toàn và tin cậy đang là vấn đề được các tổ chức và doanh nghiệp đặc biệt quan tâm. Trong đó, yếu tố an toàn mạng luôn được đặt lên hàng đầu. Nắm bắt được nhu cầu của các tổ chức và doanh nghiệp, một số tập đoàn công nghệ thông tin và truyền thông hàng đầu trên thế giới đã đưa ra nhiều giải pháp bảo mật cũng như các Firewall (cả phần cứng lẫn phần mềm) để bảo vệ môi trường mạng được trong sạch và an toàn. Hiện nay, các tổ chức và doanh nghiệp chọn cho mình cách bảo vệ hệ thống mạng của họ bằng nhiều cách khác nhau, trong đó, Isa Server được dùng khá phổ biến.

ISA Server là phần mềm Firewall chạy trên hệ điều hành Windows server 2003 Service Pack 2 của Microsoft. Kế thừa các ưu điểm của những điểm của những phiên bản trước đó, ISA Server 2006 đem đến cho người dùng một giao diện thân thiện, các thao tác quản trị đơn giản và dễ thực hiện. Đồng thời, phiên bản mới này có thể được cấu hình để trở thành firewall với các vai trò đa dạng như : bảo vệ hệ thống mạng nội bộ, tăng tốc độ truy cập web, quản lý băng thông, xuất bản web server , FTP server, Mail server, VPN Gateway…

Mong rằng phần mềm ISA Server 2006 nhằm bảo đảm an toàn cho những hệ thống mạng nhỏ đến trung bình, kết hợp với PC Monitor Console và một số tính năng của Mail Mdeamon được trình bày trong đồ án sẽ giúp cho những doanh nghiệp vừa và nhỏ đang có nhu cầu muốn bảo vệ hệ thống mạng nội bộ của mình được tốt hơn, an toàn và trong sạch hơn.

LỜI CÁM ƠN

Sau 2 tháng nỗ lực thực hiện đồ án tốt nghiệp đã phần nào hoàn chỉnh. Ngoài sự cố gắng hết mình của bản thân và các thành viên trong nhóm, nhóm còn nhận được sự hỗ trợ rất lớn từ bạn bè, thầy cô và gia đình.

Trước hết, nhóm chúng em cám ơn đến các thầy cô đã truyền đạt những kiến thức quý báo cho chúng em trong suốt quá trình học tập. Đặc biệt, nhóm chúng em xin gởi lời cám ơn chân thành và sâu sắc đến thầy Nguyễn Duy, thầy đã tận tình hướng dẫn giúp đỡ và đóng góp cho chúng em nhiều ý kiến quí báu trong suốt quá trình làm đồ án.

Cám ơn gia đình, những người bạn thân trong nhóm cũng như các bạn chung khóa đã luôn bên cạnh và cho những lời khuyên chân thành. Cám ơn thầy cô ở trung tâm đã tạo điều kiện tốt nhất để cho nhóm chúng em cũng như các nhóm khác thực hiện đồ án một cách thuận lợi và suôn sẻ.

Cuối cùng, nhóm chúng em xin cám ơn tất cả mọi người, cám ơn tất cả những gì mà mọi người đã dành cho nhóm.

NHẬN XÉT

(Của giảng viên hướng dẫn)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Cần Thơ, ngày……..tháng…….năm 2011

Giảng viên hướng dẫn

Nguyễn Duy

NHẬN XÉT

(Của giảng viên phản biện)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Cần Thơ, ngày……tháng…….năm 2011

Giảng viên phản biện

Mục lục

GIỚI THIỆU SƠ LƯỢC ĐỒ ÁN

- **Tên đồ án:**

Thiết kế và xây dựng giải pháp quản trị an ninh mạng với phần mềm Firewall ISA Server 2006 cho mô hình doanh nghiệp vừa và nhỏ

- **Nội dung đồ án :**

Xây dựng hệ thống mạng nội bộ cho doanh nghiệp vừa và nhỏ.

Sử dụng phần mềm Firewall ISA Server 2006 để bảo vệ hệ thống mạng nội bộ và tăng tốc độ truy cập web,quản lý băng thông, xuất bản Web Server , Mail Server…

- **Mục tiêu đồ án**

Thiết kế và xây dựng giải pháp quản trị an ninh mạng với phần mềm Firewall ISA Server 2006 bảo vệ mạng nộ bộ. Ngăn chặn sự xâm nhập của các Hacker dò tìm những lổ hỏng của các port thông qua mạng Internet. Bên cạnh đó, sử dụng những chức năng có sẵn và những chức năng add-in của ISA Server 2006 để hạn chế các nhân viên sử dụng internet không hợp lý. Đồng thời sử dụng các chức năng trên để Publish các dịch vụ Web, Mail ra ngoài internet nhằm phuc vụ quá trình làm việc của các nhân viên. Ngoài ra, các nhân viên có thể truy cập từ xa qua mạng nhờ chức năng VPN Client To Site…

Tuy nhiên, Firewall ISA Server 2006 chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ. Firewall ISA Server 2006 không thể ngăn chặn sự xâm nhập của nhân tố con người như nhân viên, hoặc USB có chứa các virus độc hại. Vì thế, chúng em đã kết hợp phần mềm Pc monitor console cho phép quan sát màn hình của những máy tính được nối trong mạng.

Theo cách này có thể quan sát nhân viên sử dụng máy tính và ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn bên ngoài internet.

- **Lĩnh vực ứng dụng**

Ứng dụng thực tiễn để giải quyết những vấn đề về quản trị và an ninh mạng trong mô hình của Doanh Nghiệp vừa và nhỏ.

CHƯƠNG I : TỔNG QUAN VỀ FIREWALL

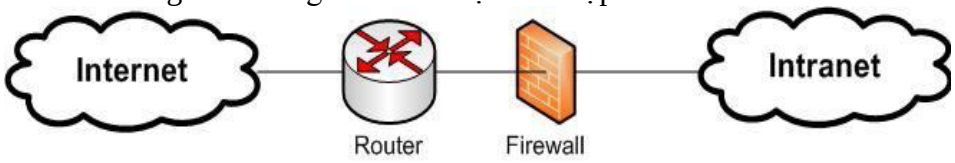
1. Firewall là gì ?

Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống

Thông thường Firewall được đặt giữa mạng bên trong (Intranet) của một công ty, tổ chức, ngành hay một quốc gia, và Internet. Vai trò chính là bảo mật thông tin, ngăn chặn sự truy nhập không mong muốn từ bên ngoài (Internet) và cấm truy nhập từ bên trong (Intranet) tới một số địa chỉ nhất định trên Internet.

2. Phân loại firewall

Firewall được chia làm 2 loại, gồm Firewall cứng và Firewall mềm:
Firewall cứng: Là những firewall được tích hợp trên Router.



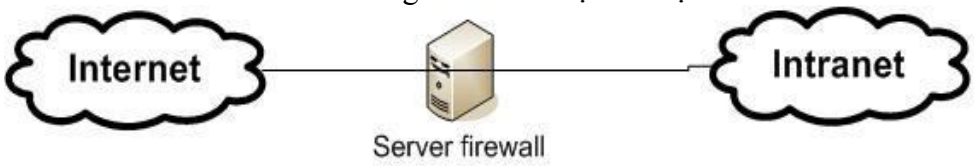
Đặc điểm của Firewall cứng:

Không được linh hoạt như Firewall mềm: Không thể thêm chức năng, thêm quy tắc như firewall mềm

Firewall cứng hoạt động ở tầng thấp hơn Firewall mềm (Tầng Network và tầng Transport)

Firewall cứng không thể kiểm tra được nột dung của gói tin.
Ví dụ Firewall cứng: NAT (Network Address Translate).

Firewall mềm: Là những Firewall được cài đặt trên Server.



Đặc điểm của Firewall mềm:

Tính linh hoạt cao: Có thể thêm, bớt các quy tắc, các chức năng.

Firewall mềm hoạt động ở tầng cao hơn Firewall cứng (tầng ứng dụng)

Firewal mềm có thể kiểm tra được nội dung của gói tin (thông qua các từ khóa).

Ví dụ về Firewall mềm: Zone Alarm, Microsoft ISA Server 2006, Norton Firewall…

3. Chức năng chính:

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet.

Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet). Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet

vào Intranet). Theo dõi luồng dữ liệu mạng giữa Internet và Intranet. Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập. Kiểm soát người sử dụng và việc truy nhập của người sử dụng. Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng.

4. Cấu trúc firewall

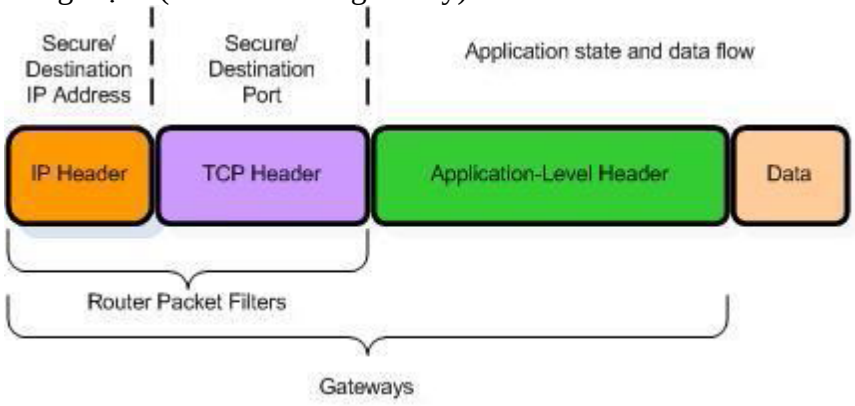
FireWall bao gồm :

Một hoặc nhiều hệ thống máy chủ kết nối với các bộ định tuyến (router) hoặc có chức năng router. Các phần mềm quản lý an ninh chạy trên hệ thống máy chủ.

Thông thường là các hệ quản trị xác thực (Authentication), cấp quyền (Authorization) và kế toán (Accounting).

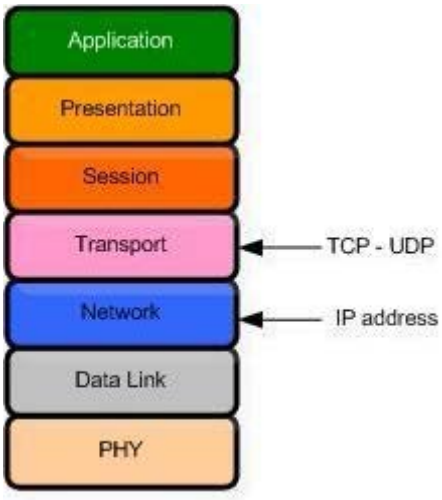
5. Các thành phần của FireWall

Một FireWall bao gồm một hay nhiều thành phần sau:
Bộ lọc packet (packet- filtering router);
Cổng ứng dụng (Application-level gateway hay proxy server);
Cổng mạch (Circuite level gateway).



6. Bộ lọc paket (Paket filtering router)

Nguyên lý :



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 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 chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS…) thành các gói dữ liệu (data pakets) rồi gán cho các paket 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 những con số địa chỉ của chúng.
Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không. Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng.

- Địa chỉ IP nơi xuất phát (IP Source address)
- Địa chỉ IP nơi nhận (IP Destination address)
- Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)
- Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)
- Cổng TCP/UDP nơi nhận (TCP/UDP destination port)
- Dạng thông báo ICMP (ICMP message type)
- Giao diện packet đến (incomming interface of packet)
- Giao diện packet đi (outcomming interface of packet)

Nếu luật lệ lọc packet được thoả mãn thì packet được chuyển qua firewall. Nếu không packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết
nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng 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 các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ.

7. Ưu điểm:

Đa số các hệ thống firewall đều sử dụng bộ lọc packet. Một trong những ưu điểm của phương pháp dùng bộ lọc packet là chi phí thấp vì cơ chế lọc packet đã đợc bao gồm trong mỗi phần mềm router. Ngoài ra, bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng.

8. Những hạn chế của firewall

Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó.

Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không “đi qua” nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đờng dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

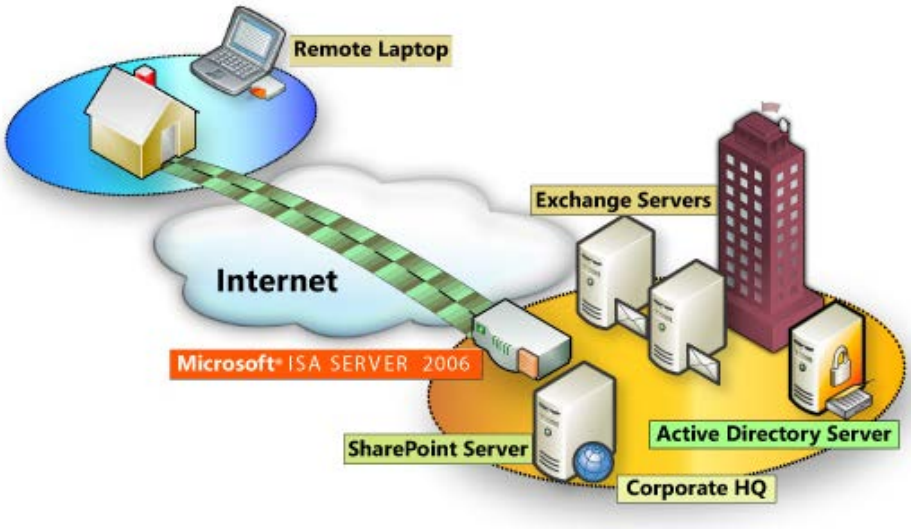
Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

Firewall không thể làm nhiệm vụ và quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của firewall. Tuy nhiên, Firewall vẫn là giải pháp hữu hiệu được áp dụng rộng rãi.

CHƯƠNG II : GIỚI THIỆU ISA SERVER 2006

1. Microsoft ISA Server 2006 là gì ?

Microsoft ISA Server 2006 là phần mềm, được tạo ra nhằm bảo vệ hệ thống mạng nội bộ trước sự tấn công từ Internet, đồng thời giúp cho người sử dụng trong mạng nội bộ truy cập các ứng dụng và dữ liệu một cách an toàn.



Các phiên bản của ISA Server 2006

ISA Server 2006 có hai phiên bản: Standard và Enterprise. Trong đó phiên bản Standard được thiết kế cho những người dùng cần bảo vệ hệ thống mạng nhỏ với chỉ một firewall. Cao cấp hơn, phiên bản Enterprise được thiết kế cho những hệ thống mạng trung tâm trở lên với một hay vài nhóm firewall.

So sánh giữa 2 phiên bản :Standard Editionvà Enterprise Edition

- Về cơ bản thì bản Standard và bản Enterprise có các chức năng tương đương nhau.
- Bản Enterprise có hỗ trợ thêm 3 tính năng sau không có trong bản Standard:

+ *Centralized storage of configuration data:*

Trong khi bản Standard lưu thông tin về cấu hình (configuration information -> conf info) trong registry trên chính máy cài ISA thì bản Enterprise lưu conf info của nó trên một thư mục (directory) riêng biệt. Khi bạn cài bản Enterprise bạn phải chỉ ra một hay nhiều máy đóng vai trò là máy lưu cấu hình (Configuration storage server). Các storage server này sử dụng ADAM (Active Directory Application Data) để lưu trữ cấu hình của tất cả các ISA trong tổ chức. ADAM có thể cùng lúc cài đặt trên nhiều máy, nên bạn có thể có nhiều storage server.(Bạn có thể cài ADAM lên máy khác ko có ISA hay cài lên máy ISA cũng được). Dữ liệu trên các storage server này sẽ tự nhân bản (replicate) cho nhau theo chu kỳ. Nhờ đó hỗ trợ tốt hơn cho người quản trị. Ví dụ như bạn muốn thay đổi cấu hình của một hay nhiều ISA server bạn chỉ việc ngồi vào một trong những storage server mà làm. Còn với bản Standard, bạn phải đến từng máy để cấu hình.

+ *Support for Cache Array Routing Protocol – CARP:*

Bản Enterprise cho phép ta chia sẻ việc cache giữa một dãy các ISA với nhau. Với bản Enterprise, một dãy gồm nhiều máy ISA sẽ được cấu hình trở thành một vùng cache đơn luận lý bằng cách kết nối khả năng cache của tất cả các ISA lại với

nhau. Để thực hiện tính năng này, ISA sử dụng CARP. Cơ chế như sau : khi một máy client đi một trang web nào đó, CARP sẽ chỉ định một ISA trong dãy cache lại trang đó. Khi một máy client khác đi trang web khác, CARP chỉ định tiếp một máy ISA khác cache lại trang web. Cứ luân phiên như thế. Khi một client bất kì đi một trang web đã được cache thì CARP sẽ chỉ định ra máy ISA nào đã cache trang đó để trả về cho máy client. CARP giúp tối ưu hóa khả năng cache.

+ *Integration of Network Load Balancing - NLB : (Tích hợp cân bằng tải lên ISA)*

NBL là một thành phần network có sẵn trong Windows 2000 Server và Windows Server 2003. Sử dụng NLB tức là chúng ta phải chấp nhận dư thừa (redundancy), ta sẽ có từ 2 đến nhiều máy cùng chức năng (vd cùng là ISA) để cân bằng đường truyền, tránh hiện tượng quá tải. NLB cũng là một hình thức backup, vì nếu có một máy bị down (chết) thì sẽ có máy khác thay thế nhiệm vụ trong thời gian phục hồi máy kia. NLB đáp ứng nhu cầu về tính ổn định và tính sẵn sàng cao trong hệ thống.

Với bản Standard, bạn phải cấu hình NLB bằng tay. Còn với bản Enterprise, NLB được tích hợp vào ISA nên bạn có thể quản lý NLB từ ISA. Bạn có thể dùng ISA Server Management Console để cấu hình, quản lý, giám sát (monitor) NLB.

2. Các đặc điểm của Microsoft ISA 2006:

Cung cấp tính năng Multi-networking: Kỹ thuật thiết lập các chính sách truy cập dựa trên địa chỉ mạng, thiết lập firewall để lọc thông tin dựa trên từng địa chỉ mạng con,…

Unique per-network policies: Đặc điểm Multi-networking được cung cấp trong ISA Server cho phép bảo vệ hệ thống mạng nội bộ bằng cách giới hạn truy xuất của các Client bên ngoàiinternet, bằng cách tạo ra một vùng mạng ngoại vi perimeter network (được xem là vùng DMZ,demilitarized zone, hoặc screened subnet), chỉ cho phép Client bên ngoài truy xuất vào cácServer trên mạng ngoại vi, không cho phép Client bên ngoài truy xuất trực tiếp vào mạng nội bộ.

Stateful inspection of all traffic: Cho phép giám sát tất cả các lưu lượng mạng.

NAT and route network relationships: Cung cấp kỹ thuật NAT và định tuyến dữ liệu cho mạng con.

Network templates: Cung cấp các mô hình mẫu (network templates) về một số kiến trúc mạng, kèm theo một số luật cần thiết cho network templates tương ứng.

Cung cấp một số đặc điểm mới để thiết lập mạng riêng ảo (VPN network) và truy cập từ xa cho doanh nghiệp như giám sát, ghi nhận log, quản lý session cho từng VPN Server, thiết lập access policy cho từng VPN Client, cung cấp tính năng tương thích với VPN trên các hệ thống khác.

Cung cấp một số kỹ thuật bảo mật (security) và thiết lập Firewall cho hệ thống nhưAuthentication, Publish Server, giới hạn một số traffic

Cung cấp một số kỹ thuật cache thông minh (Web cache) để làm tăng tốc độ truy xuất mạng,giảm tải cho đường truyền, Web proxy để chia sẻ truy xuất Web

Cung cấp một số tính năng quản lý hiệu quả như: giám sát lưu lượng, reporting qua Web, exportvà import cấu hình từ XML configuration file, quản lý lỗi hệ thốngthông qua kỹ thuật gởi thôngbáo qua E-mail,..

Application Layer Filtering (ALF): là một trong những điểm mạnh của ISA Server 2006, khônggiống như packet filtering firewall truyền thống, ISA 2006 có

thể thao tác sâu hơn như có thể lọcđược các thông tin trong tầng ứng dụng. Một số đặc điểm nổi bậc của ALF:

Cho phép thiết lập bộ lọc HTTP inbound và outbound HTTP.

Chặn được các cả các loại tập tin thực thi chạy trên nền Windows như .pif, .com,…

Có thể giới hạn HTTP download.

Có thể giới hạn truy xuất Web cho tất cả các Client dựa trên nội dung truy cập.

Có thể điều kiển truy xuất HTTP dựa trên chữ ký (signature).

Điều khiển một số phương thức truy xuất của HTTP.

3. Cài đặt Microsoft Server 2006

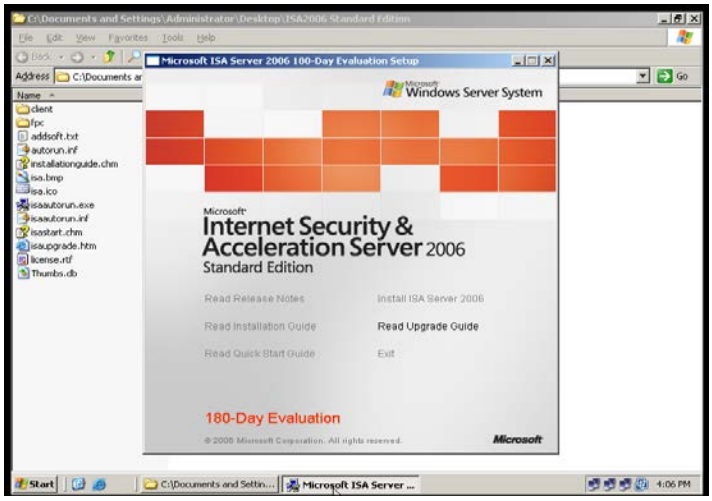
3.1. Yêu cầu hệ thống:

Thành phần	Yêu cầu
Hệ điều hành	Microsoft Windows Server 2003 32-bit service Pack 1 hoặc Microsoft Windows Server 2003 R2 32-bit.
Ram	512 MB hoặc cao hơn.
Card mạng	Một card mạng LAN (card host-only) Một card mạng DMZ (card host-only) Một card mạng WAN (card Bridged)
Ổ đĩa cài đặt	CD-ROM hoặc DVD-ROM

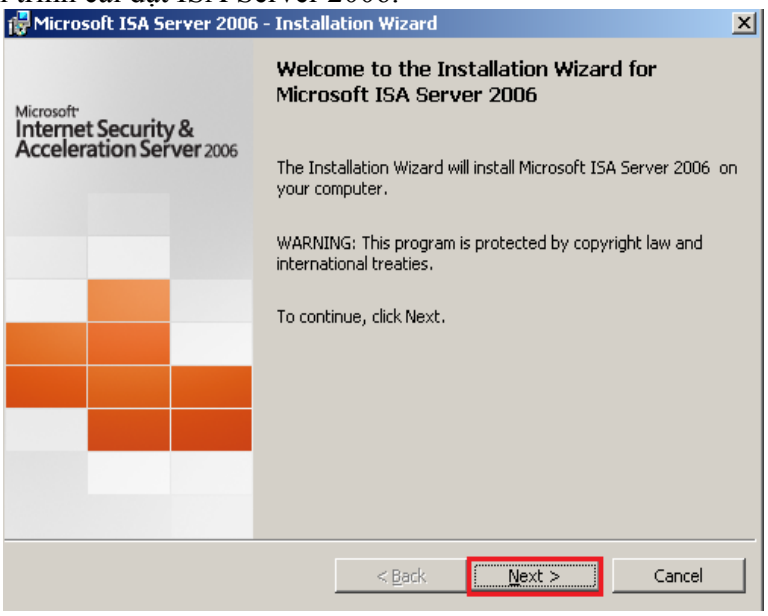
Đặt địa chỉ IP:

Card mạng	Địa chỉ IP
Card mạng LAN	IP Address: 10.0.0.1 Subnet Mask: 255.0.0.0 Default Gateway: 10.0.0.1 DNS Server: 10.0.0.2
Card mạng DMZ	IP Address: 172.16.0.1 Subnet Mask: 255.255.0.0 Default Gateway: 172.16.0.1
Card mạng WAN	IP Address: 192.168.1.100 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1 DNS Server: 8.8.8.8 8.8.4.4

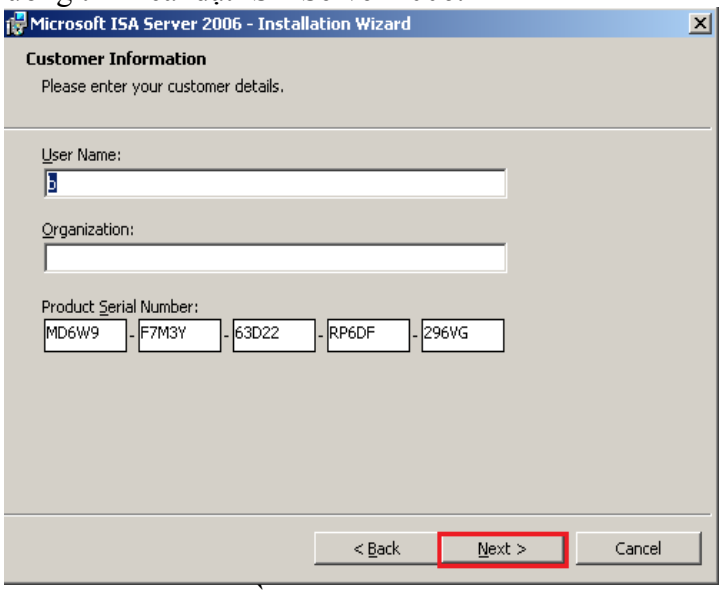
3.2. Tiến trình cài đặt:



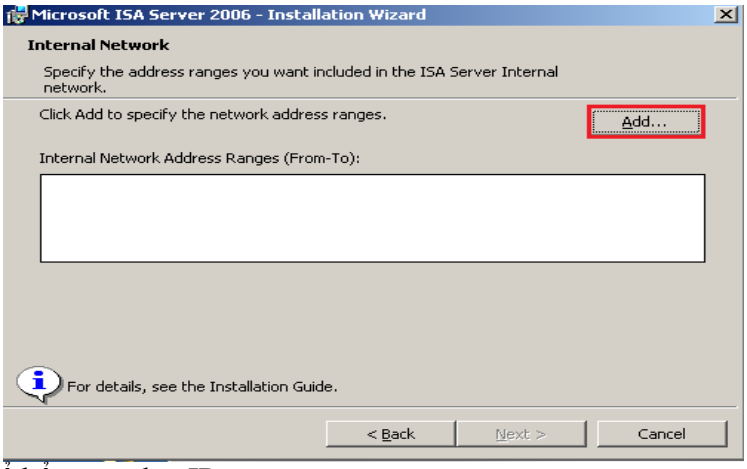
Bắt đầu tiến trình cài đặt ISA Server 2006.



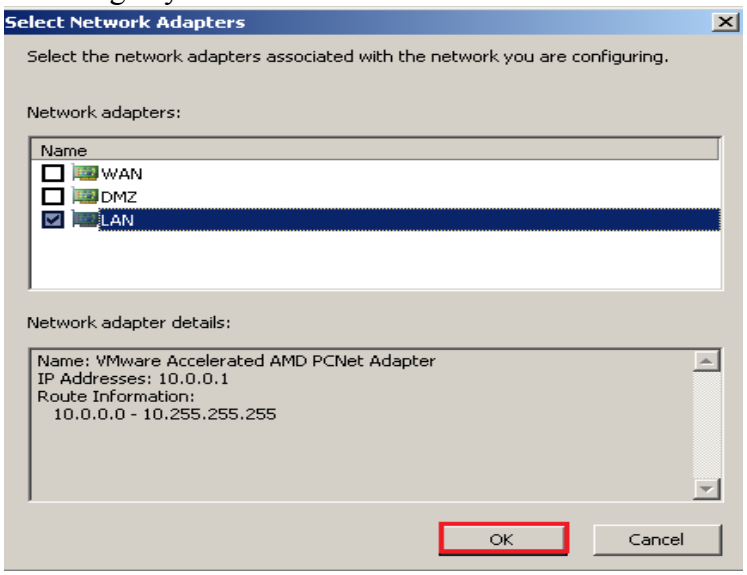
Khởi động chương trình cài đặt ISA Server 2006.



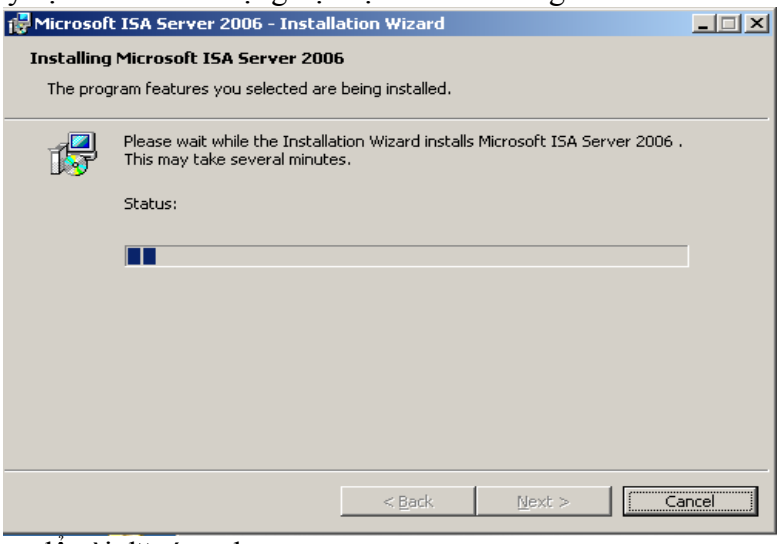
Điền dãy khóa và các thông tin về khách hàng



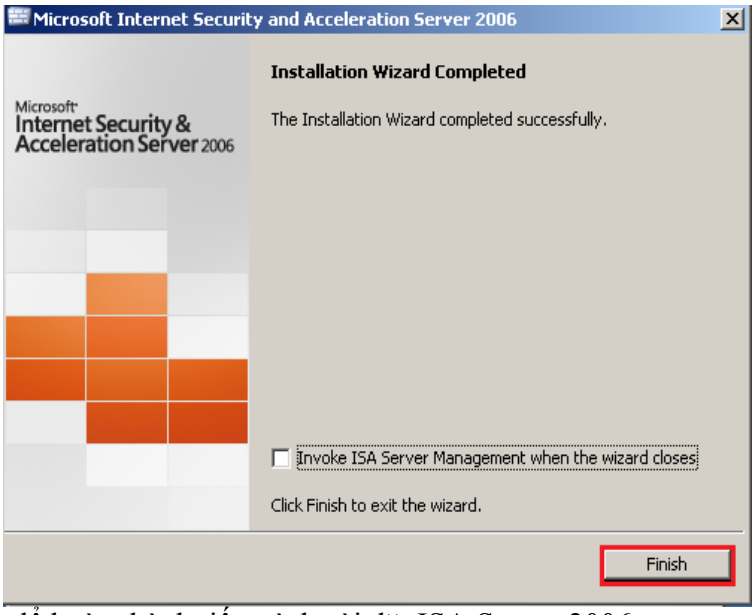
Chọn Add để bổ xung dãy IP



Bổ xung dãy địa chỉ IP cho mạng nội bộ với Add Range



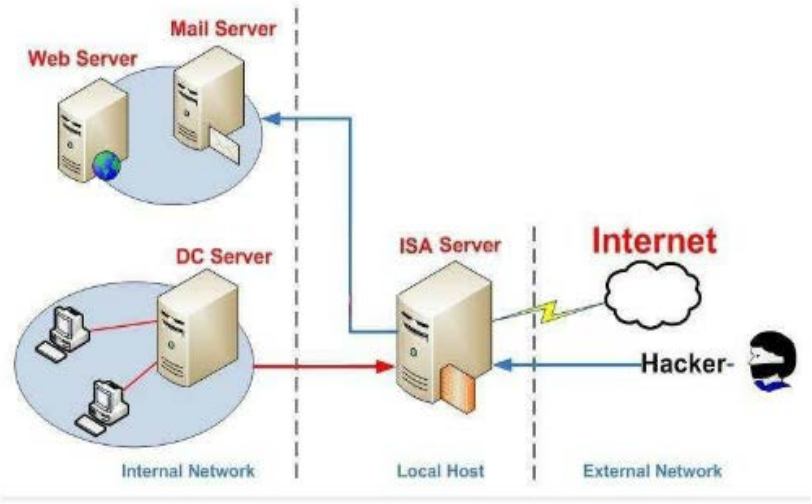
Tiếp tục next để cài đặt ứng dụng.



Nhấn Finish để hoàn thành tiến trình cài đặt ISA Server 2006

4. Cài 3 Leg Perimeter Template

- **Mô hình**



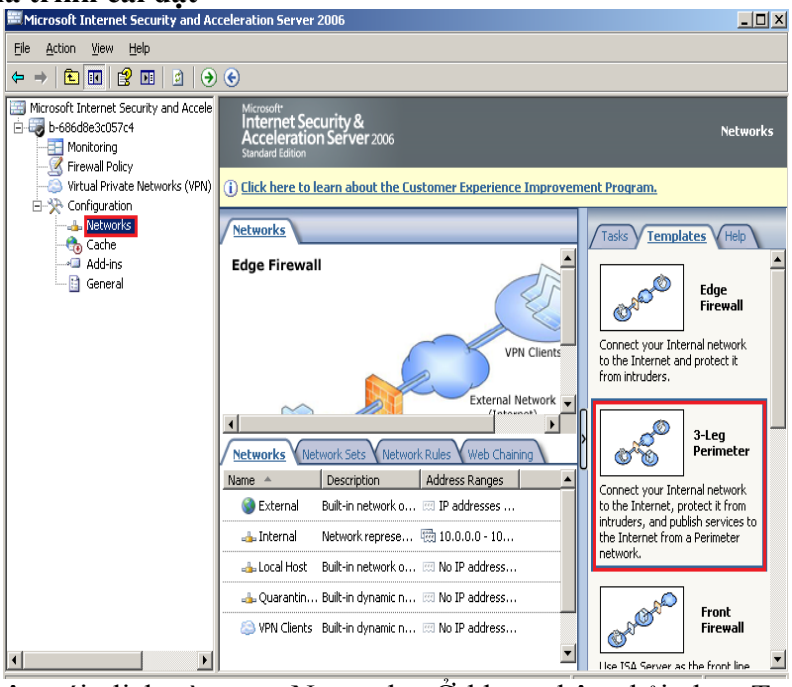
Với mô hình này trong Internal network chúng ta sẽ chia làm hai phần:

Phần thứ nhất là các máy như Mail Server …để người dùng từ External NetWork có thể truy cập vào.

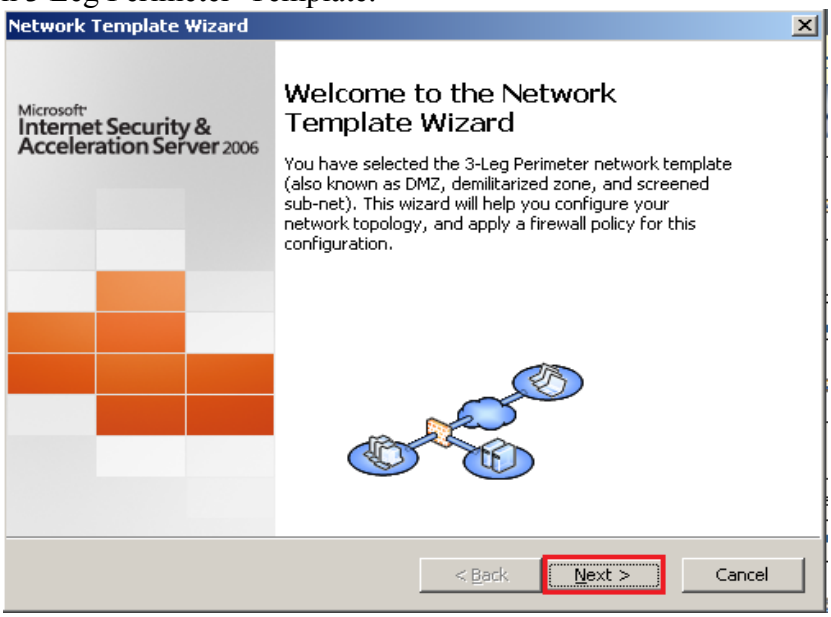
Phần thứ hai là các máy nội bộ cần được bảo mật kỹ càng hơn phần thứ nhất.

Tại máy ISA Server ta cần đến 3 card mạng.

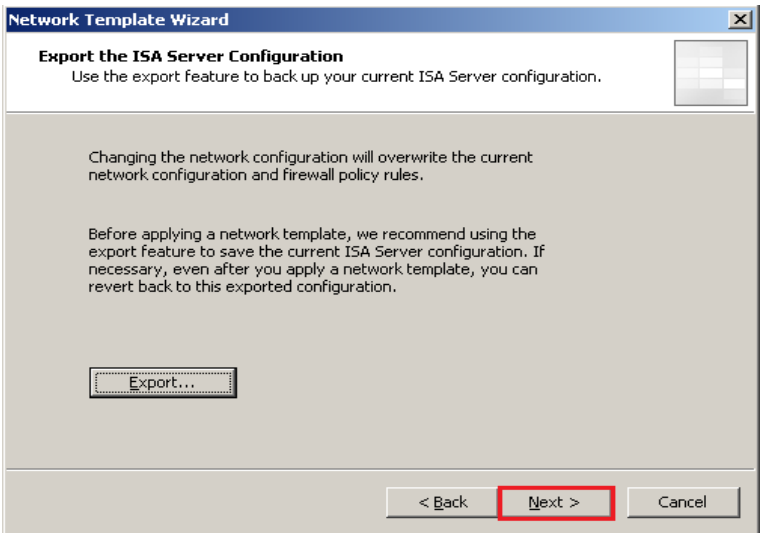
- **Quá trình cài đặt**



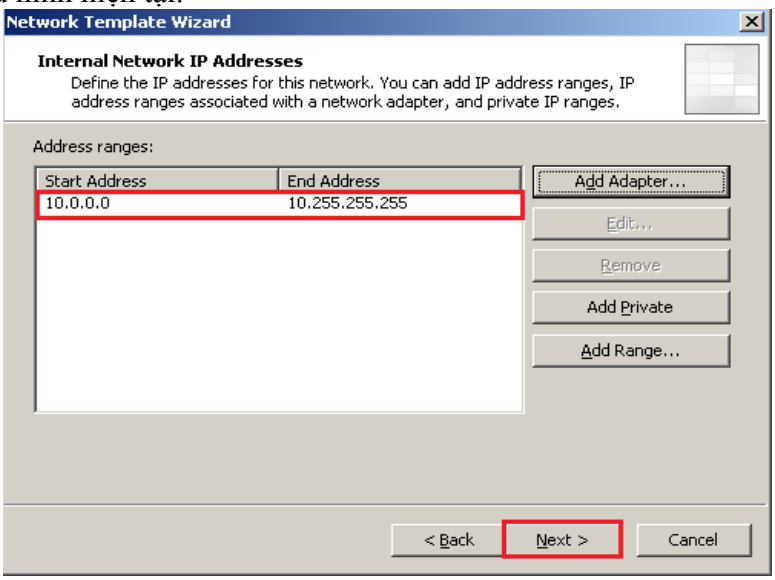
Ở khung bên trái click vào mục Networks. Ở khung bên phải chọn Templates và click chọn 3 Leg Perimeter Template.



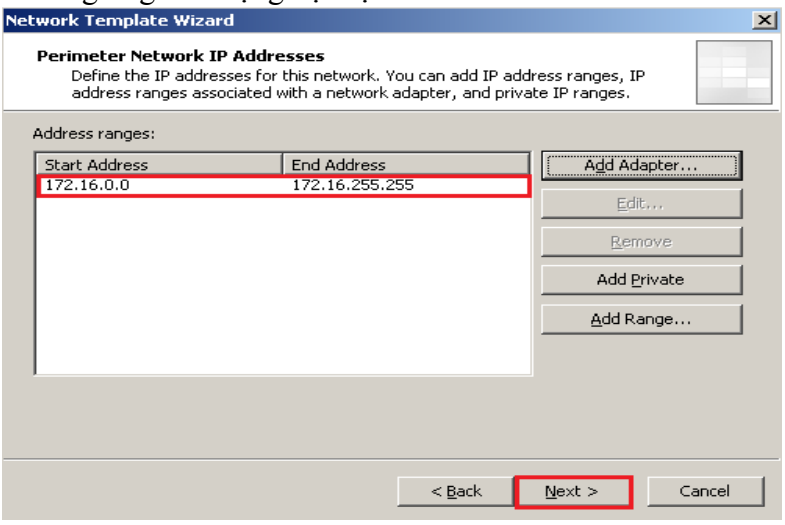
Khởi chạy trình tạo Template.



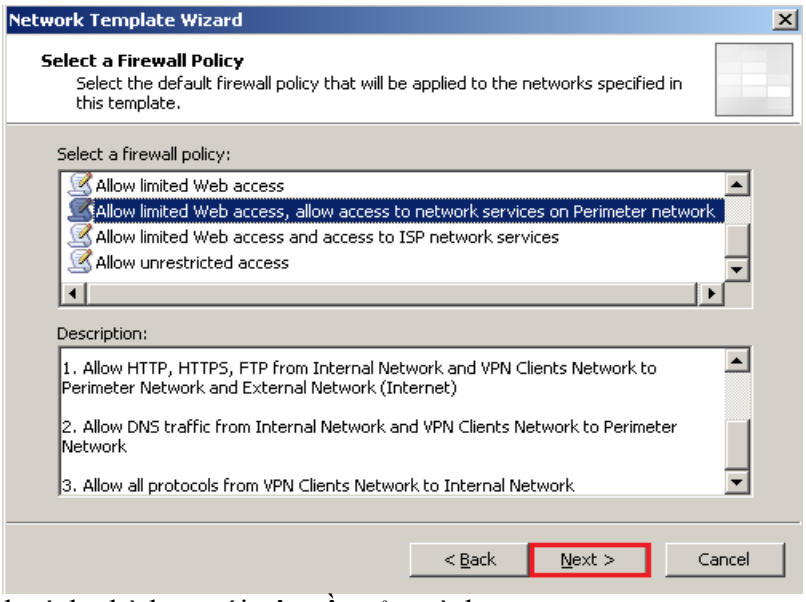
Sao lưu cấu hình hiện tại.



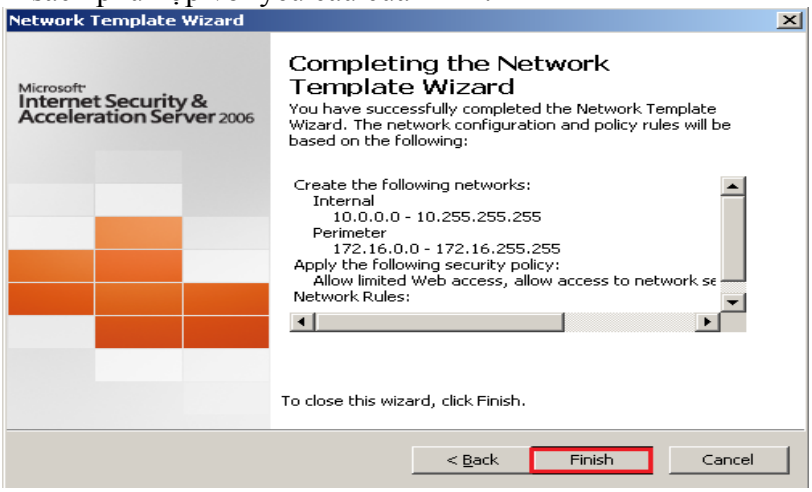
Điền dãy IP tương ứng với mạng nội bộ.



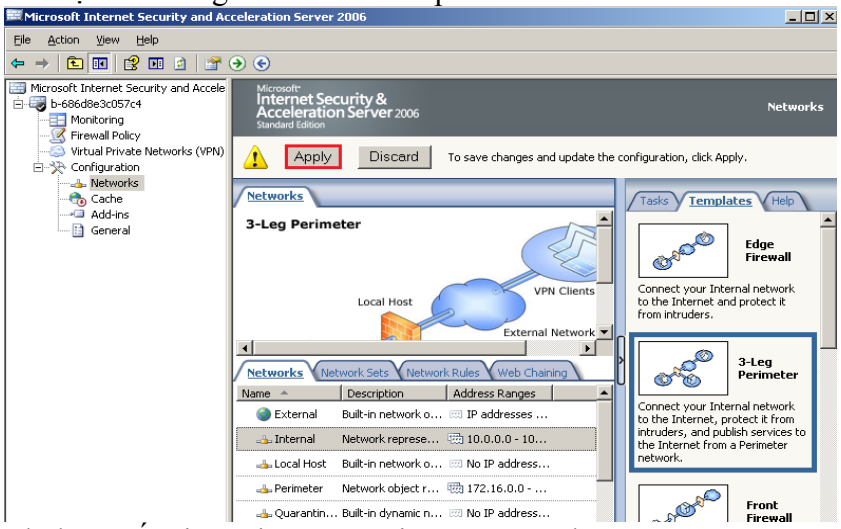
Điền dãy IP tương ứng với mạng DMZ.



Chọn chính sách phù hợp với yêu cầu của mình.



Hoàn thành việc cài 3 Leg Perimeter Template



Nhấn Apply hoàn tất việc cài 3 Leg Perimeter Template

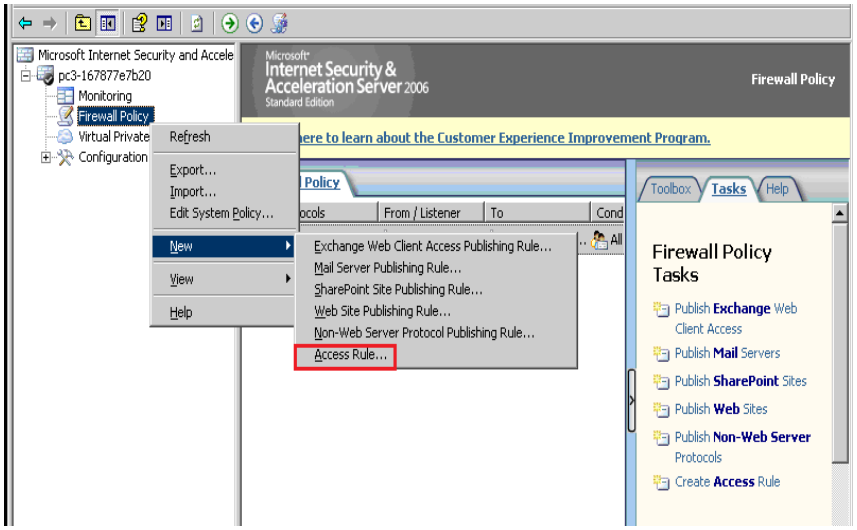
5. Thiết lập Access Rule

Access Rule điều khiển các truy cập ra bên ngoài từ một Network được bảo vệ nằm trong dến một network khác không được bảo vệ nằm ngoài.

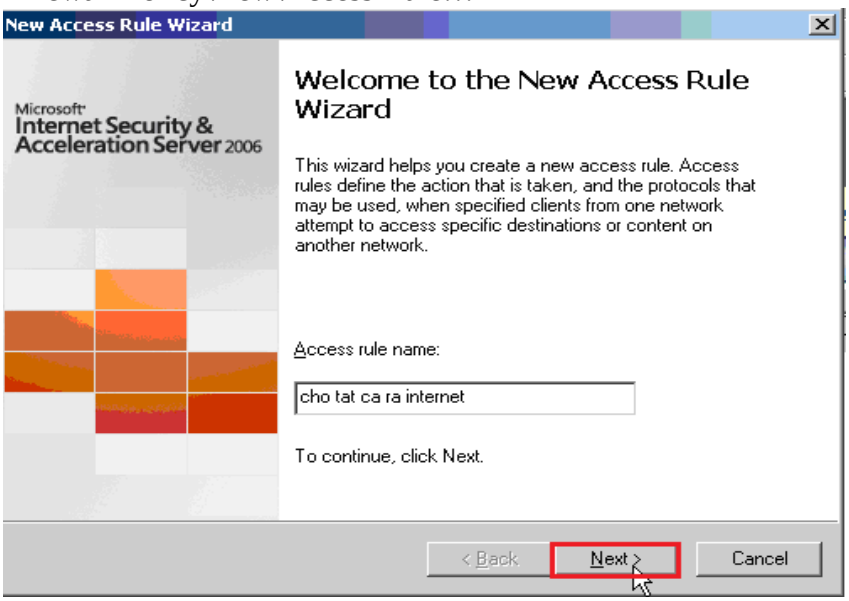
Các thành phần của cua Rule:

Rule name
Action
Protocols
Source
Destination
User
…

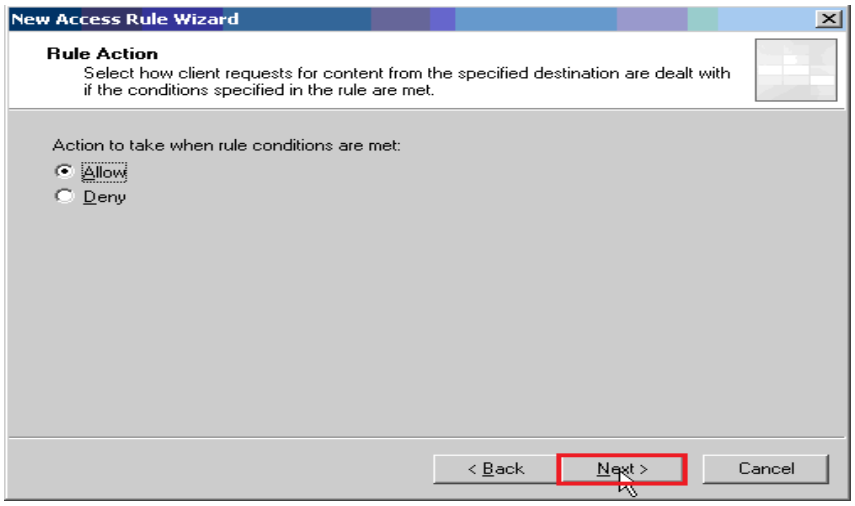
5.1. Cho vùng Lan ra ngoài Internet



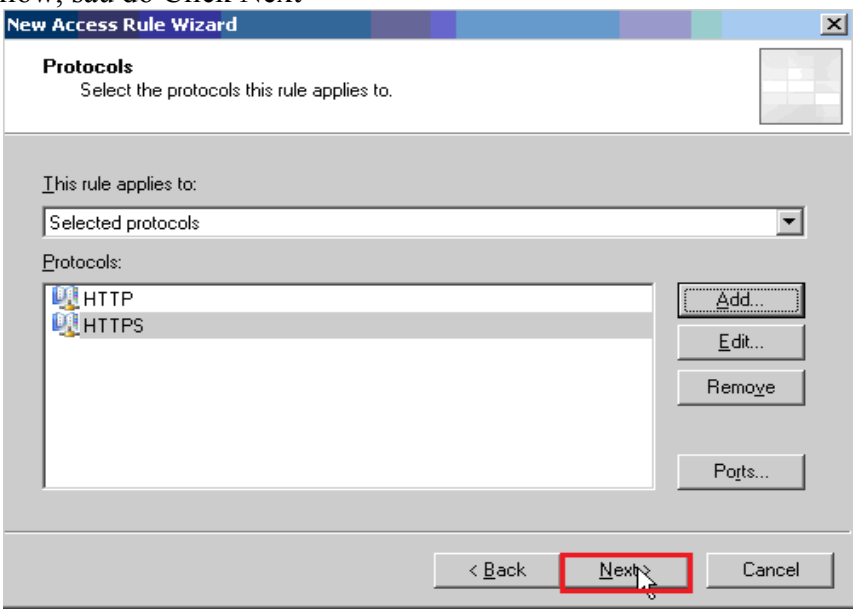
R_Click Firewall Policy\New\Access Rule…



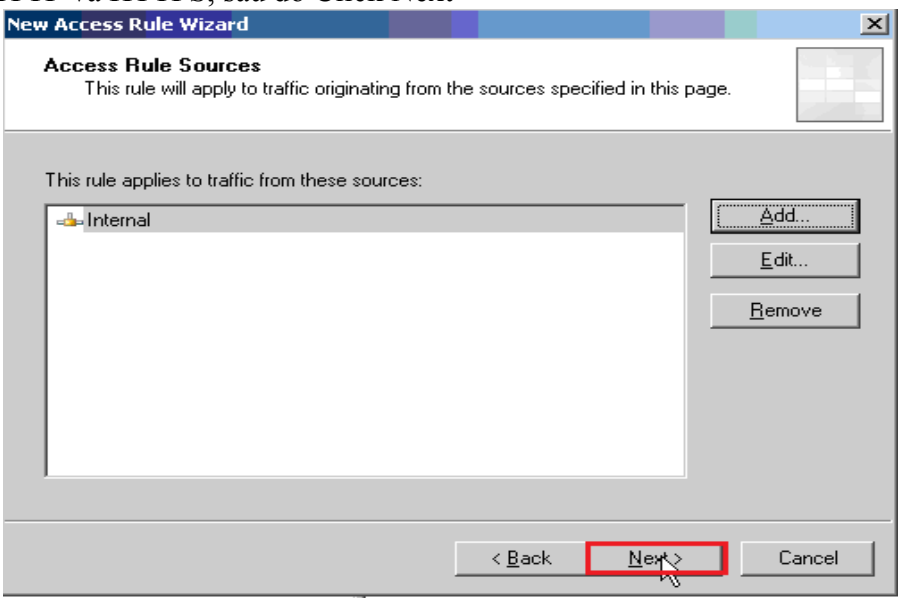
Điền tên Access Rule, sau đó Click Next



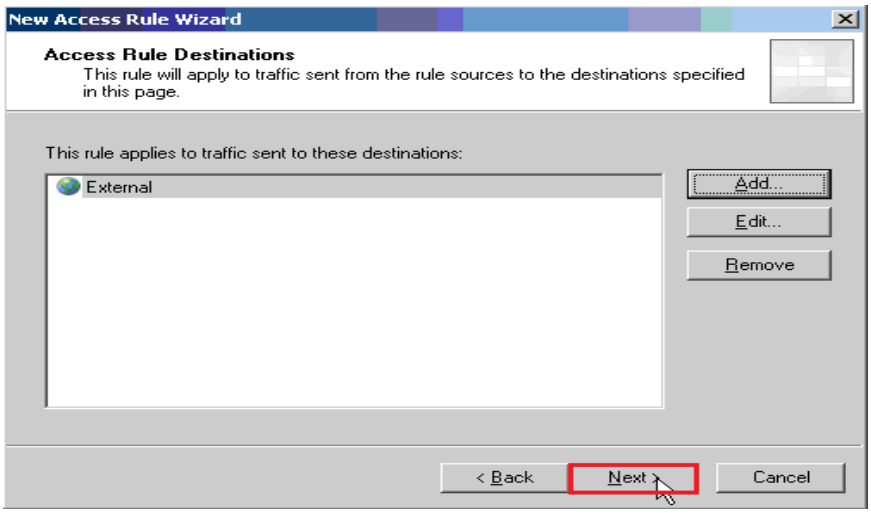
Chọn Allow, sau đó Click Next



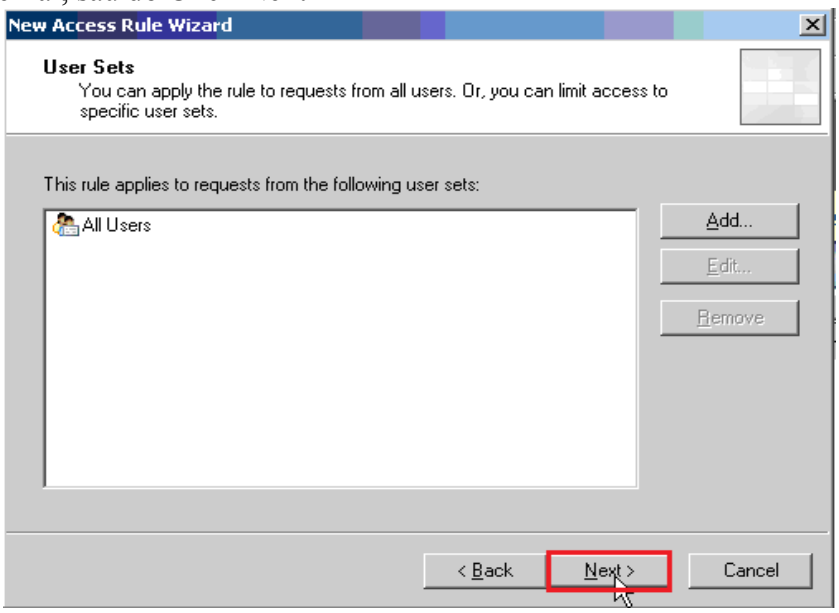
Add HTTP và HTTPS, sau đó Click Next



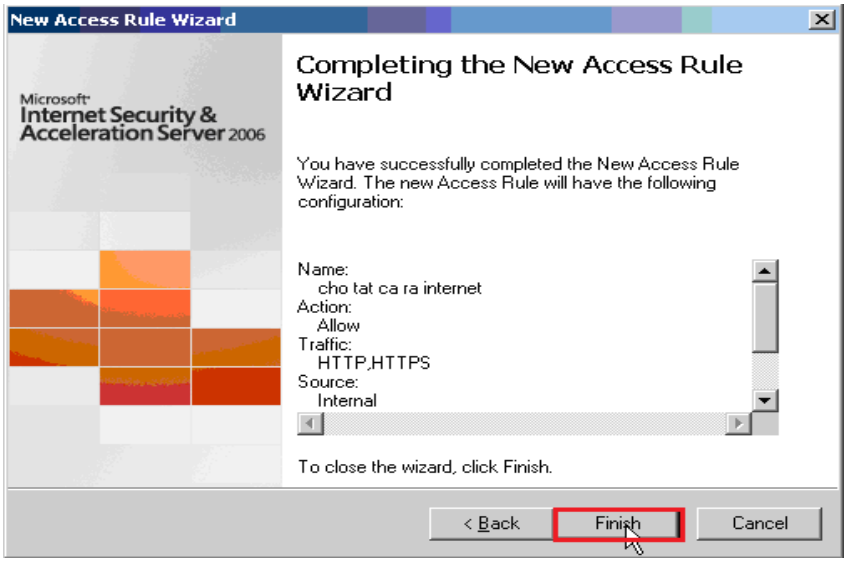
Add Internal, sau đó Click Next



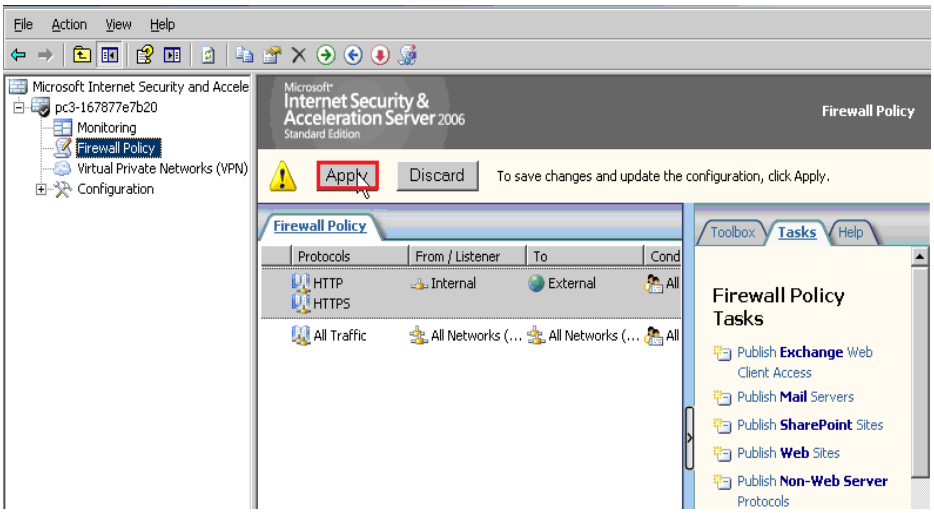
Add External, sau đó Click Next



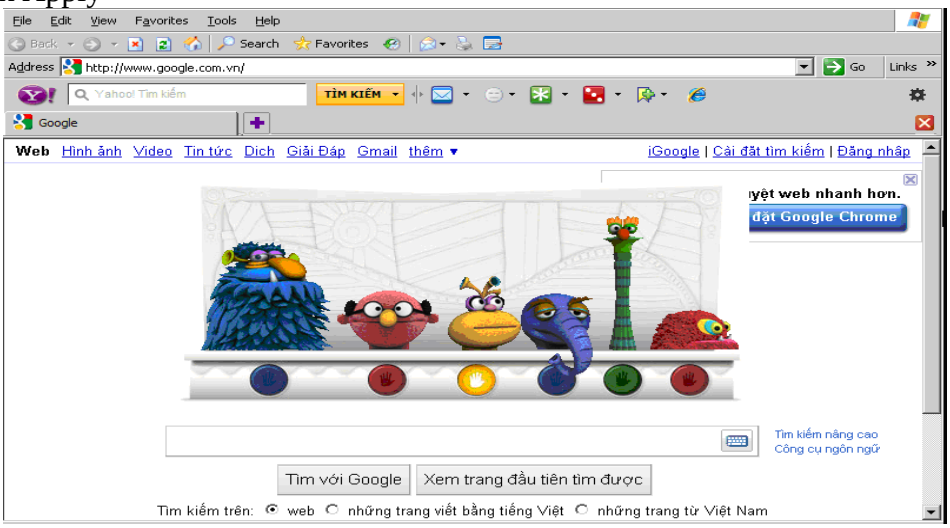
Click Next



Click Finish

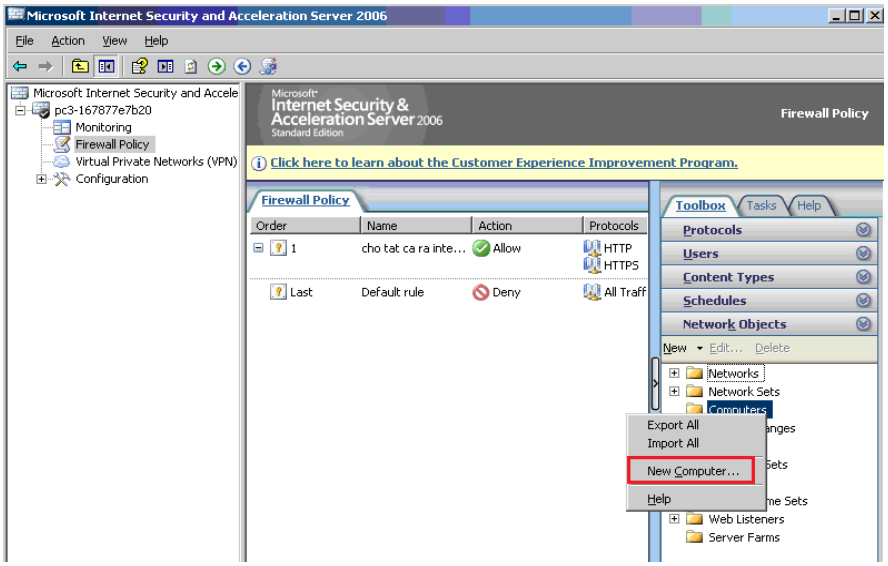


Click Apply

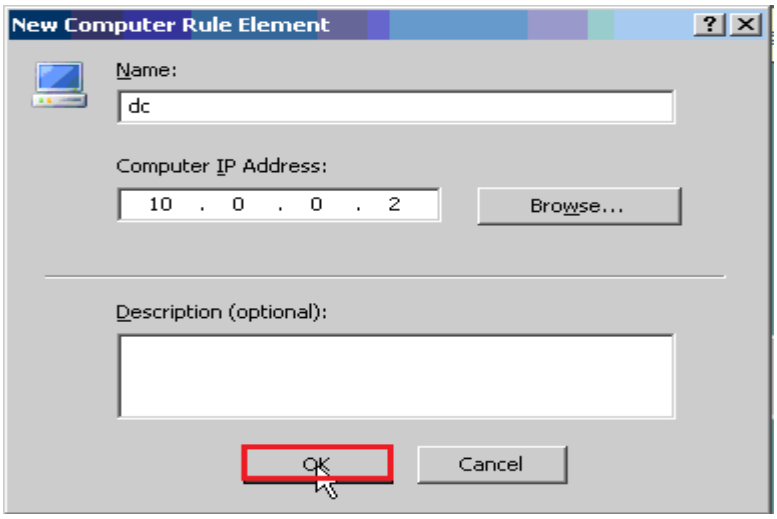


Vào máy DC trên thanh Address gõ http://google.com.vn

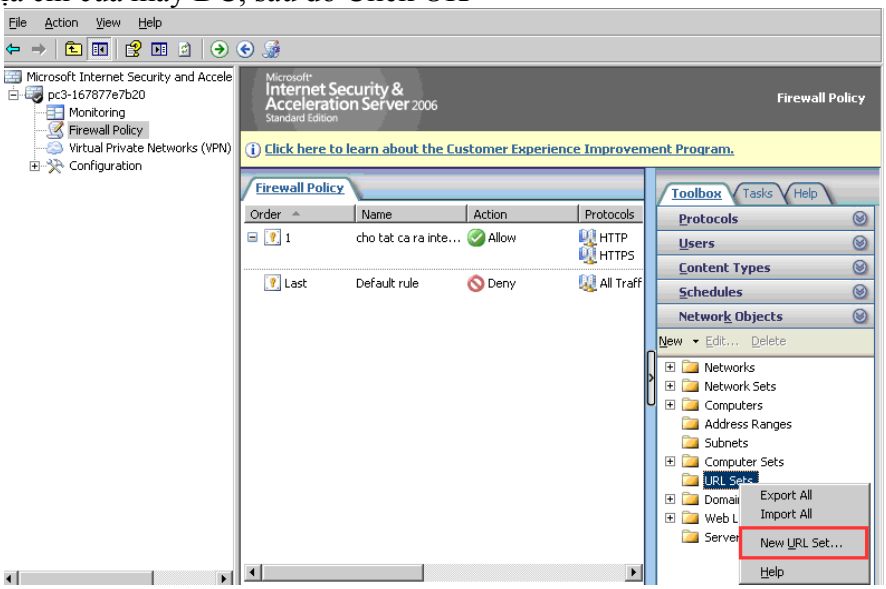
5.2. Cấm máy truy cập vào trang Web ngoisao.net



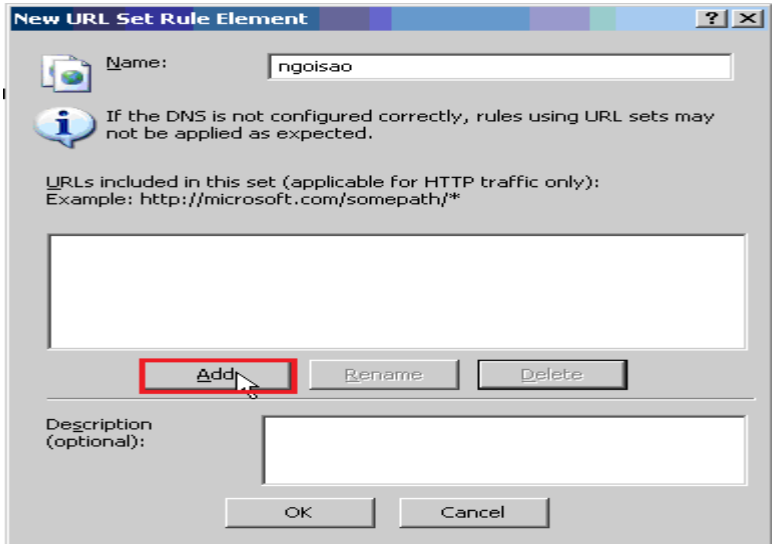
R_Click Computer\New Computer



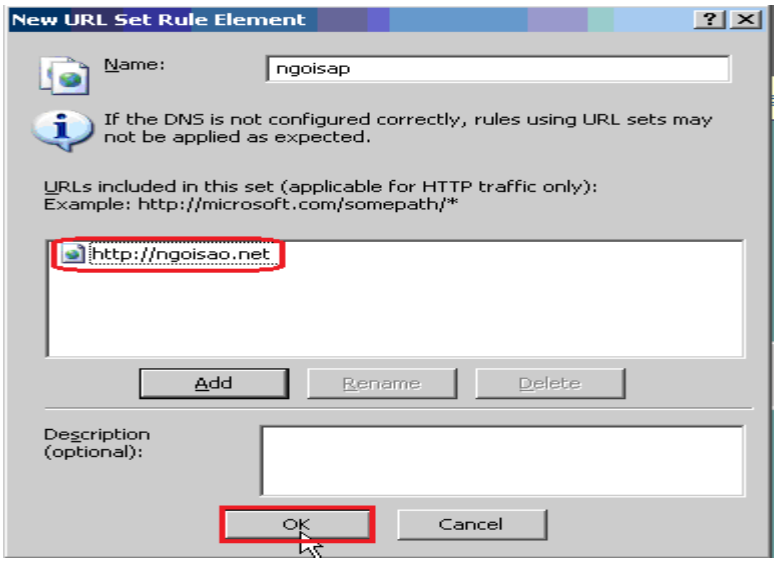
Điền địa chỉ của máy DC, sau đó Click OK



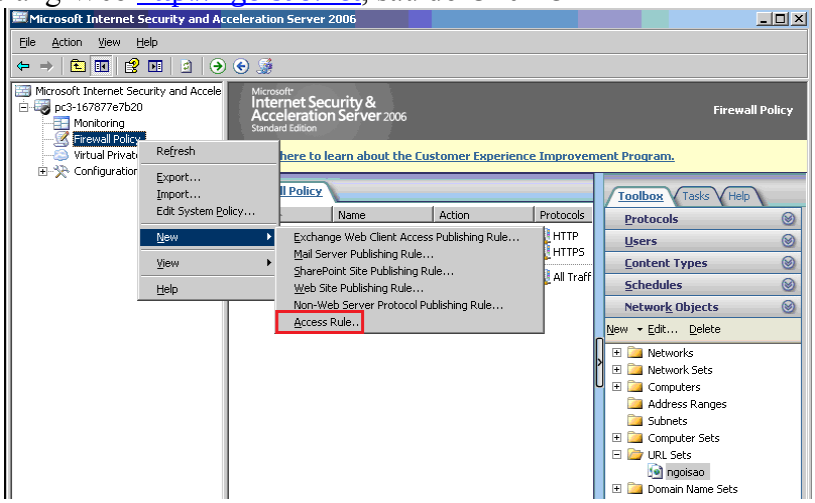
R_Click URL Sets\New URL Set…



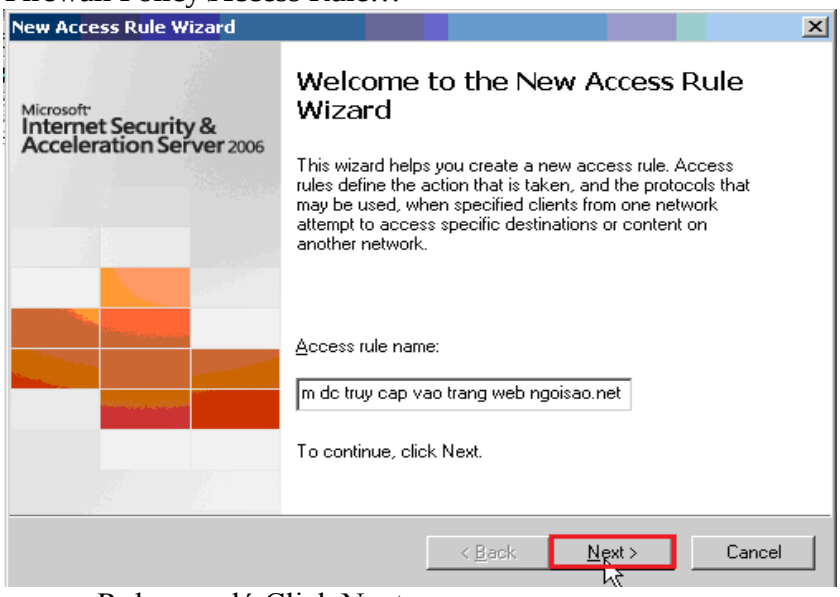
Click Add



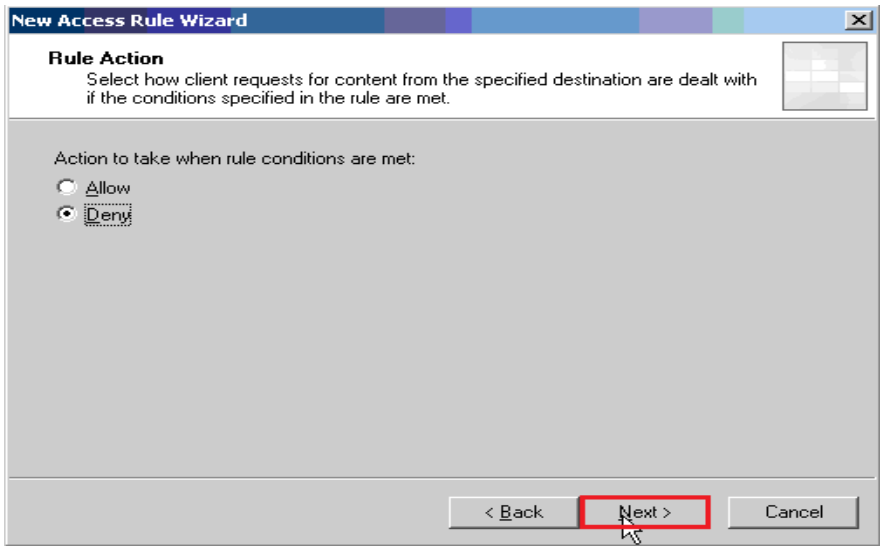
Điền tên trang Web http://ngoisao.net, sau đó Click OK



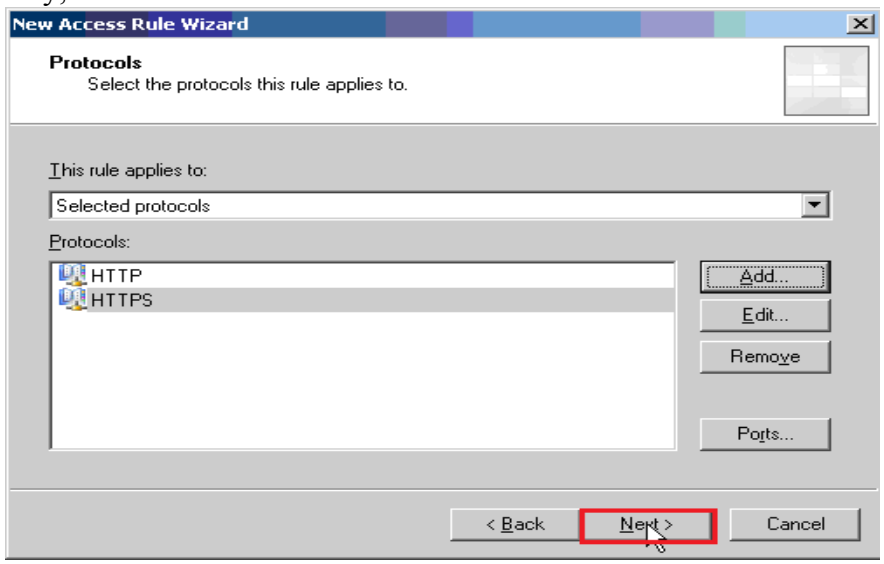
R_Click Firewall Policy\Access Rule…



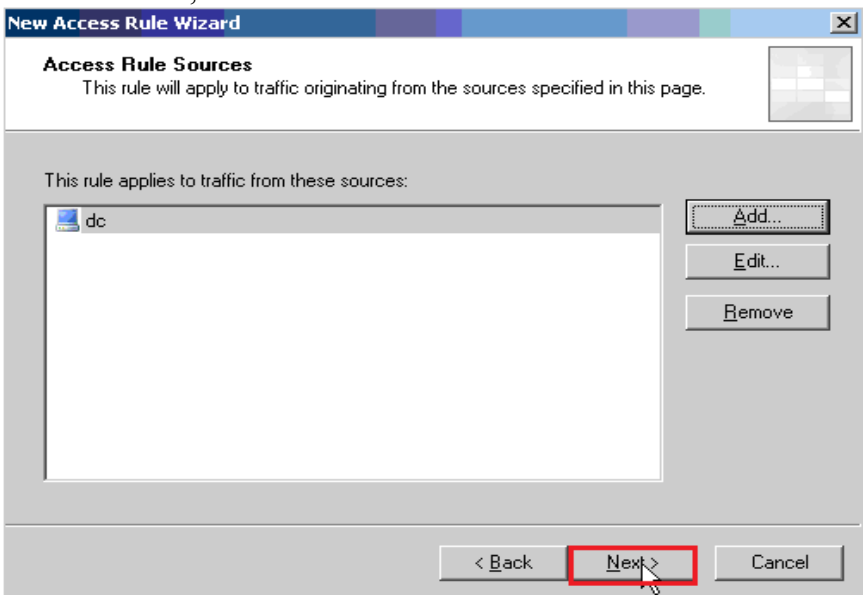
Điền tên access Rule, sau đó Click Next



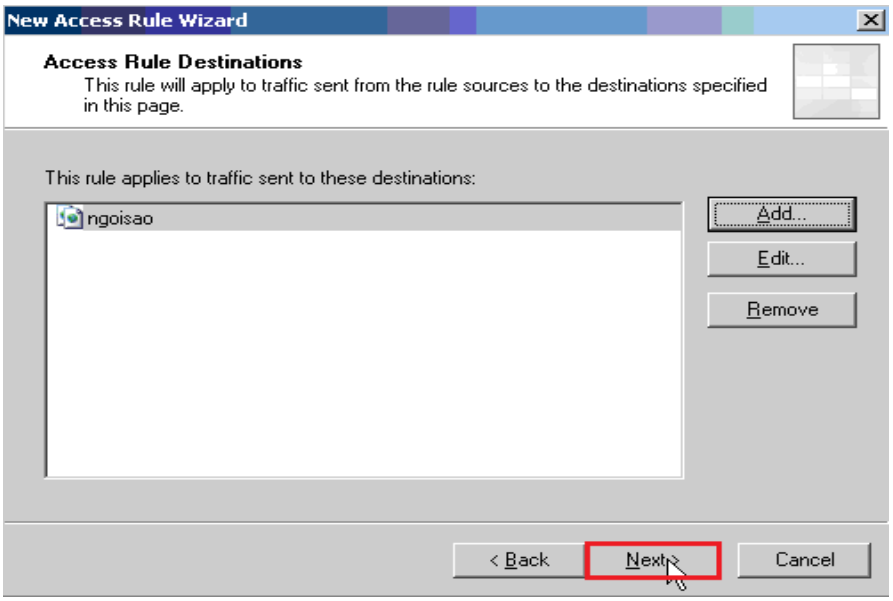
Chọn Deny, sau đó Click Next



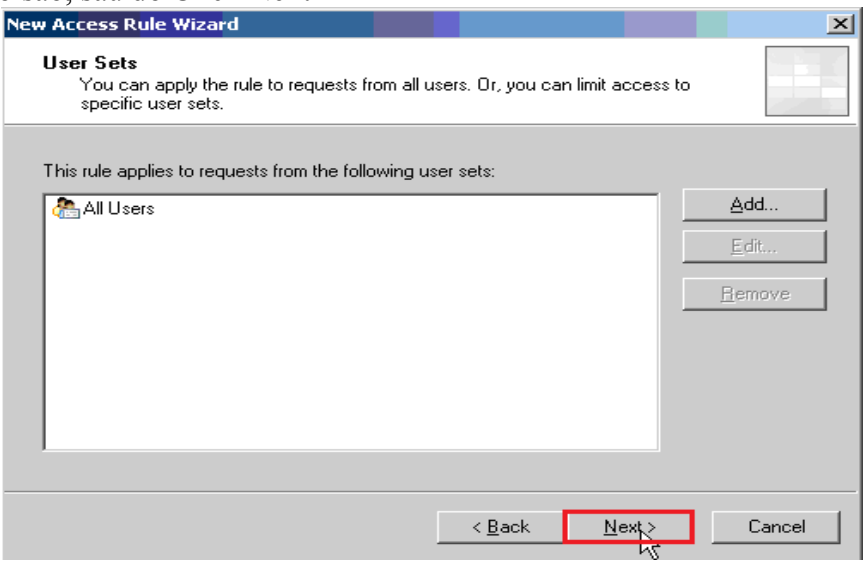
Add HTTP và HTTPS, sau đó Click Next



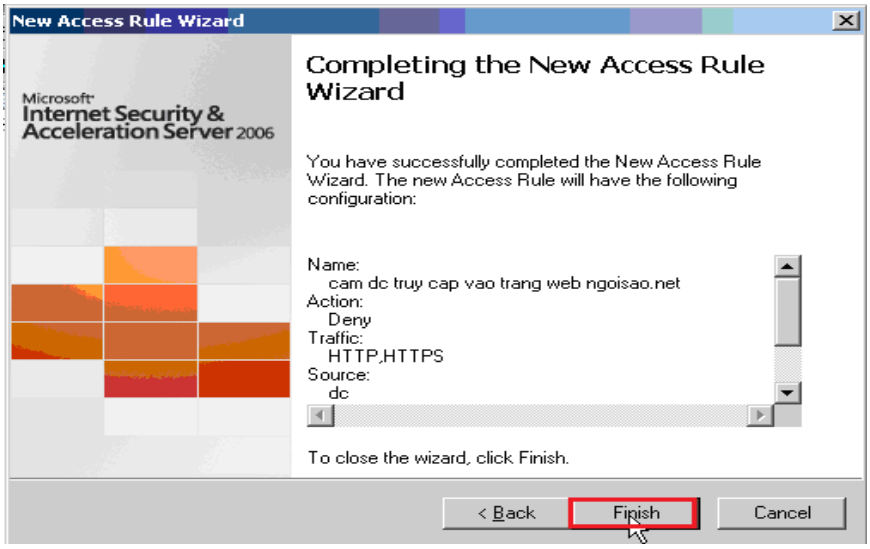
Add DC, sau đó Click Next



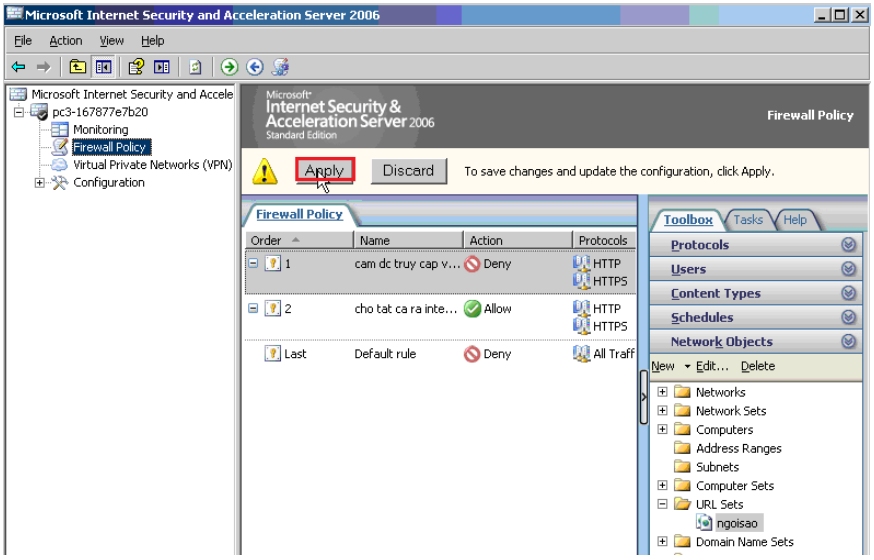
Add ngoisao, sau đó Click Next



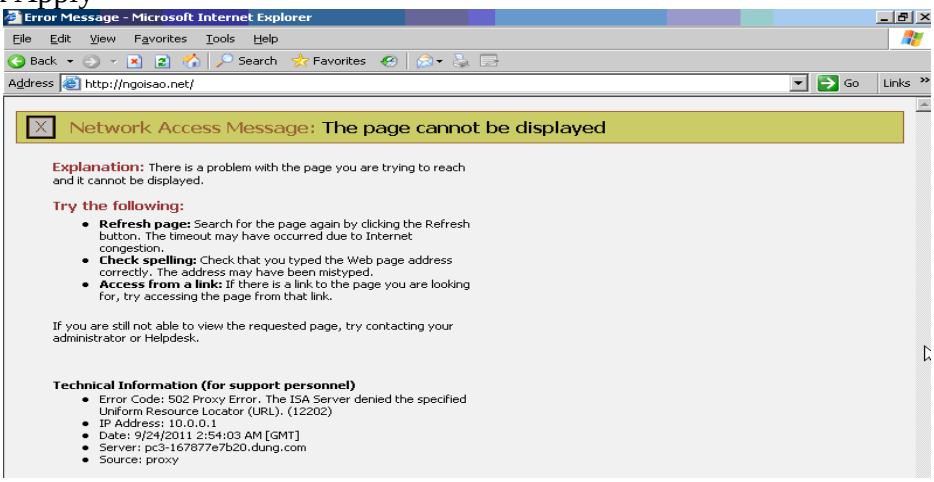
Click Next



Click Finish

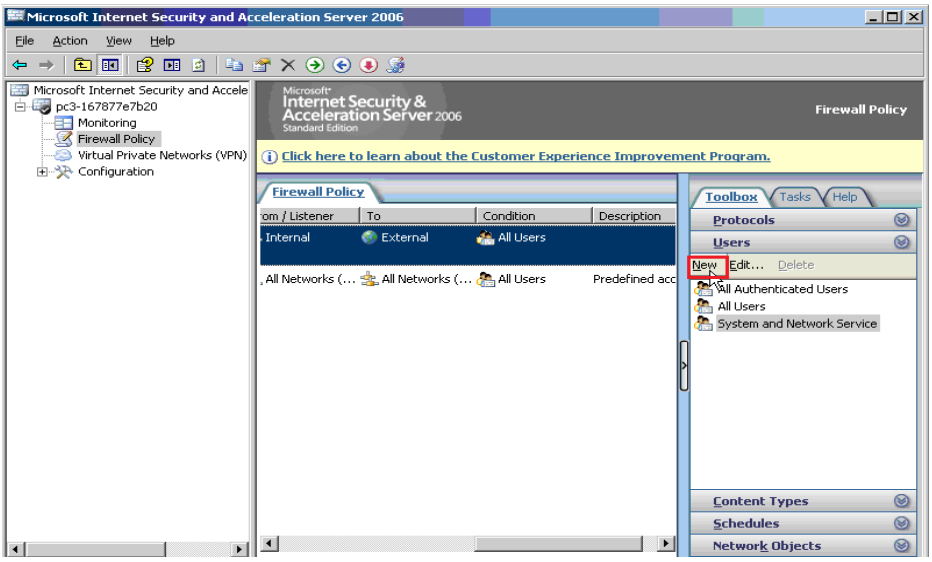


Click Apply

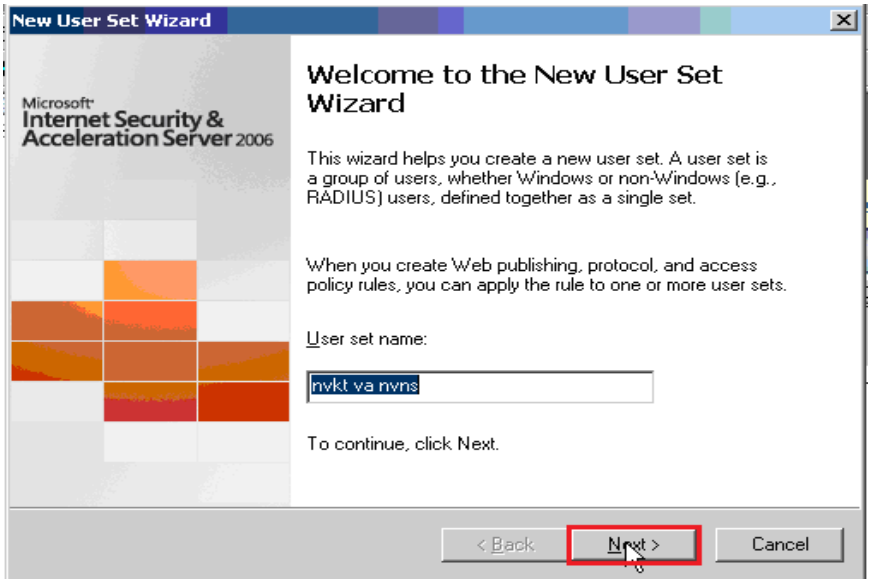


Vào máy DC trên thanh Address gõ http://ngoisao.net

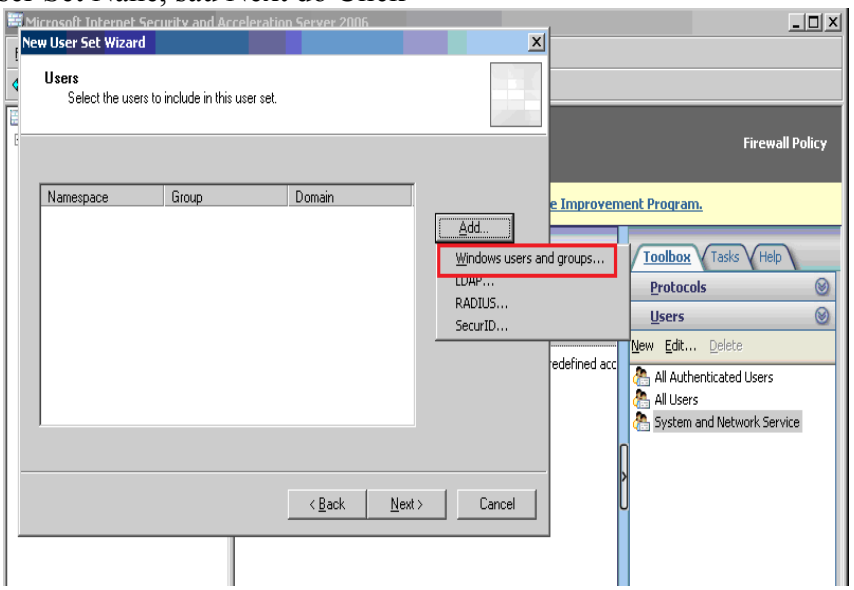
5.3. Cấm User nvkt và nvns ra ngoài internet trong giờ làm việc



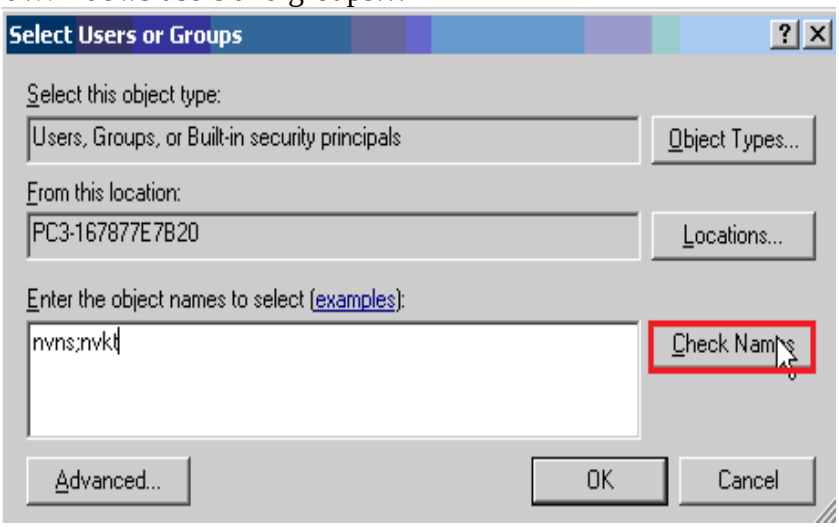
Click New



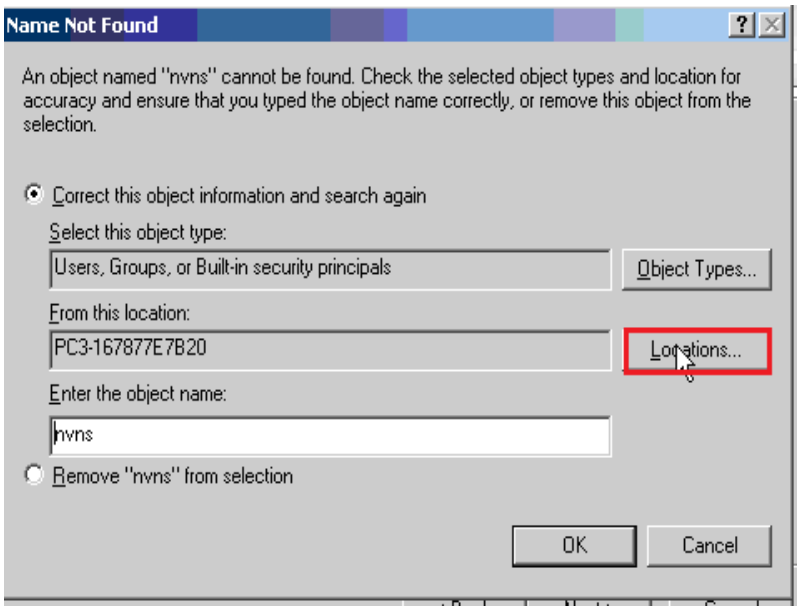
Điền User Set Nane, sau Next đó Click



Click Add\Windows users and groups…

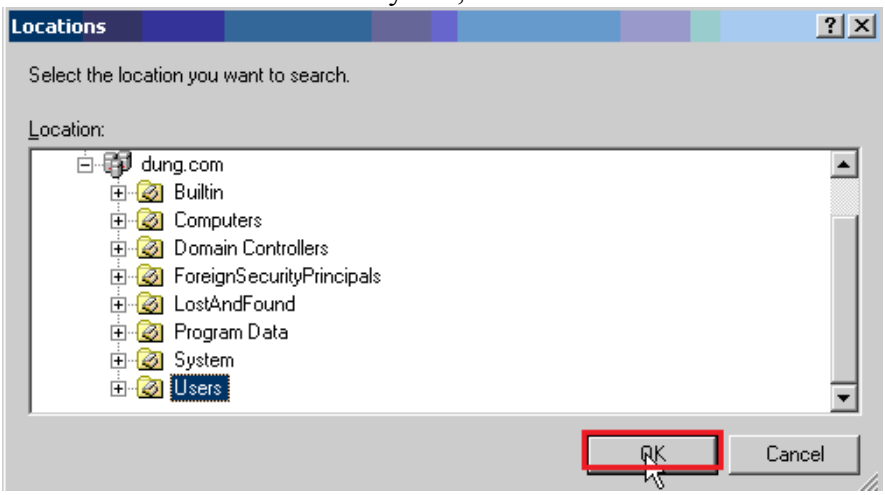


Điền tên User, sau đó Click Check Name

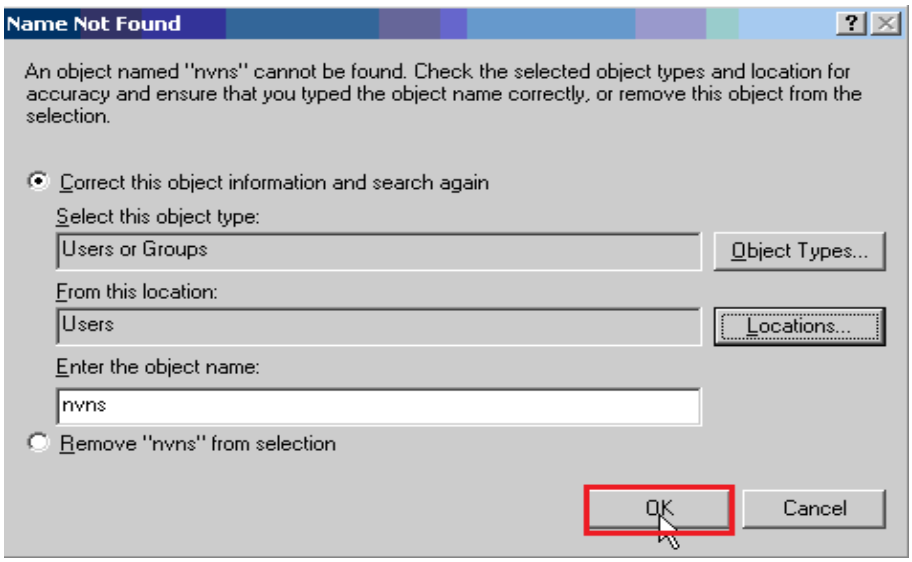


Click Locations…

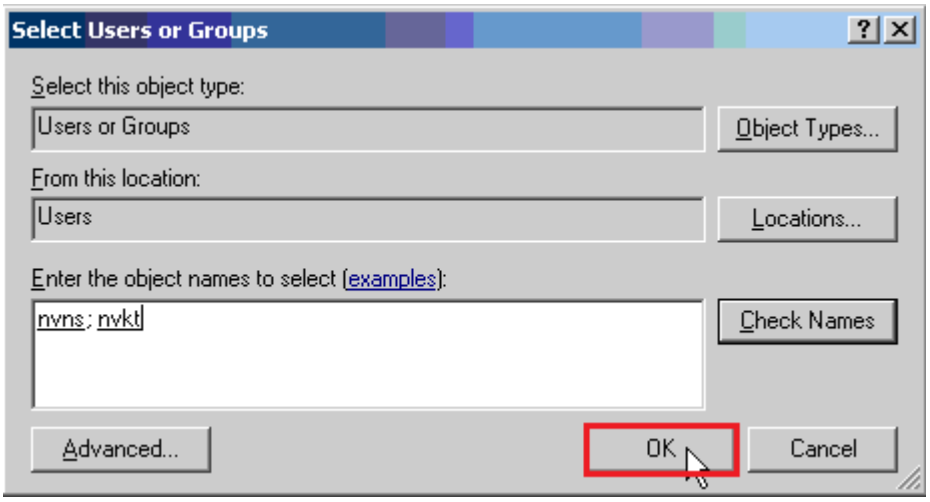
Điền User name và Password của máy DC, sau đó Click OK



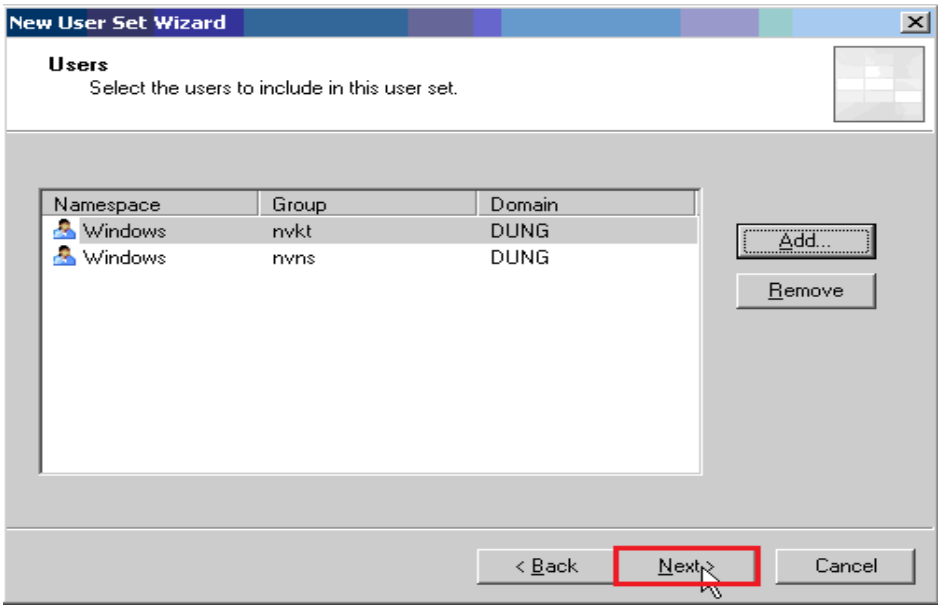
Click OK



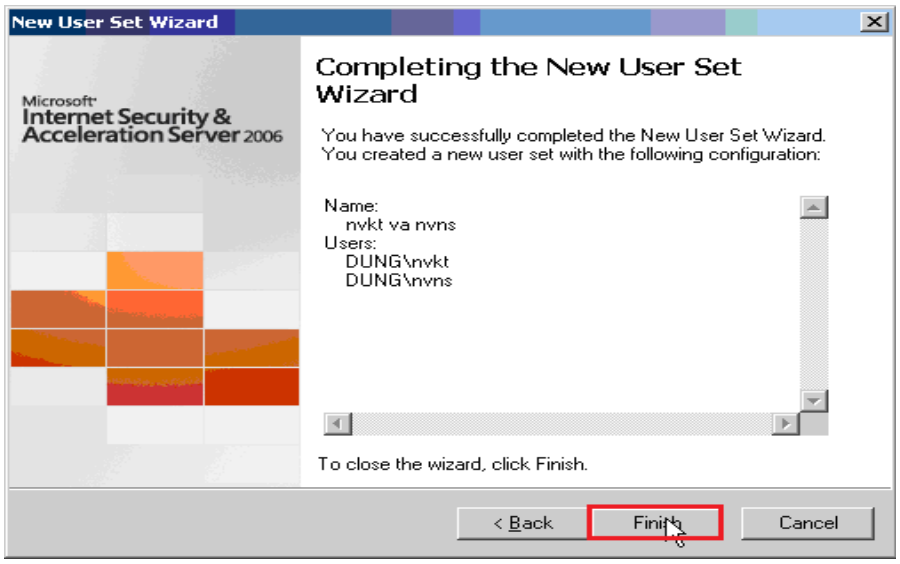
Click OK



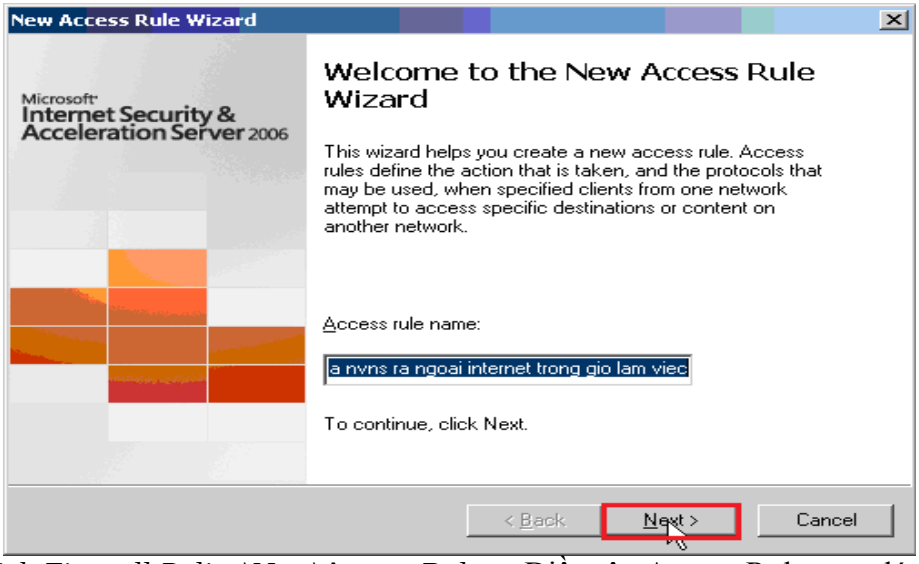
Click OK



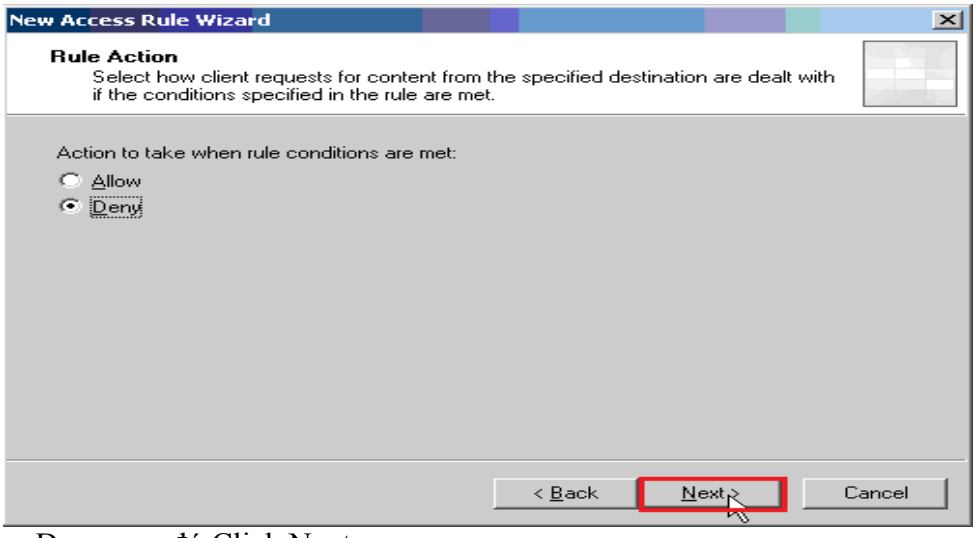
Chọn next



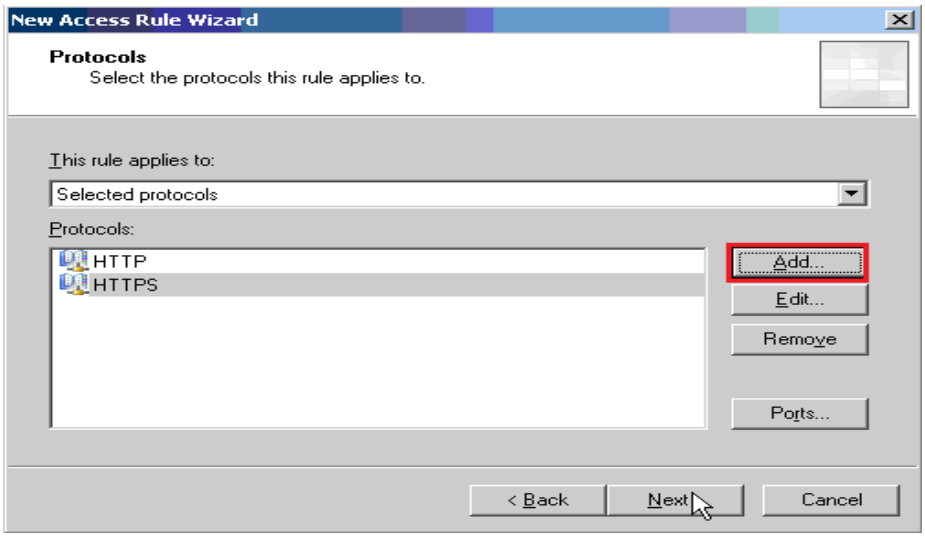
Chọn Finish



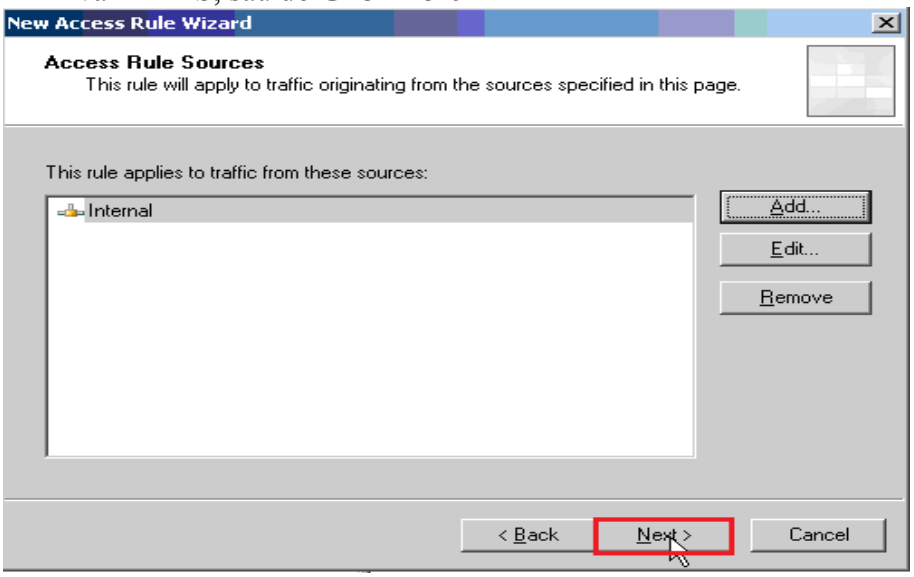
R_Click Firewall Policy\New\Access Rule… Điền tên Access Rule, sau đó Click Next



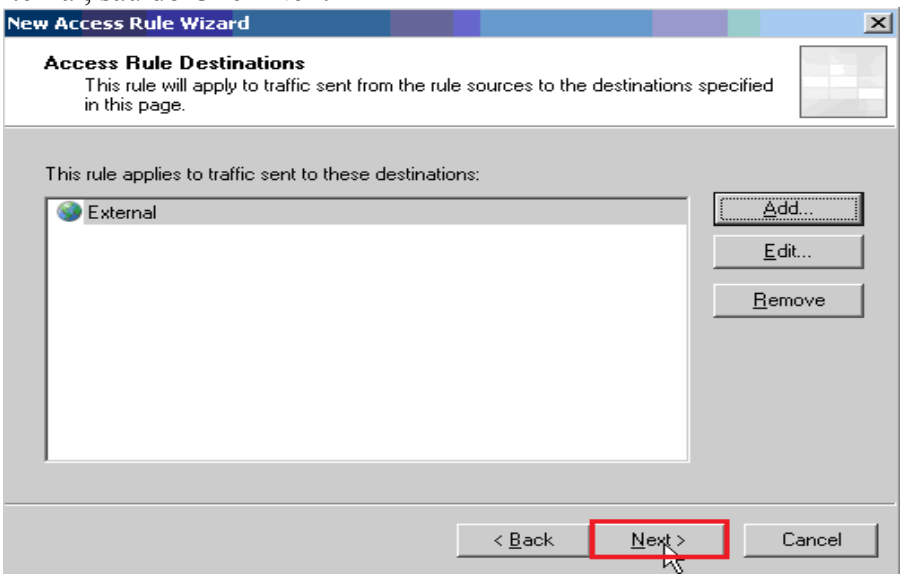
Chọn Deny, sau đó Click Next



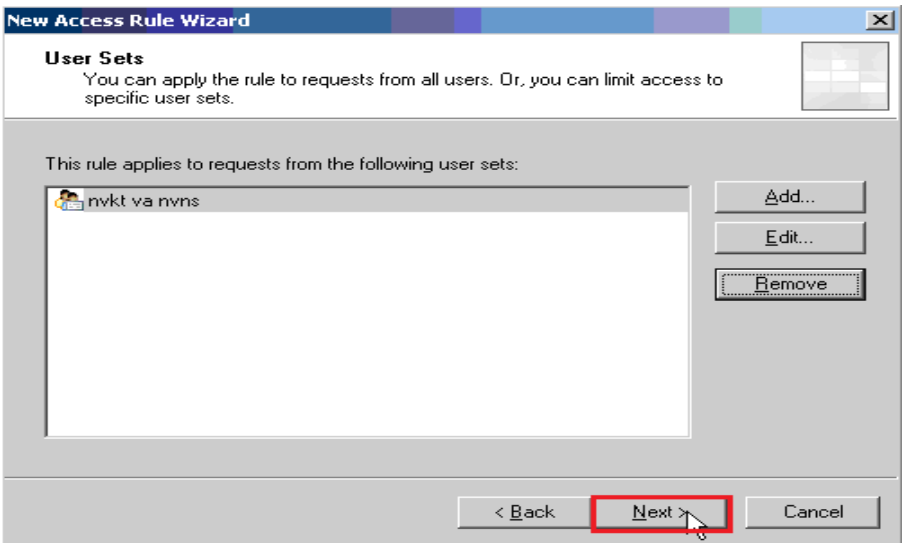
Add HTTP và HTTPS, sau đó Click Next



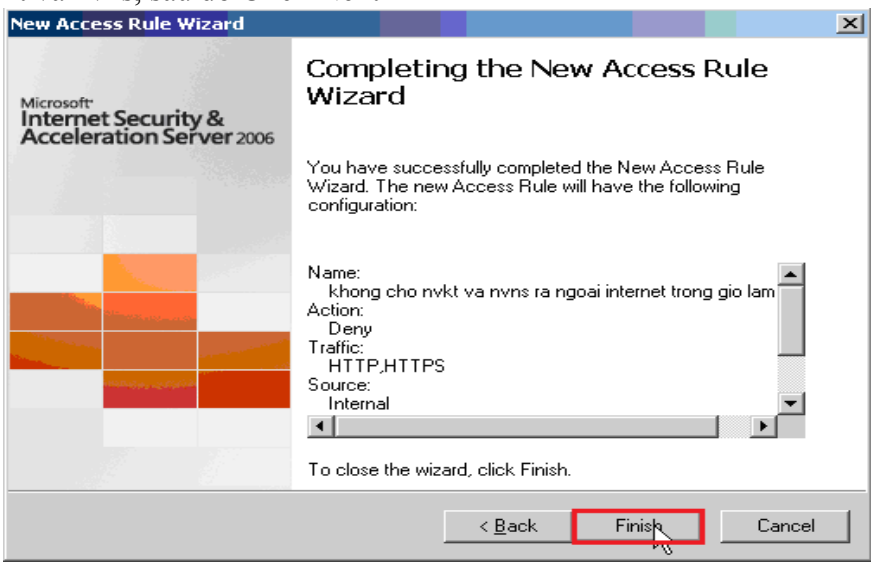
Add Internal, sau đó Click Next



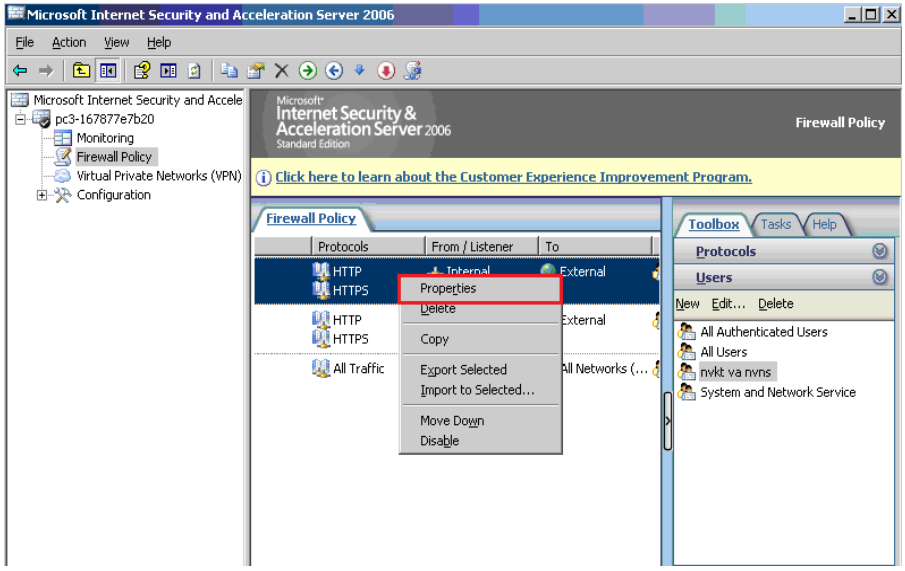
Add External, sau đó Click Next



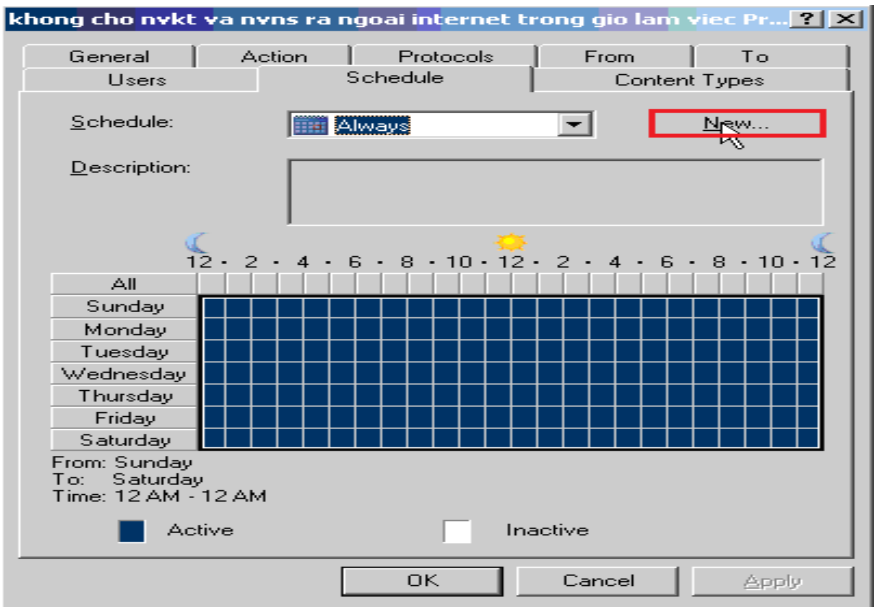
Add nvkt va nvns, sau đó Click Next



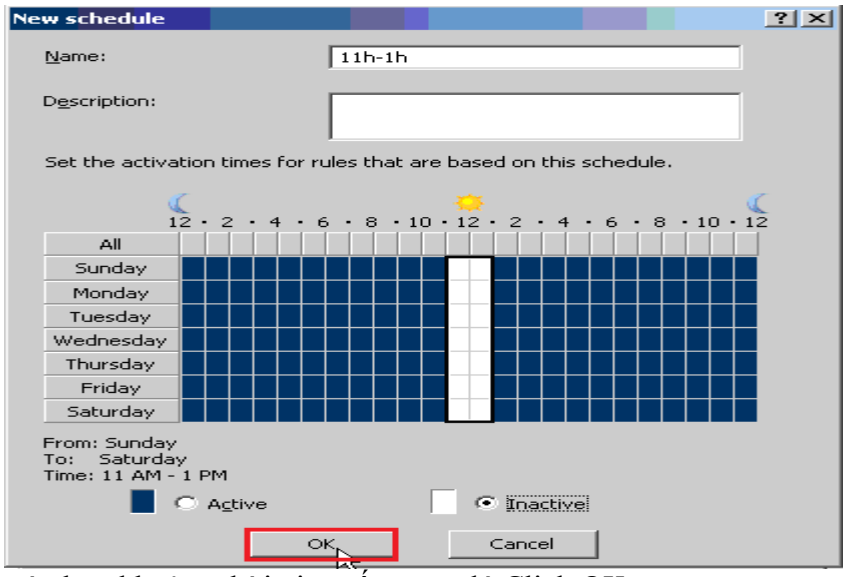
Click Finish



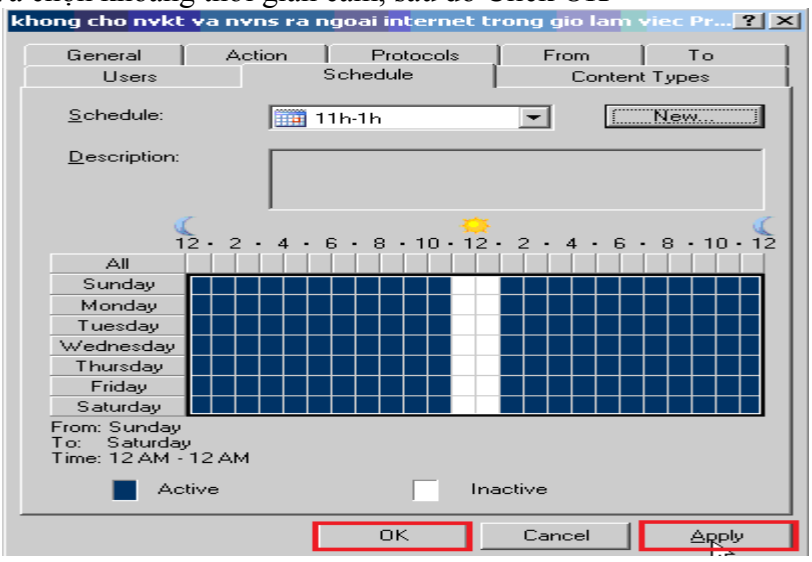
R_Click Rule vừa xet\ Properties



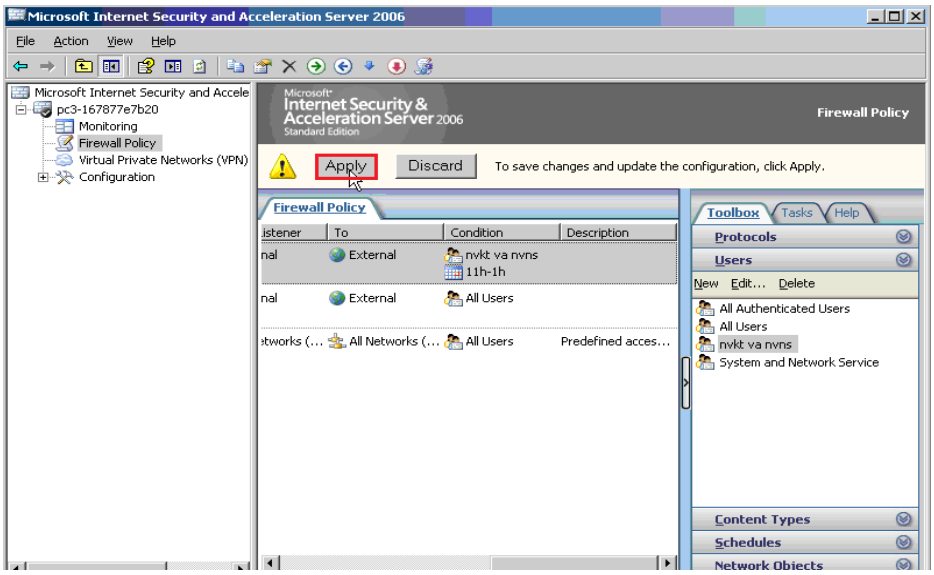
Click New



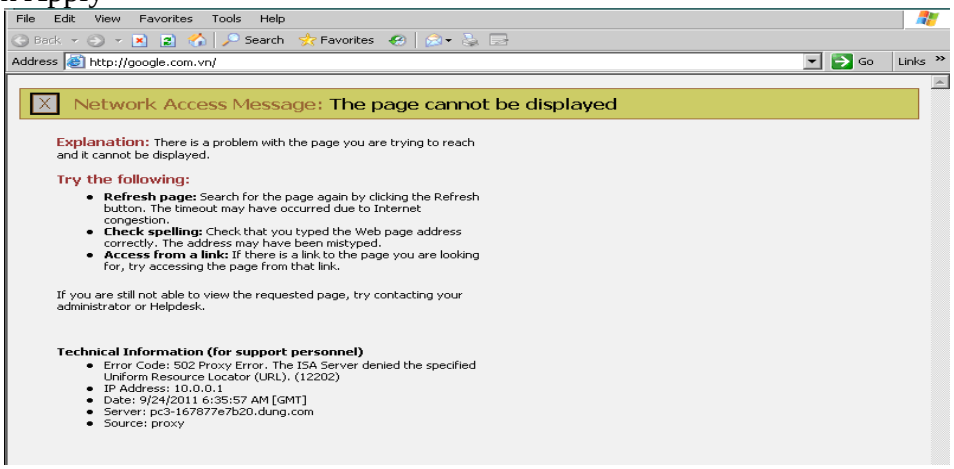
Điên tên và chọn khoảng thời gian cấm, sau đó Click OK



Click Apply\OK

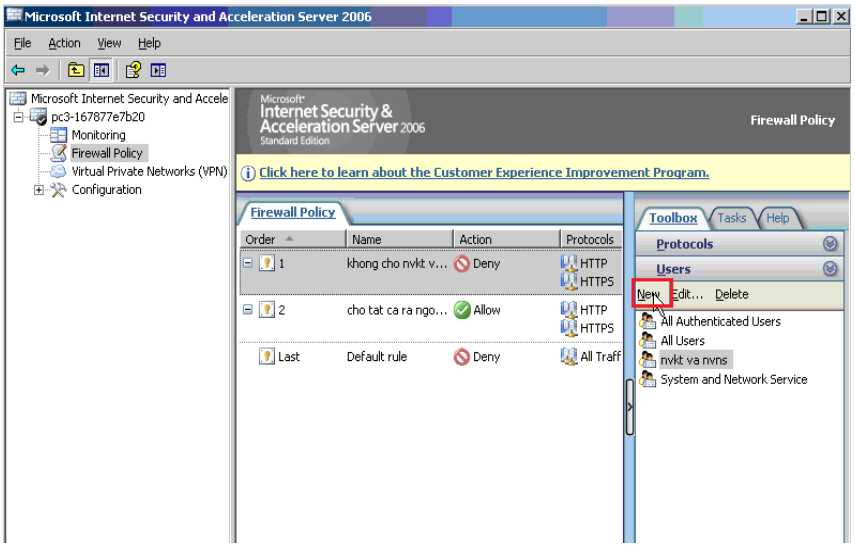


Click Apply

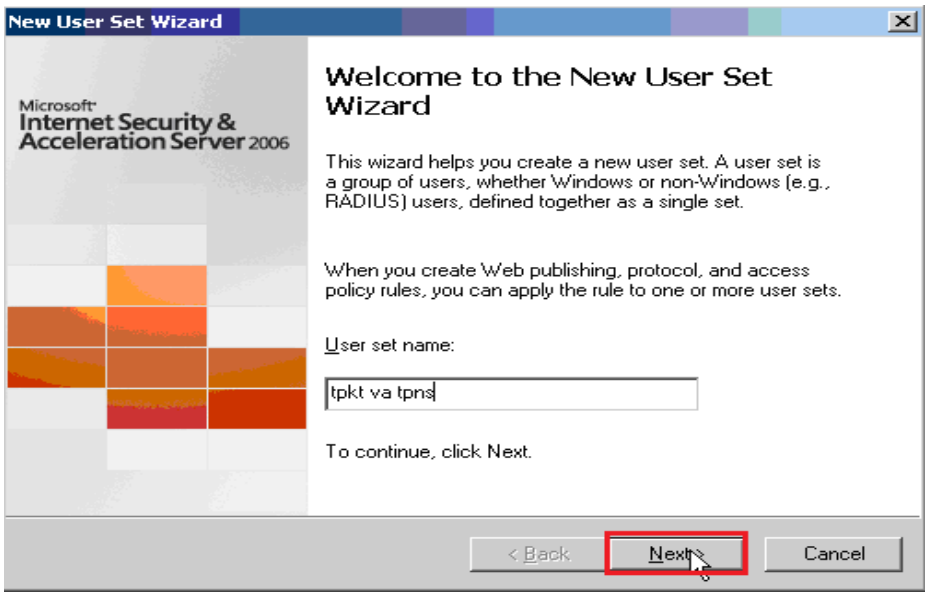


Logon User nvkt và nvns ra ngoài Inernet không được

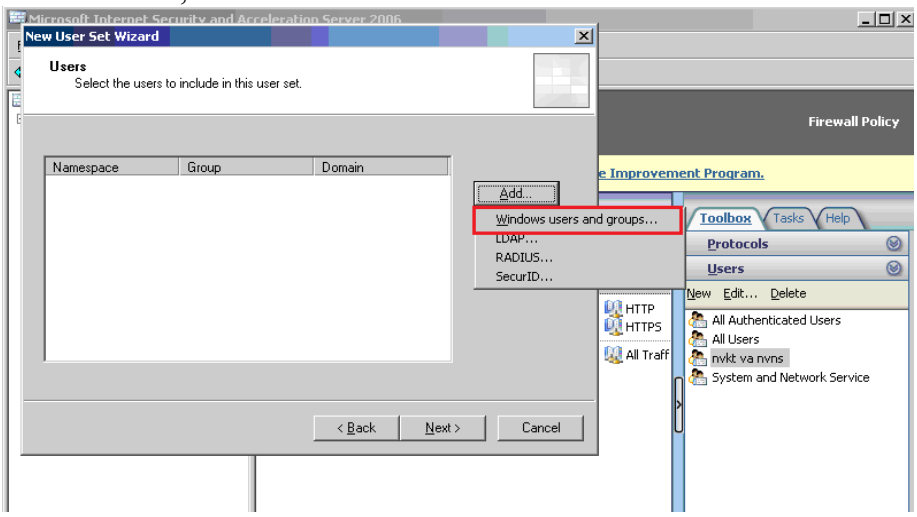
5.4. Tpkt và tpns ra ngoài internet nhưng không nhìn thấy hình và không cho download file .rar



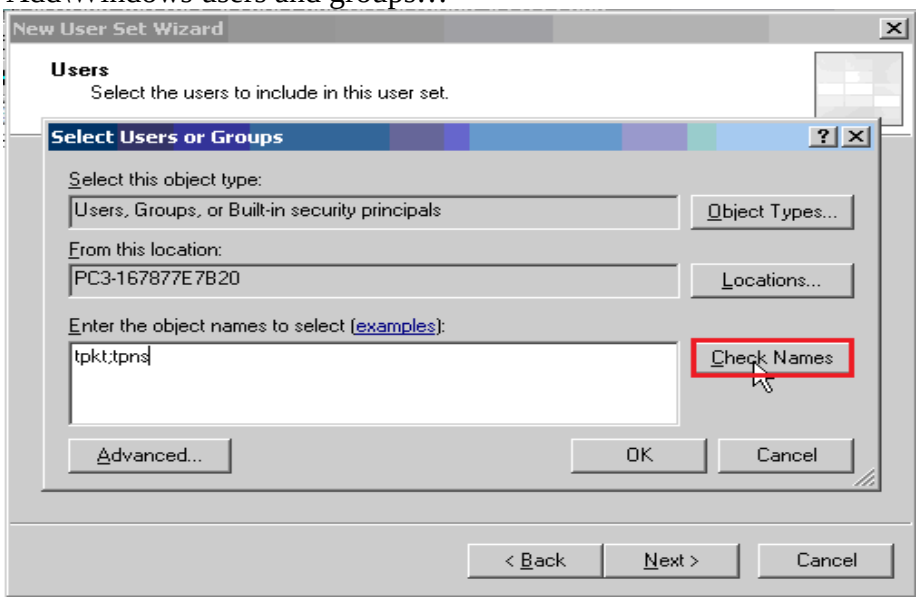
Click New



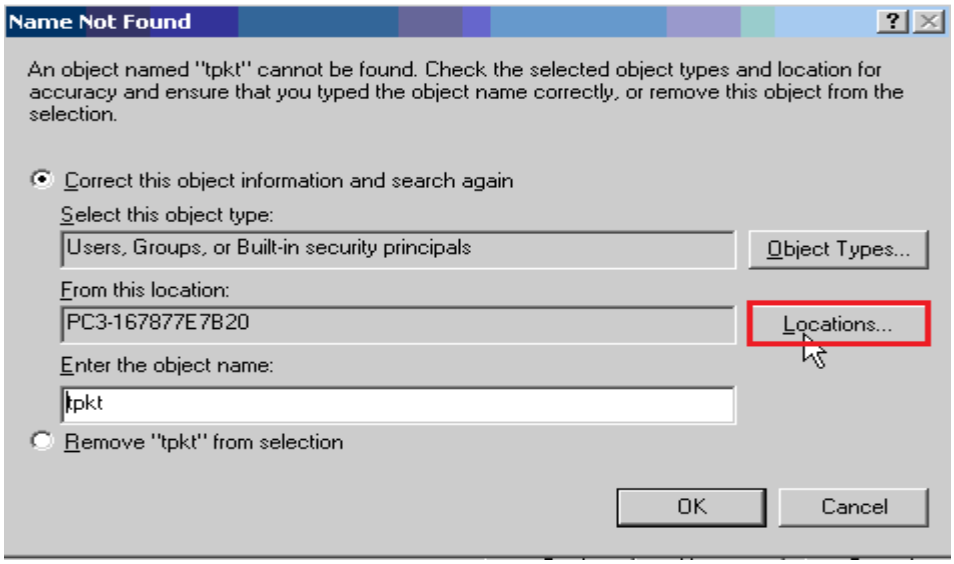
Điền User set name, sau đó Click Next



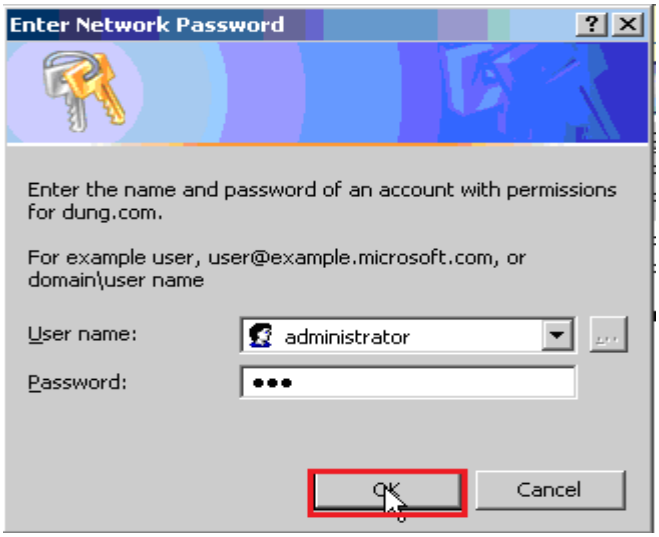
Click Add\Windows users and groups…



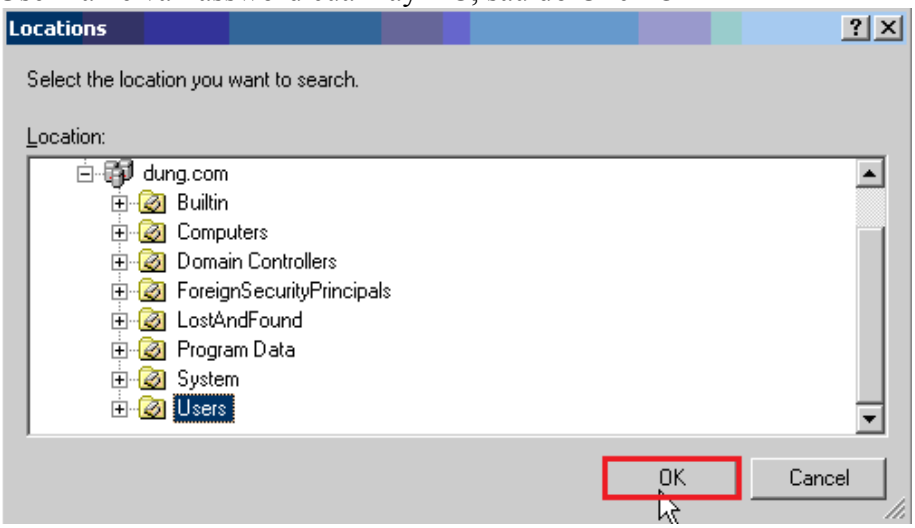
Điền tên User , sau đó Click Check Names



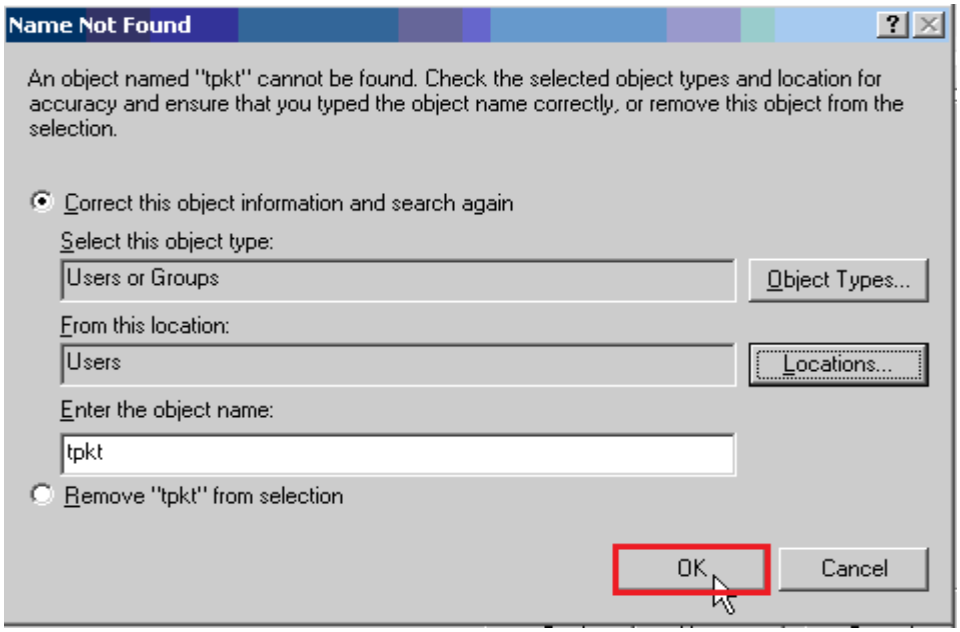
Click Locations…



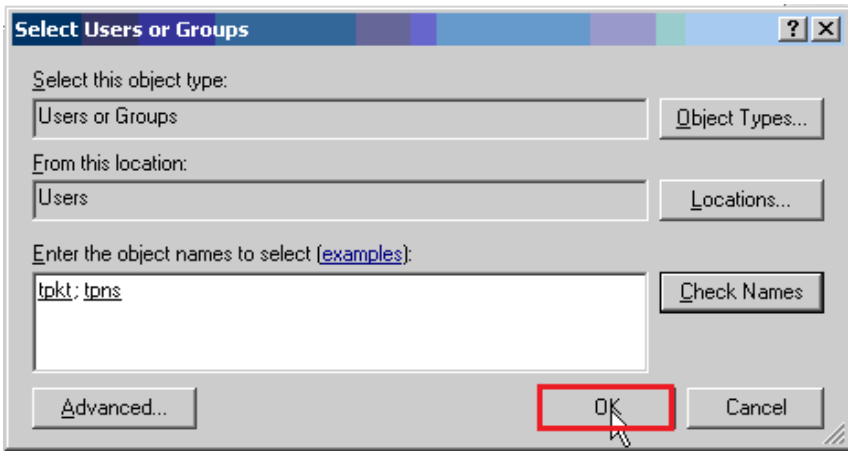
Điền User name và Password của máy DC, sau đó Click OK



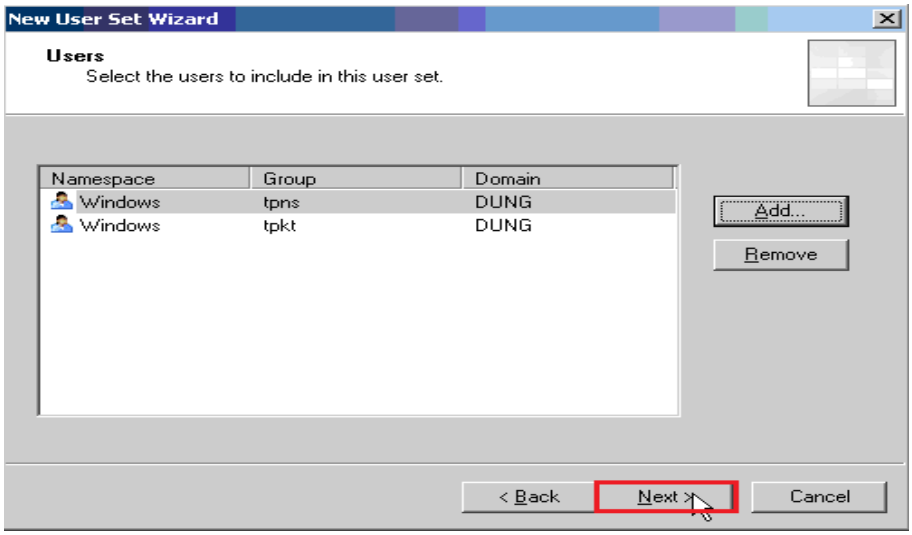
Click OK



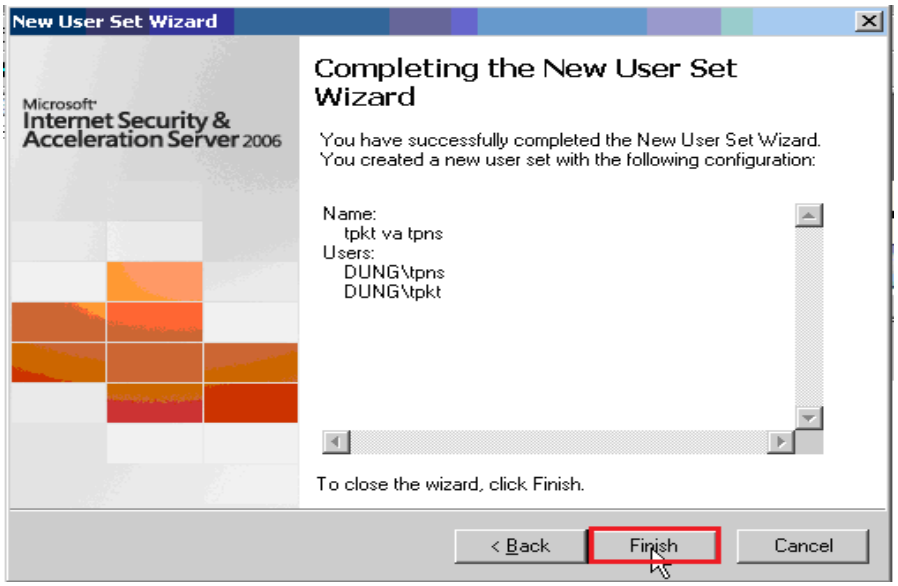
Click OK



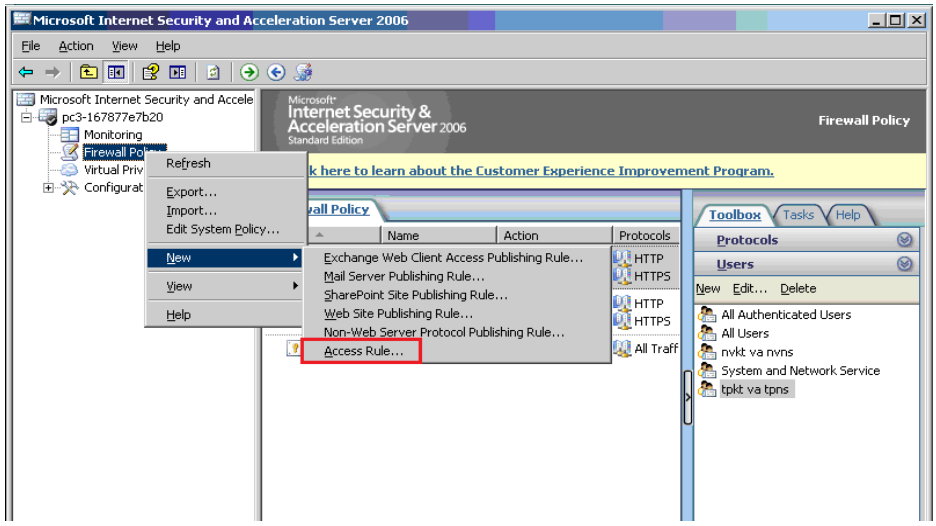
Click OK



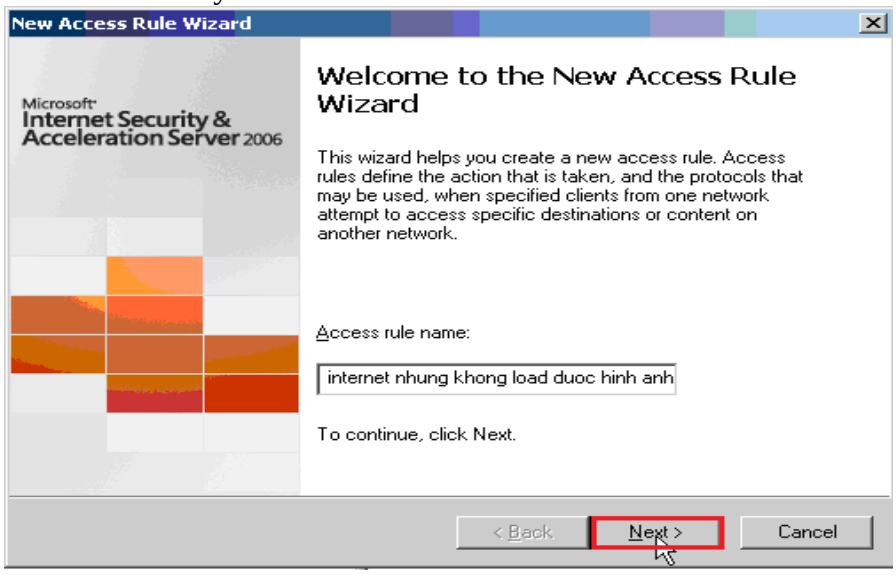
Click Next



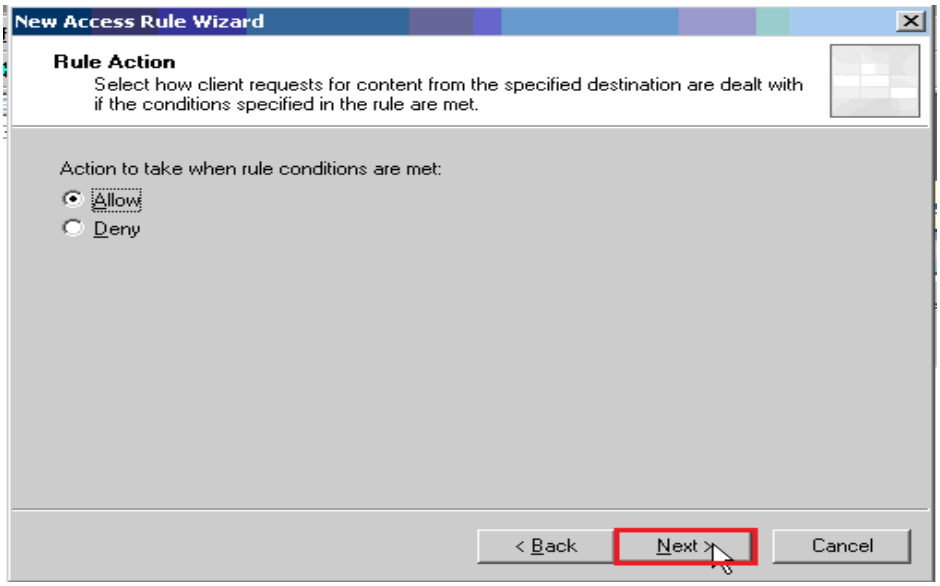
Click Finish



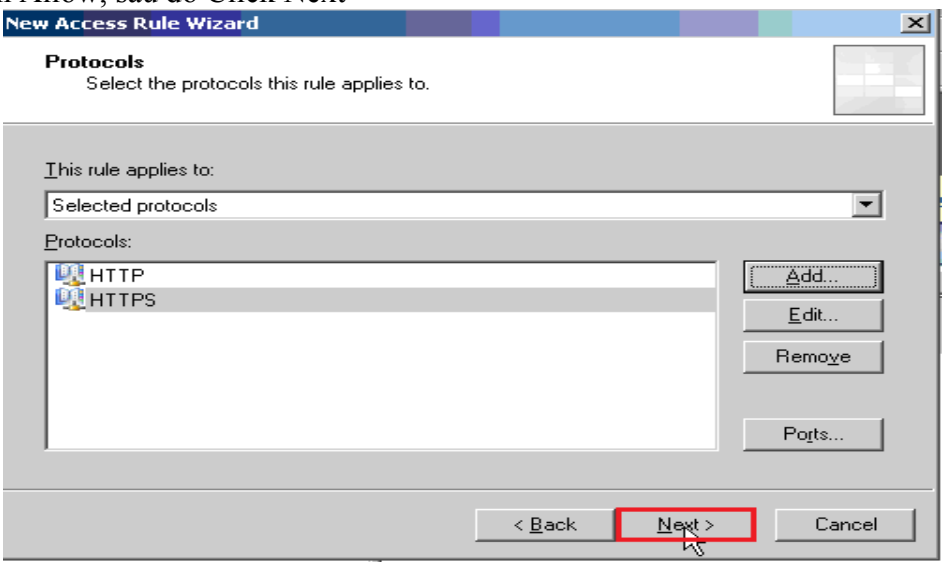
R_Click Firewall Policy\New\Access Rule…



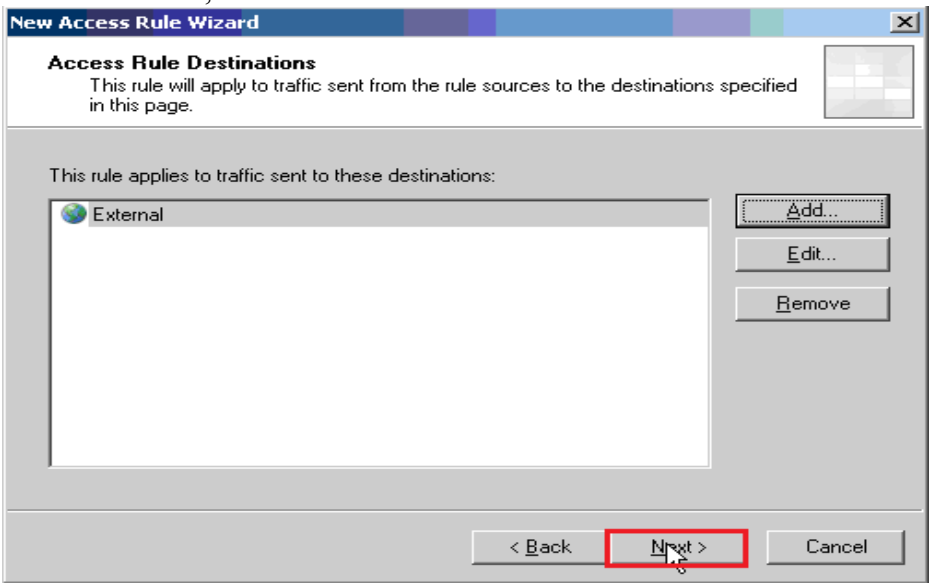
Điền tên Access Rule, sau đó Click Next



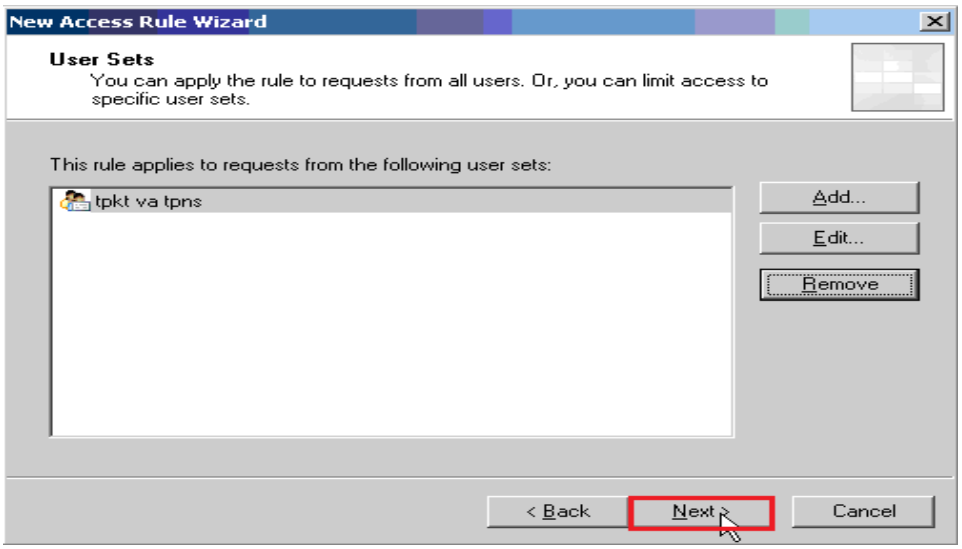
Chọn Allow, sau đó Click Next



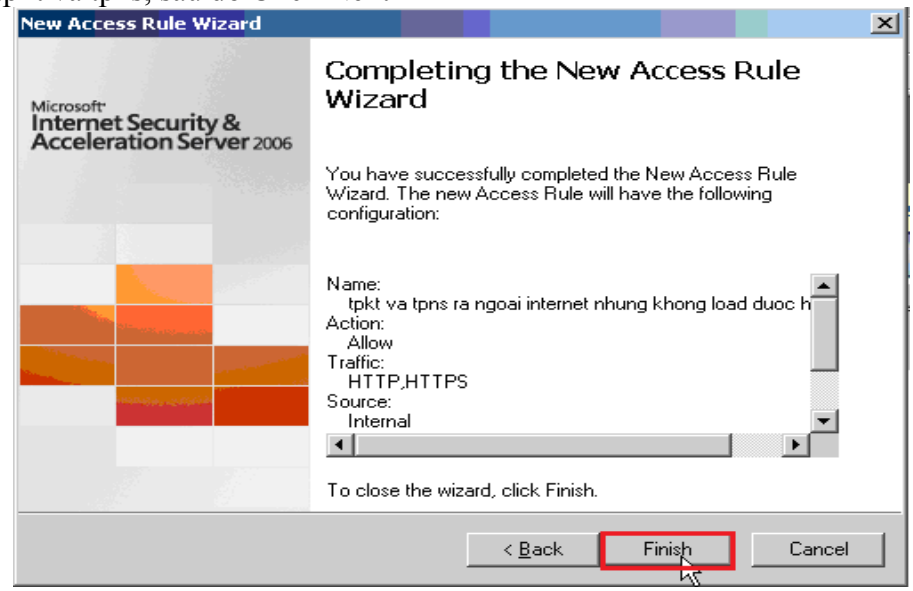
Add HTTP và HTTS, sau đó Click Next



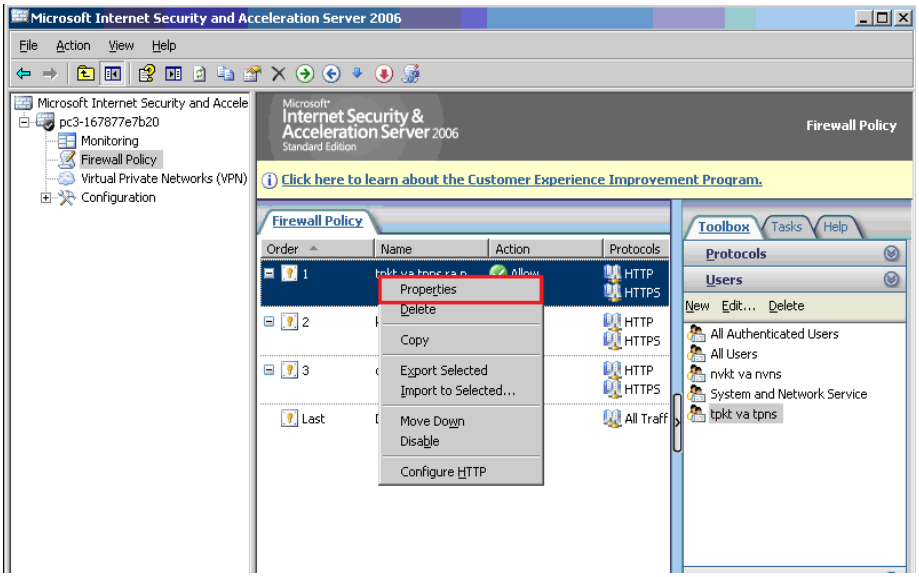
Add External, sau đó Click Next



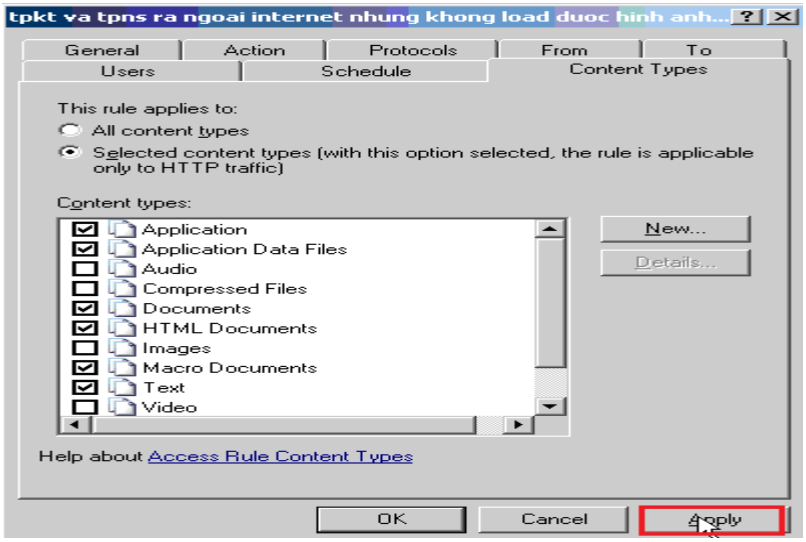
Add tpkt va tpns, sau đó Click Next



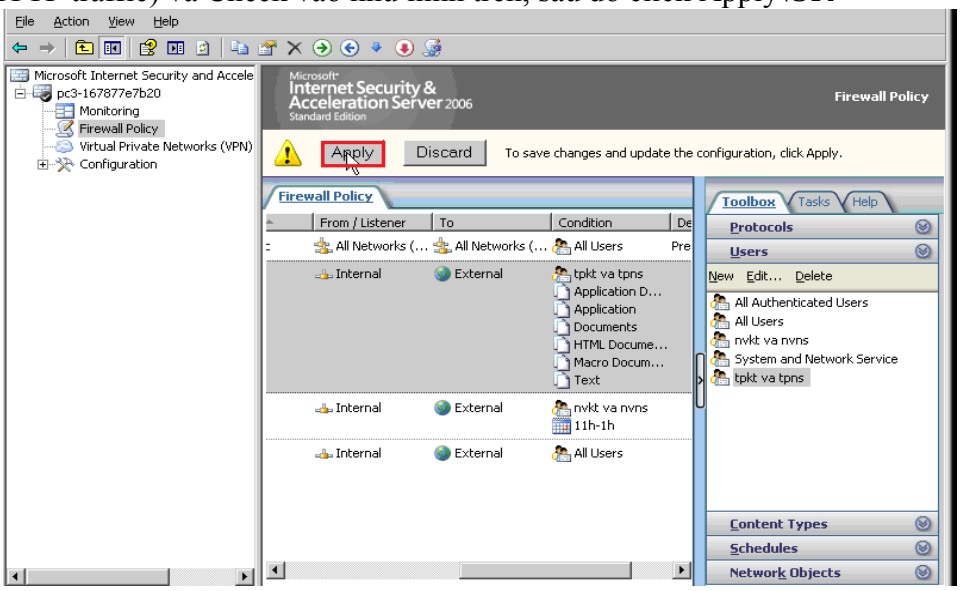
Click Finish



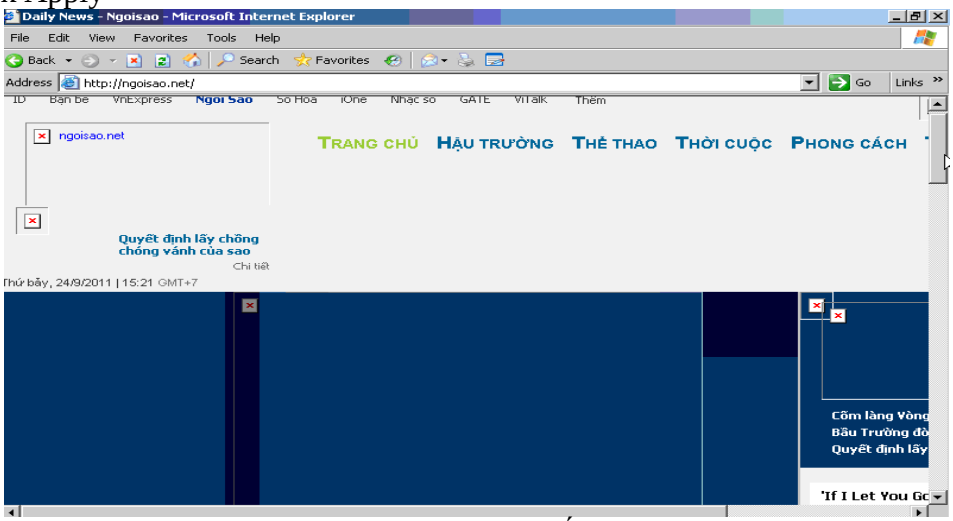
R_Click Rule vừa xét\ Properties



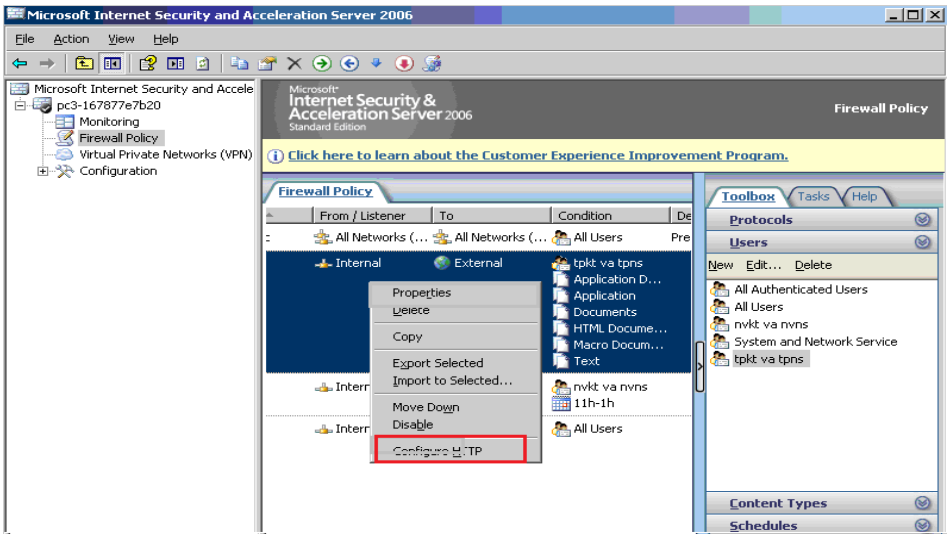
Chọn Selected content types(with this option selected, the rule is applicable only to HTTP traffic) và Check vào như hình trên, sau đó click Apply\OK



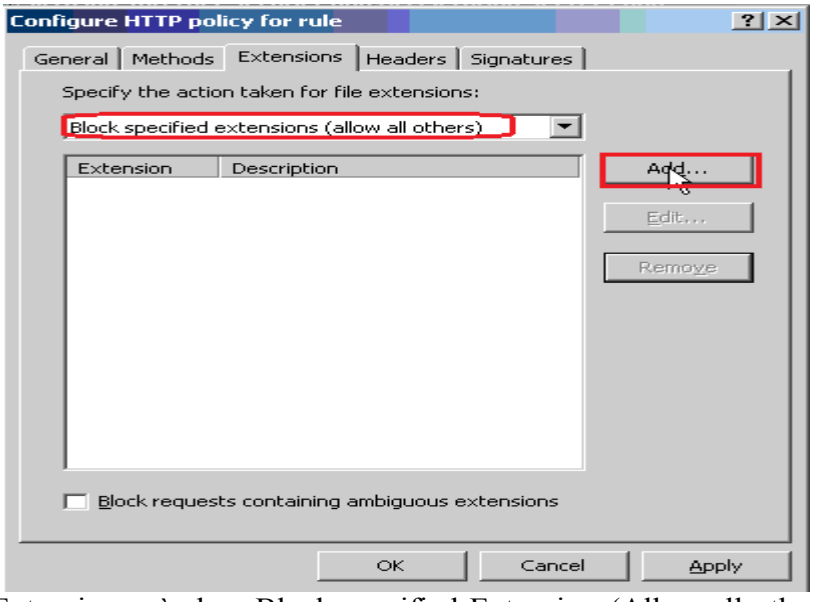
Click Apply



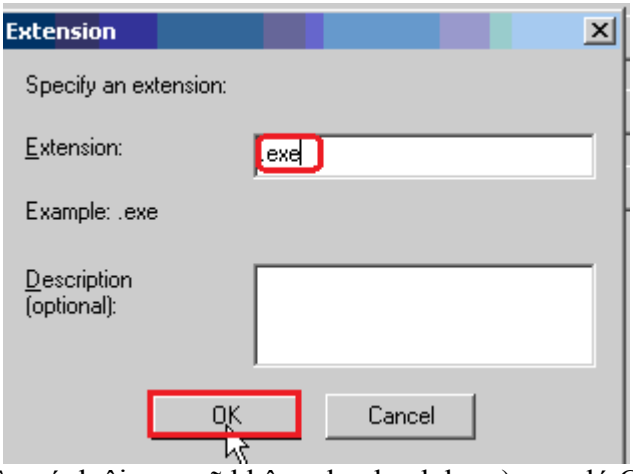
Logon tpkt và tpns ra ngoai internet sẽ không thấy hình



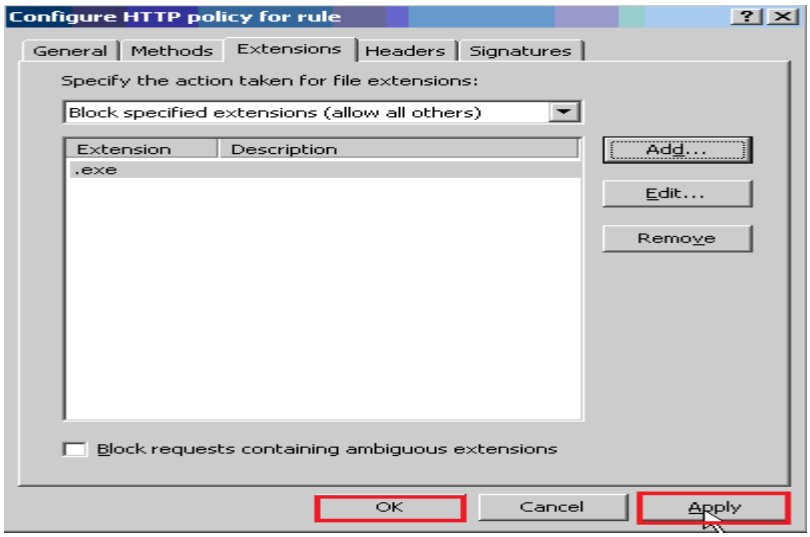
R_Click Rule vừa xét\Configure HTTP



Vào tab Extensions và chọn Block specified Extensions(Allow all other), sau đó Click Add

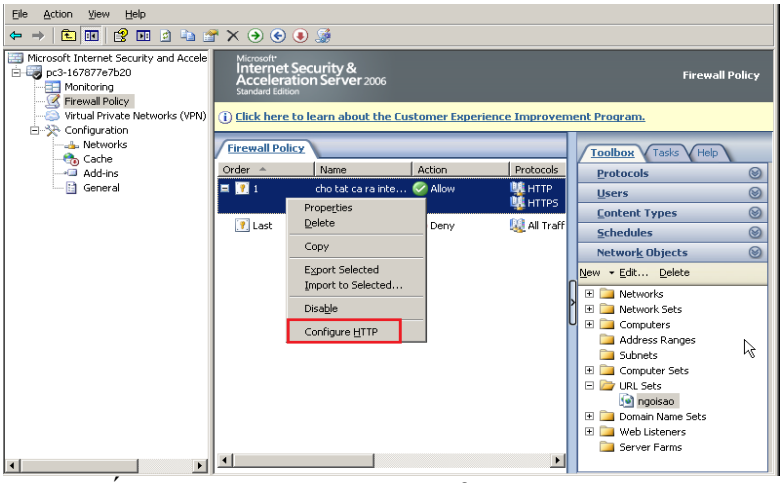


Điền .exe(file nào có đuôi .exe sẽ không dowload được), sau đó Click OK

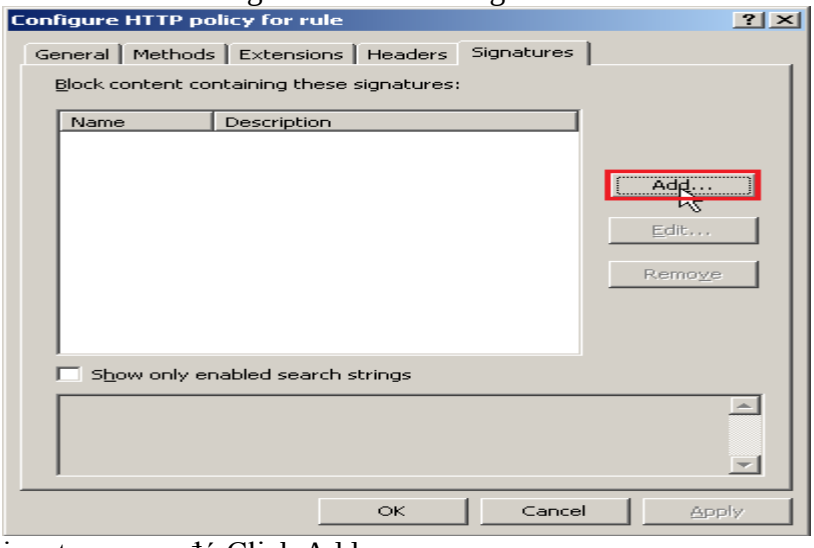


Click Apply\OK

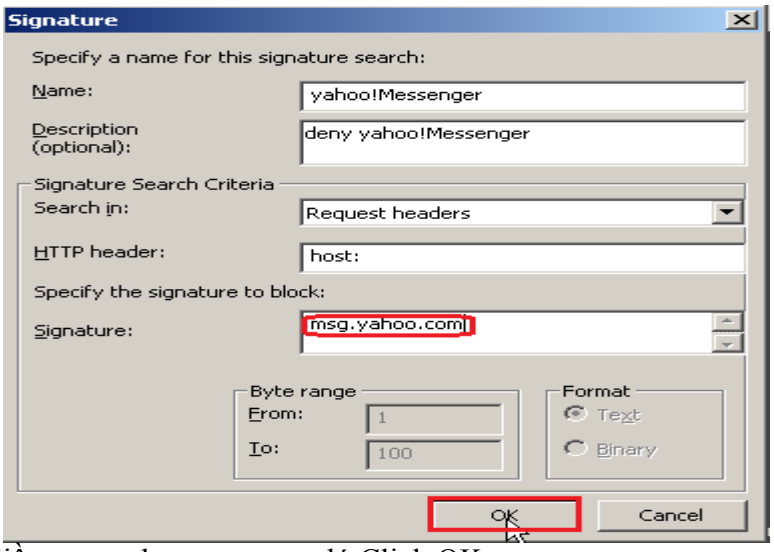
5.5. Cấm chat Yahoo!Messenger



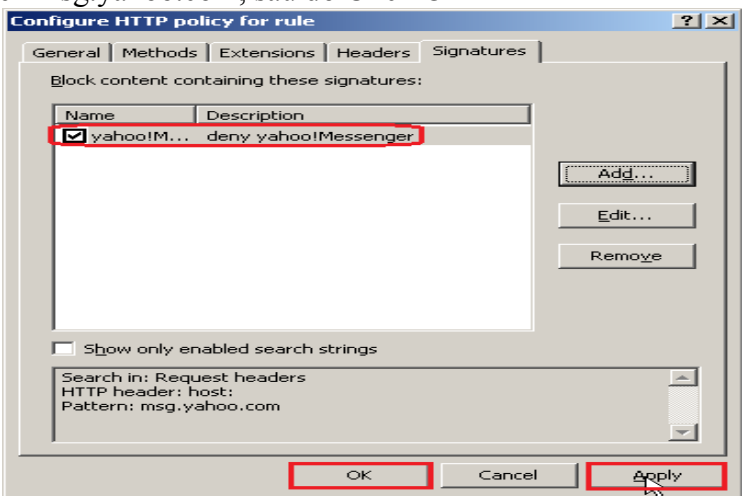
R_Click Rule cho tất cả ra ngoai internet\Configure HTTP



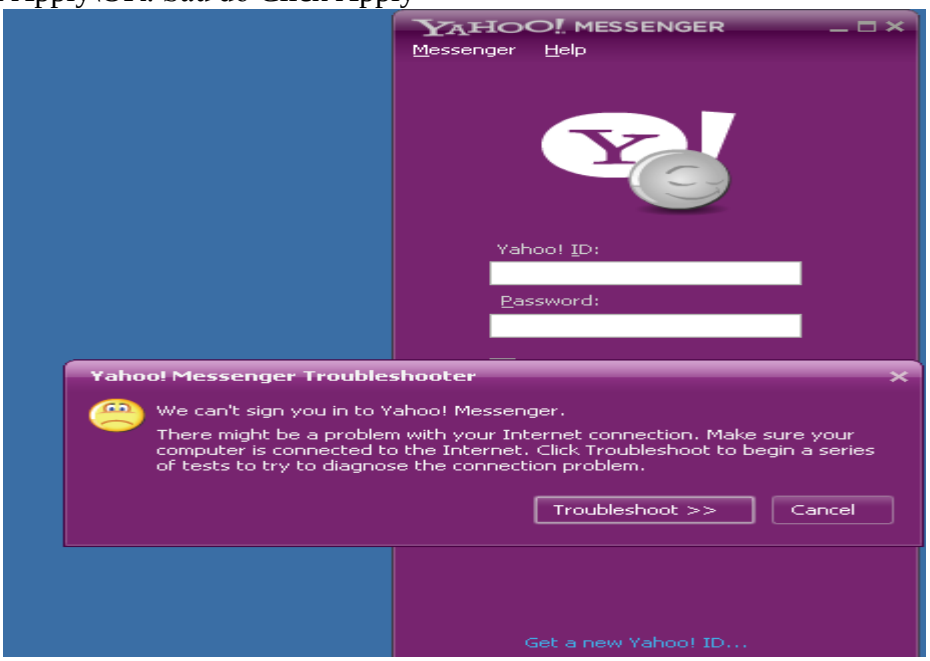
Vào tab Signatures, sau đó Click Add



Signature điền msg.yahoo.com, sau đó Click OK



Click Apply\OK. Sau đó Click Apply



Mở yahoo!Messenger logon user chang_rua91 không được

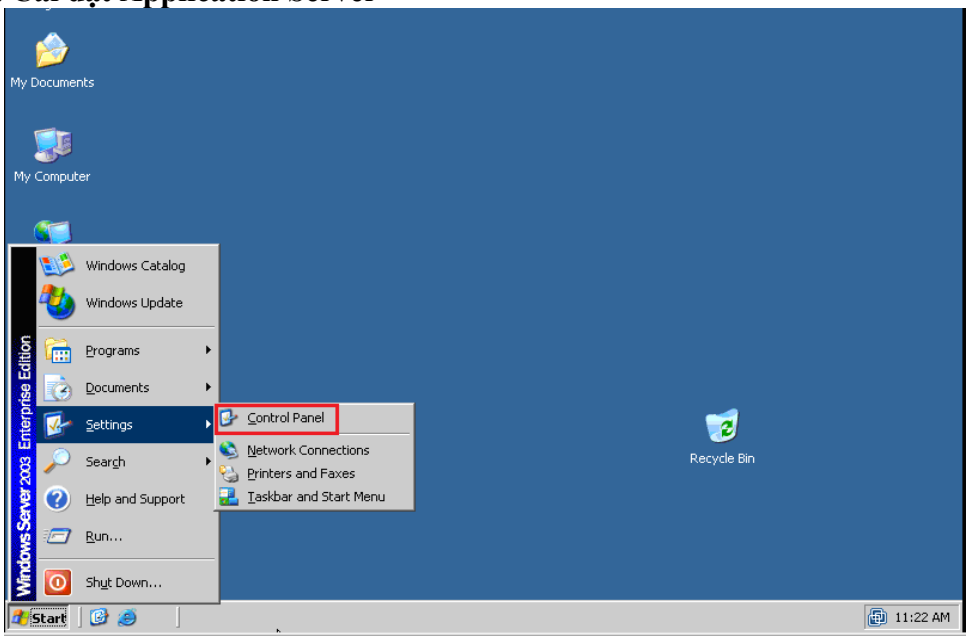
6. Pulishing website

Web publishing: Dùng để publish các Web Site và dịch vụ Web. Web Publishing đôi khi đượcgọi là 'reverse proxy' trong đó ISA Firewall đóng vai trò là Web Proxy nhận các Web request từbên ngoài sau đó nó sẽ chuyển yêu cầu đó vào Web Site hoặc Web Services nội bộ xử lý.

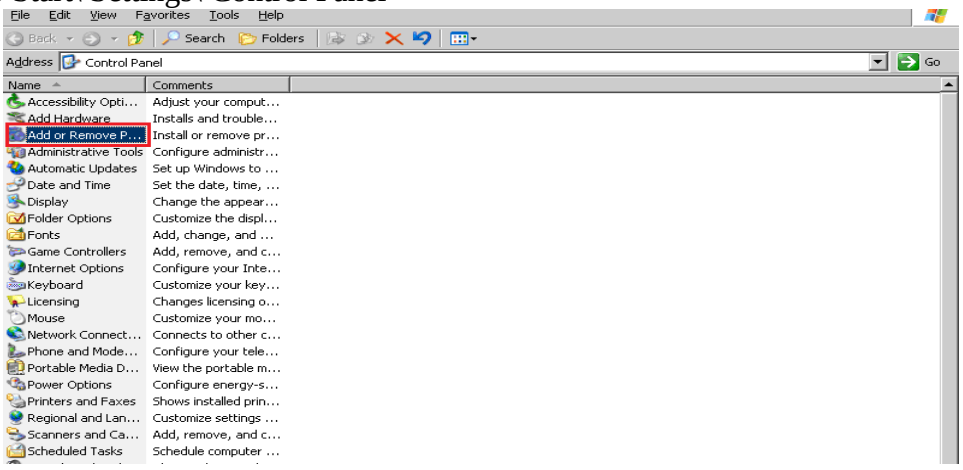
Một số đặc điểm của Web Publishing:

- Cung cấp cơ chế truy xuất ủy quyền Web Site thông qua ISA firewall.
- Chuyển hướng theo đường dẫn truy xuất Web Site (Path redirection)
- Reverse Caching of published Web Site.
- Cho phép publish nhiều Web Site thông qua một địa chỉ IP.
- Có khả năng thay đổi (re-write) URLs bằng cách sử dụng Link Translator của ISA firewall.
- Thiết lập cơ chế bảo mật và hỗ trợ chứng thực truy xuất cho Web Site (SecurID authentication,RADIUS authentication, Basic Authentication)
- Cung cấp cơ chế chuyển theo Port và Protocol.

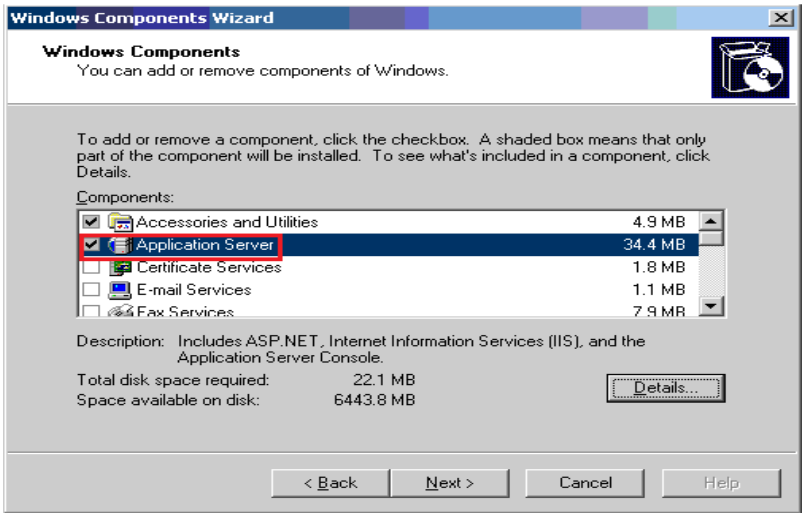
6.1. Cài đặt Application Server



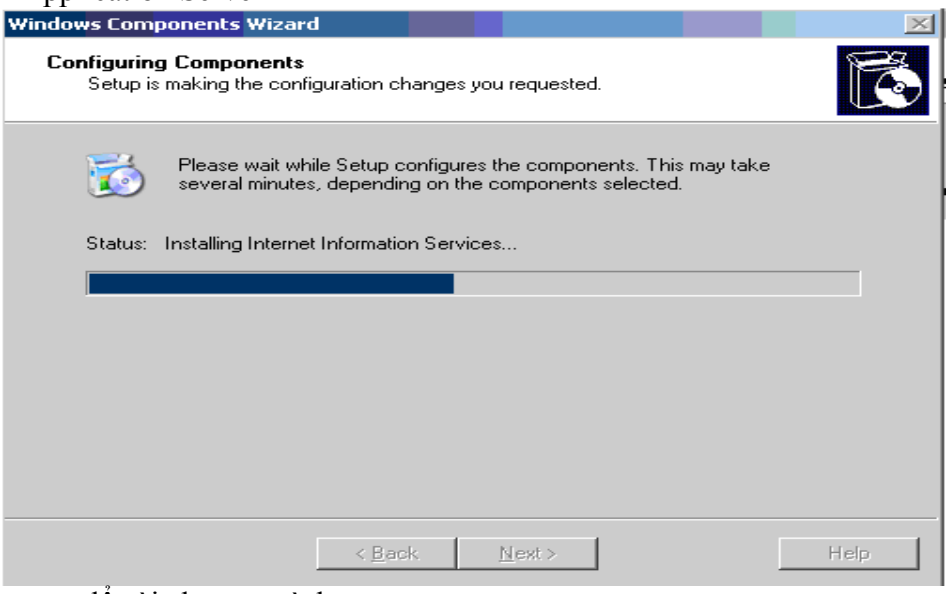
Vào Start\ Settings\ Control Panel



Click Add or Remove …



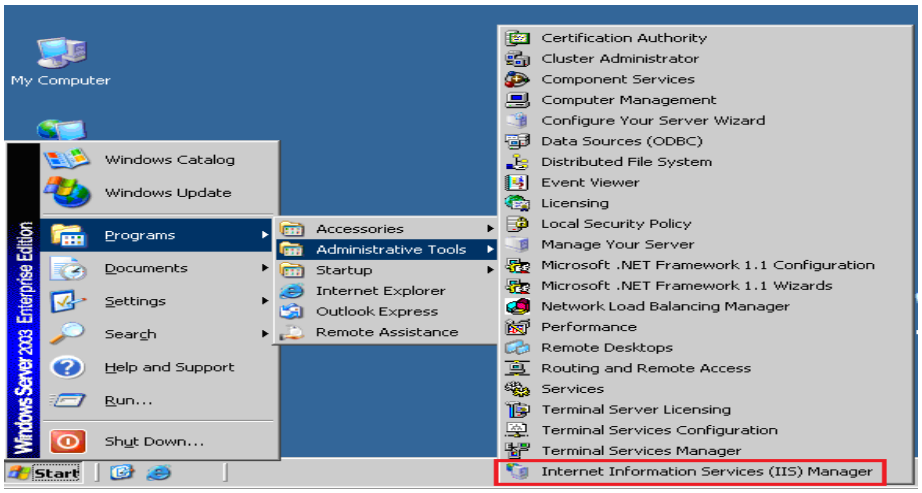
Chọn Application Server



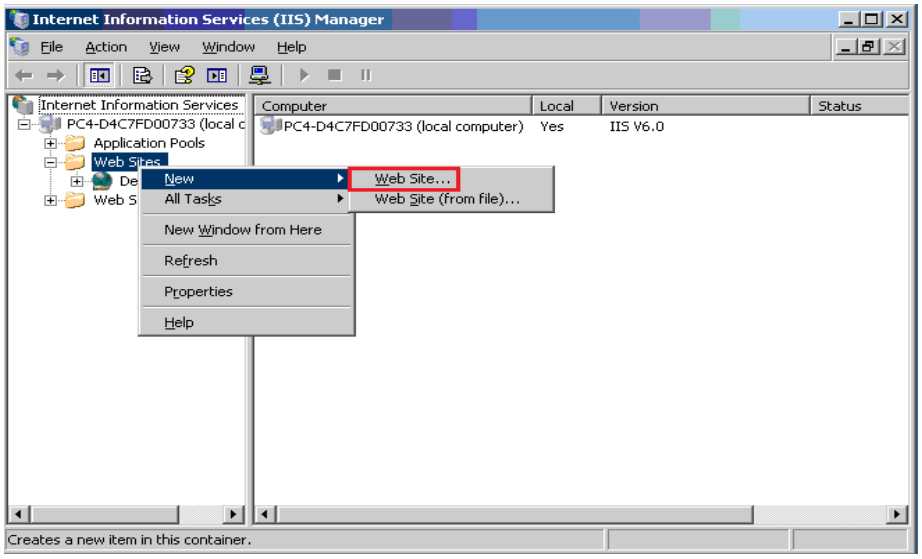
Chọn next để cài chương trình.

Click Finish

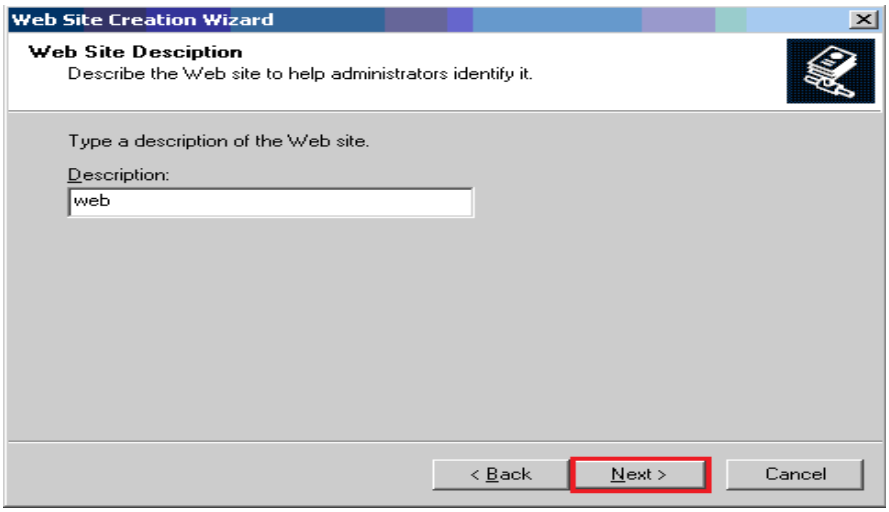
6.2. Cấu hình Web



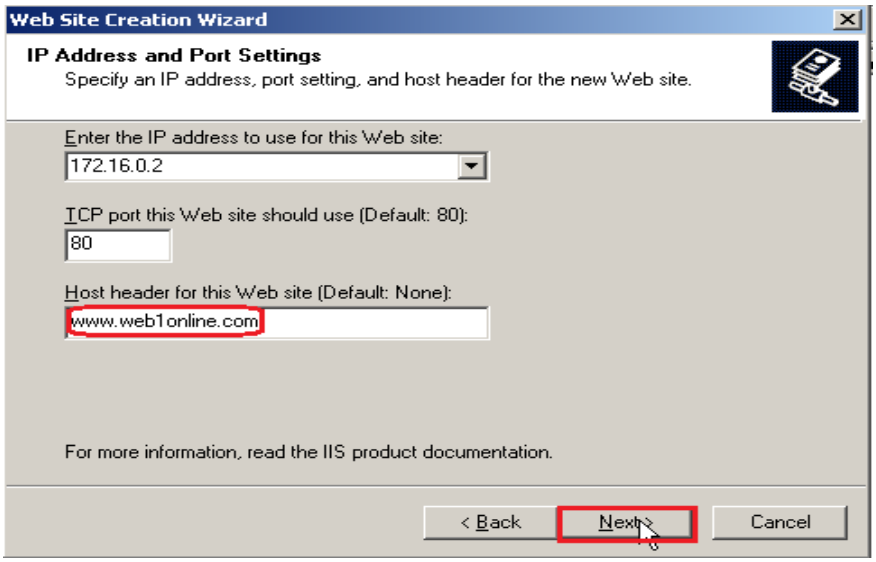
Start\Programs\Administrative Tools\ Internet Information Services(IIS)Manager



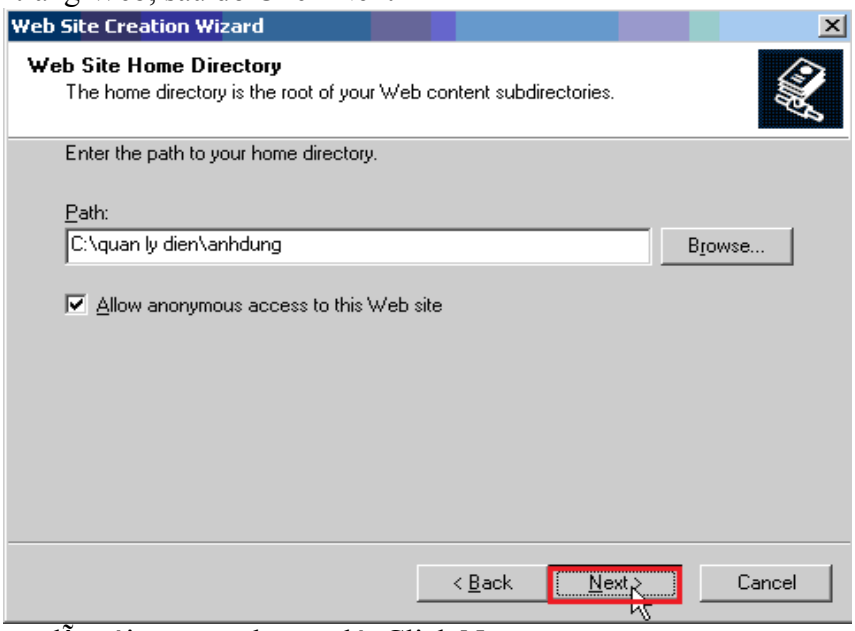
R_Click Web Sites\New\Web Site…



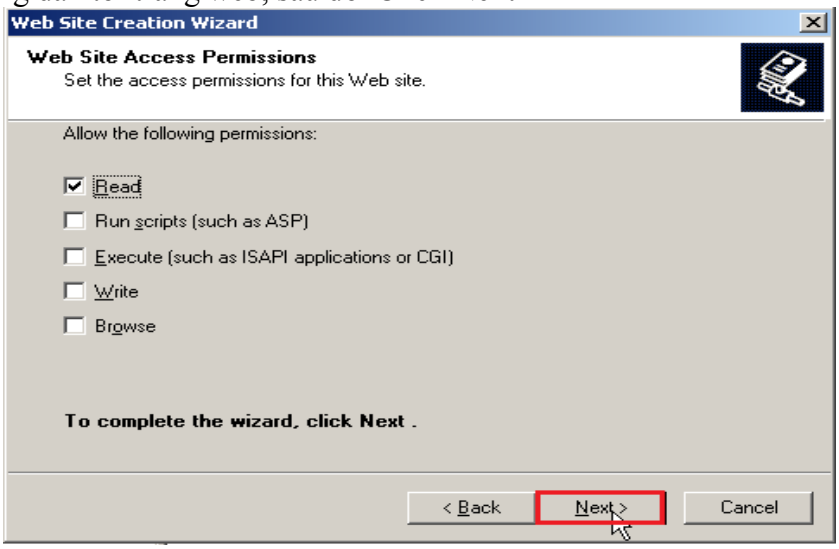
Click Next



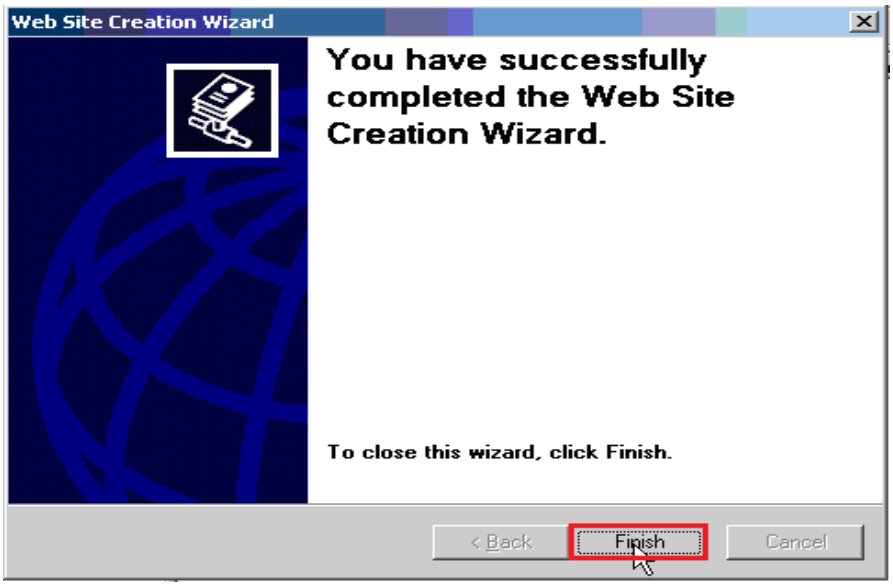
Điền tên trang Web, sau đó Click Next



Tạo đường dẫn tới trang web, sau đó Click Next

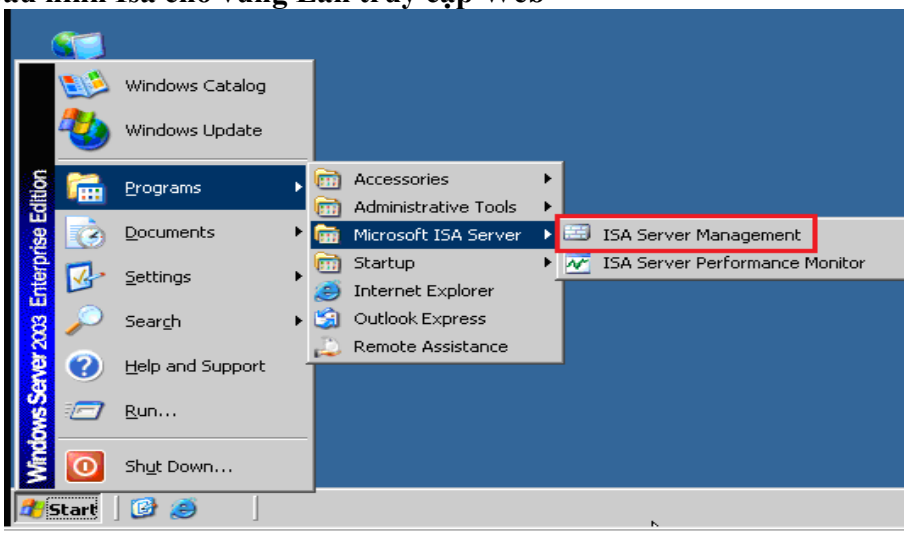


Click Next

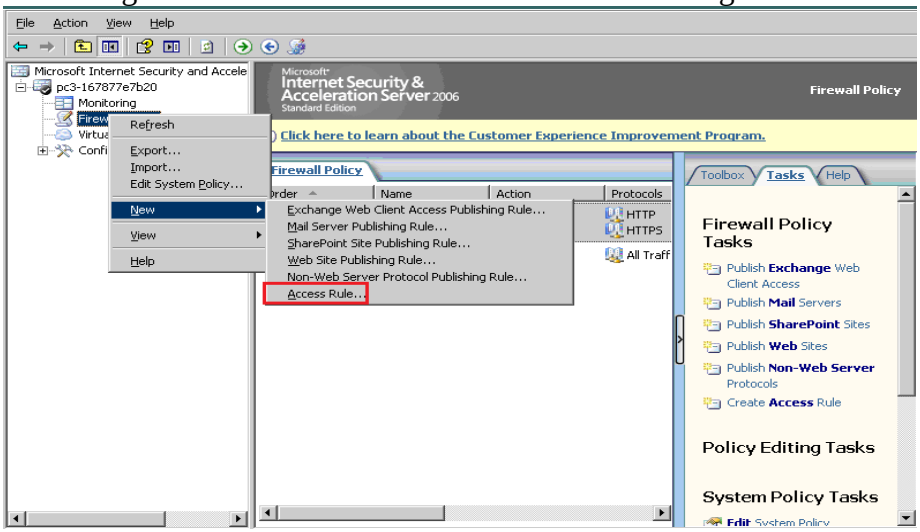


Click Finish

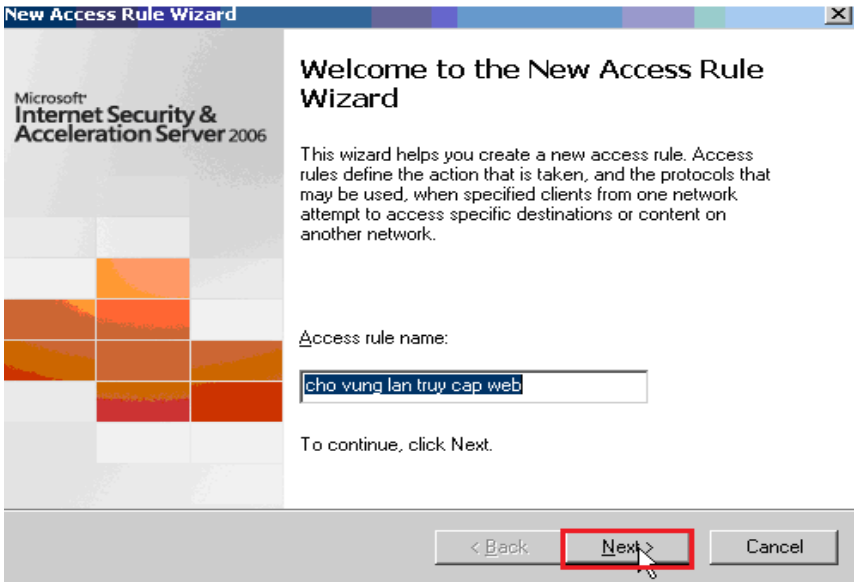
6.3. Cấu hình Isa cho vùng Lan truy cập Web



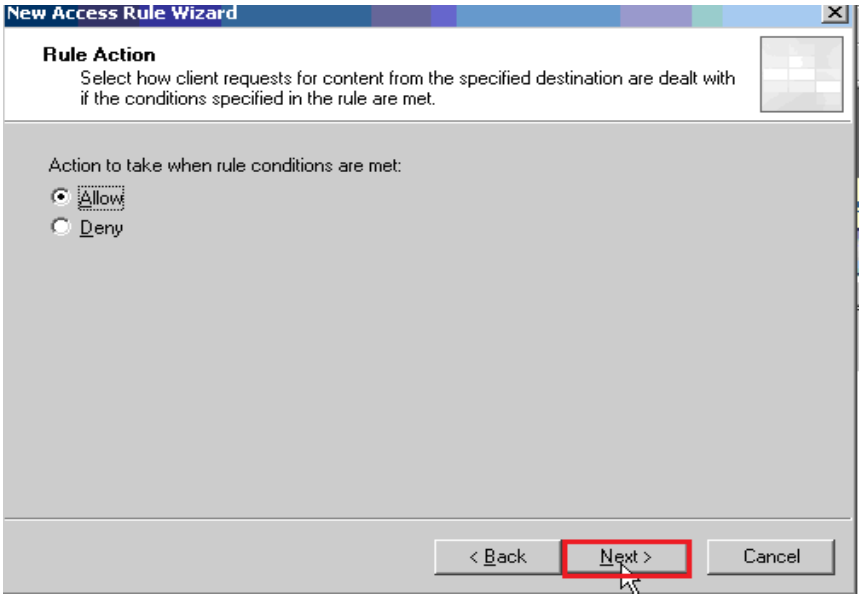
Click Start\Programs\Microsoft ISA Server\ISA Server Management



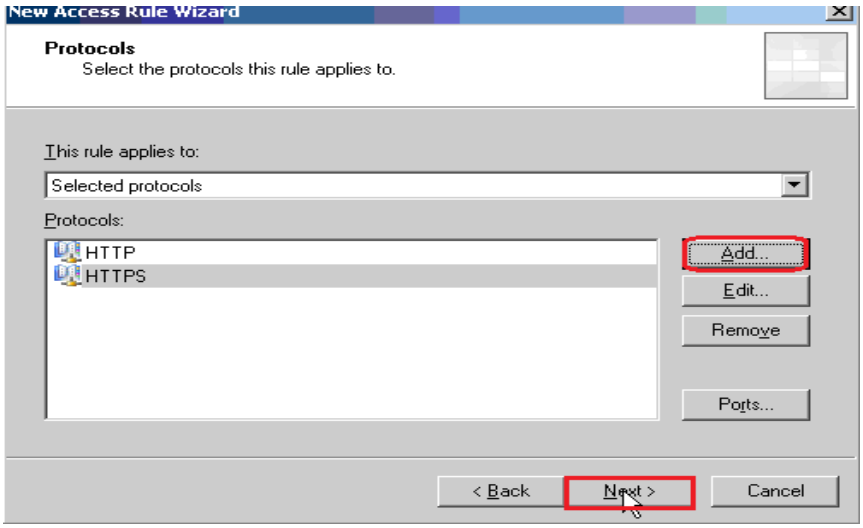
R_Click Firewall Policy\New\Access Rule…



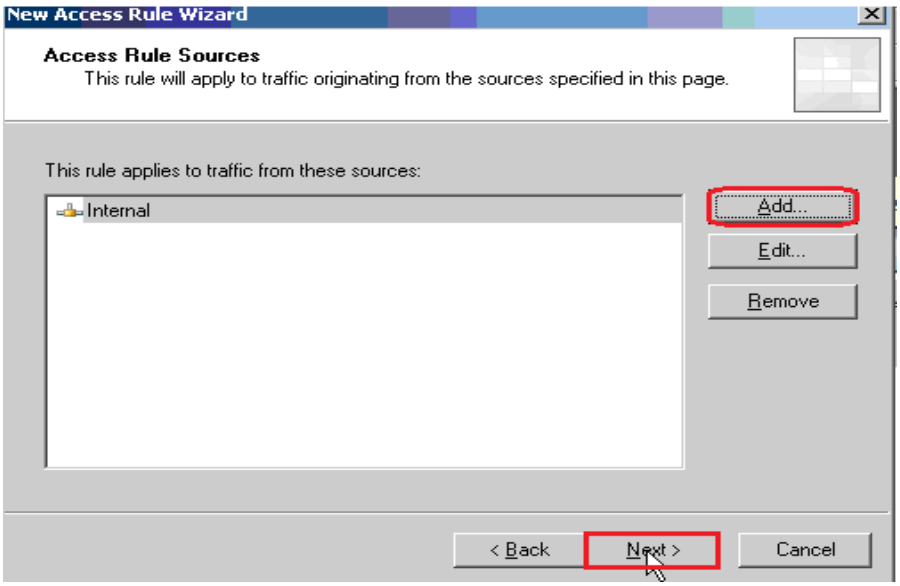
Click Next



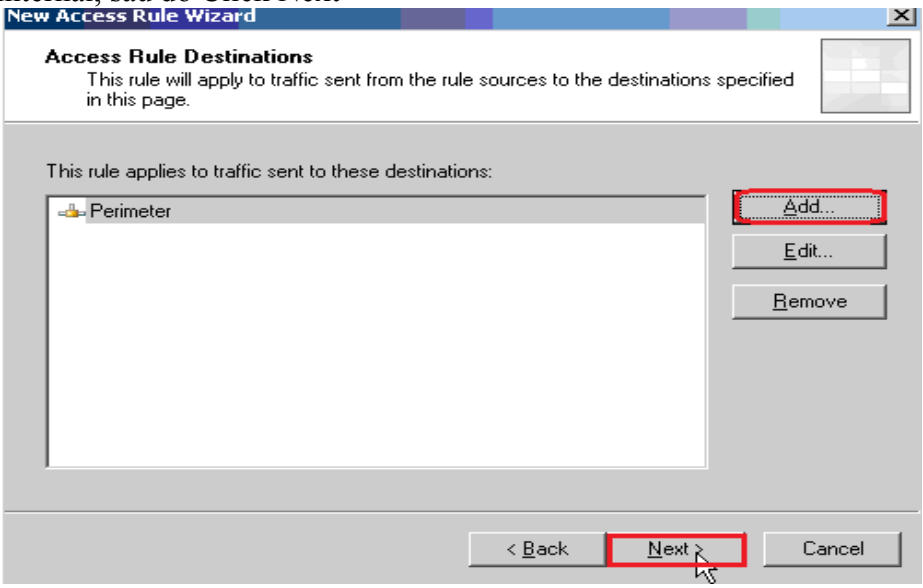
Click Next



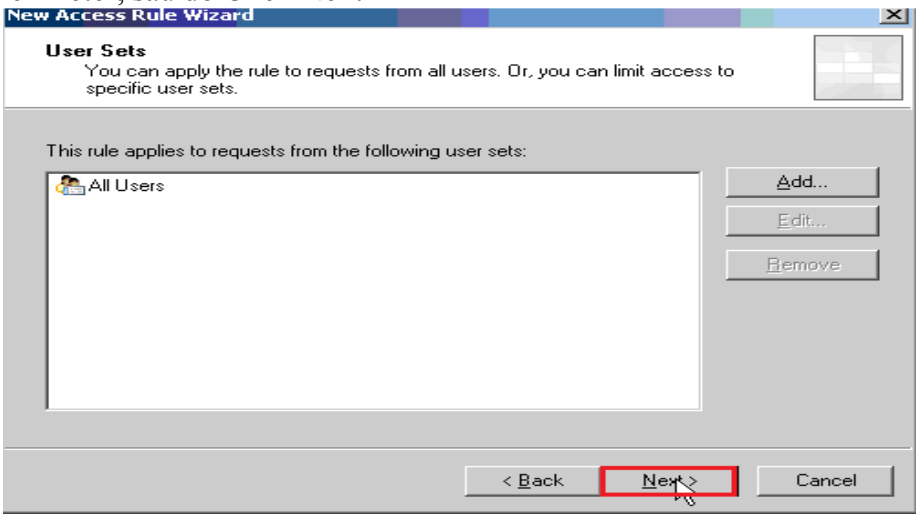
Add HTTP và HTTPS, sau đó Click Next



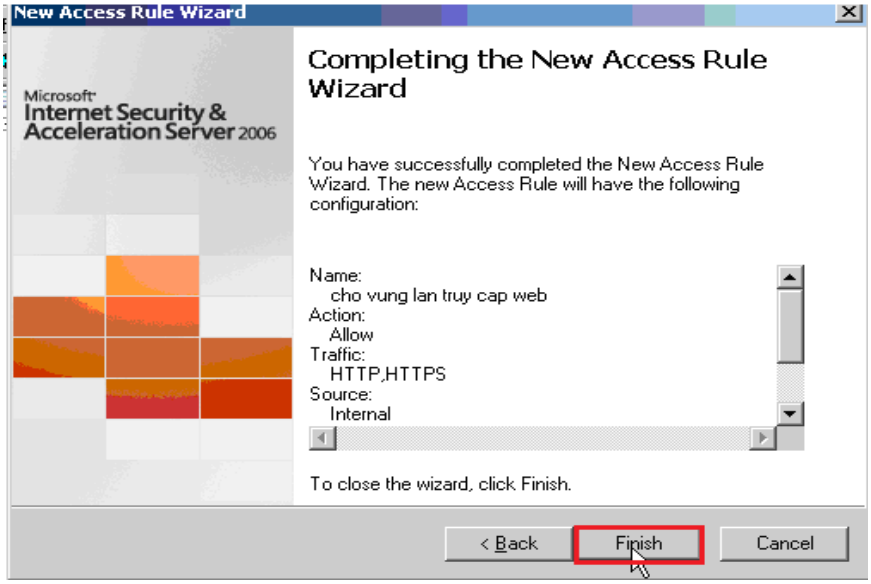
Add Internal, sau đó Click Next



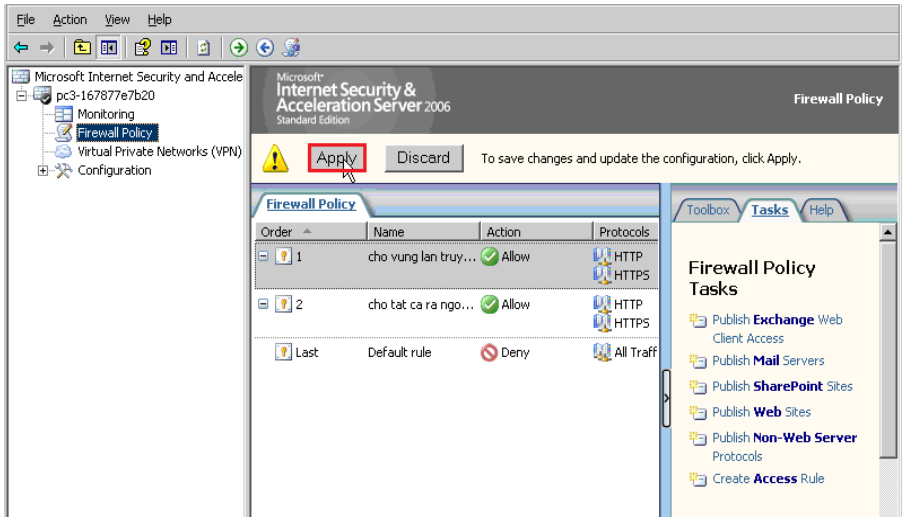
Add Perimeter, sau đó Click Next



Add All User, sau đó Click Next

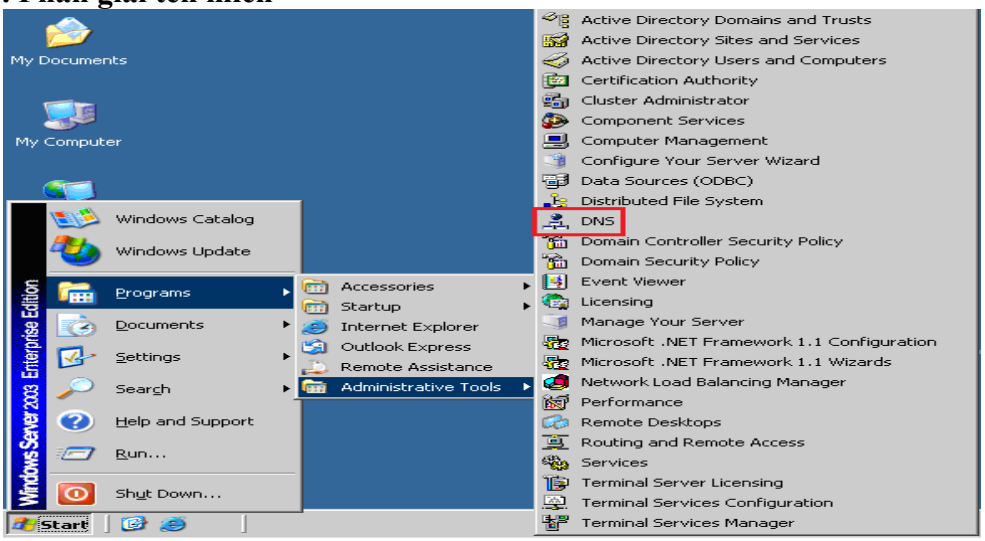


Click Finish

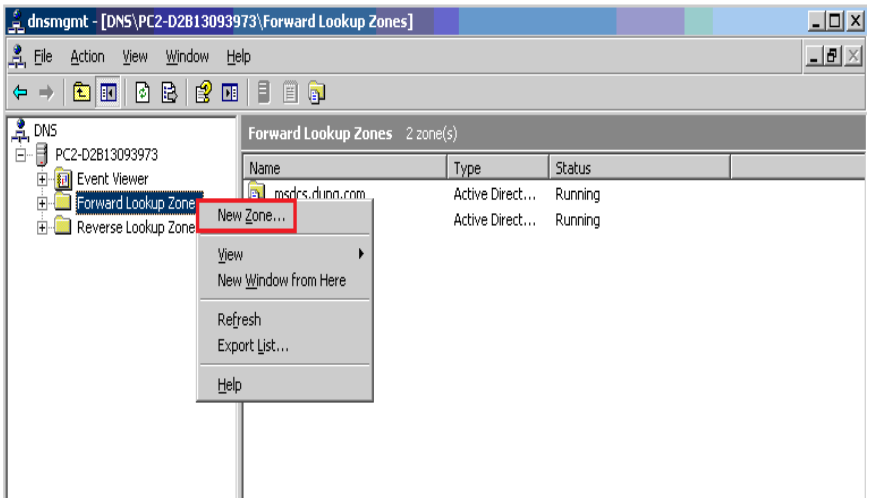


Click Apply

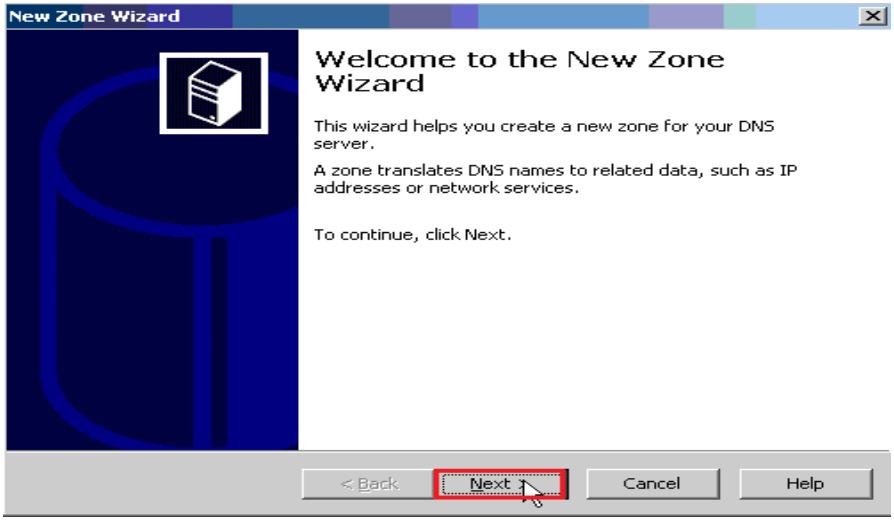
6.4. Phân giải tên miền



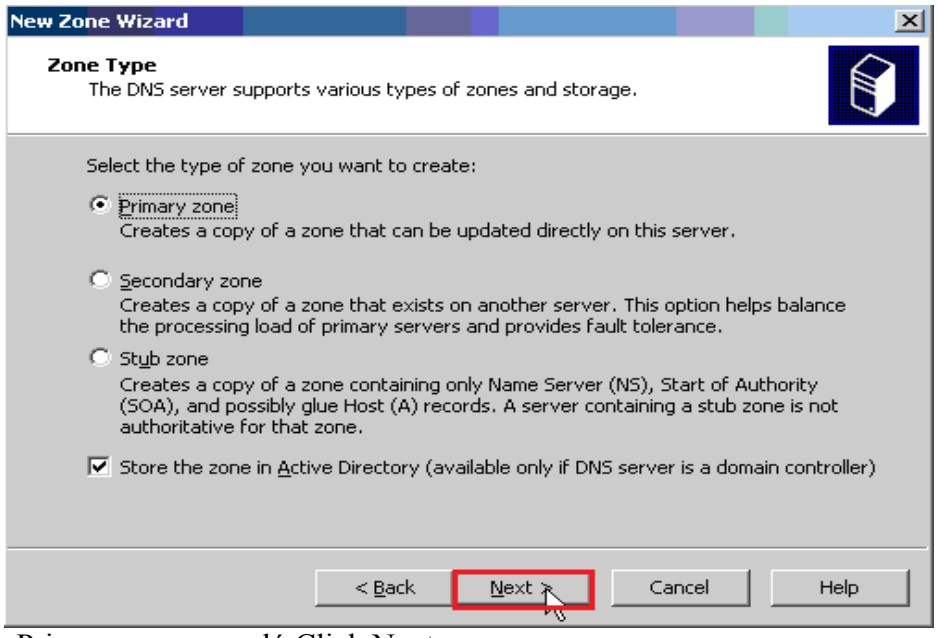
Click Start\Programs\Administrativi Tools\DNS



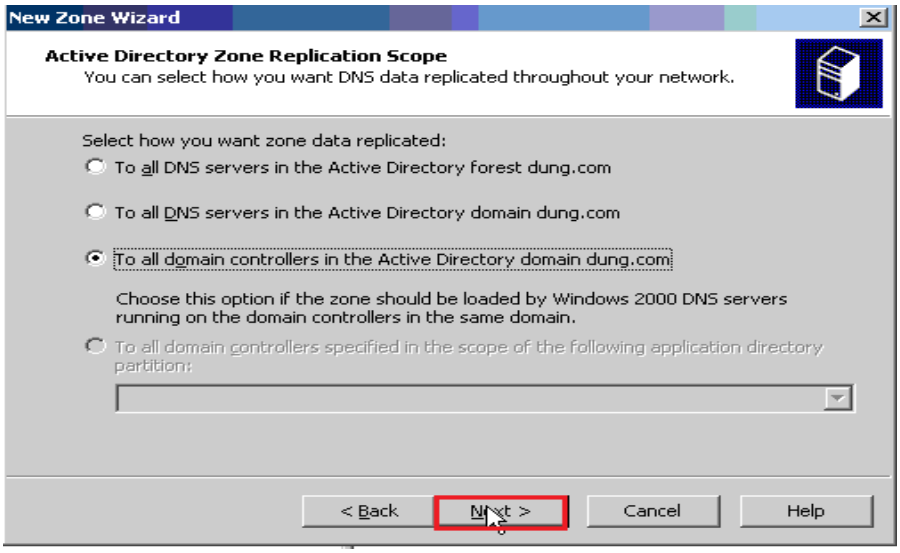
R_Click Forward Lookup Zone\New Zone…



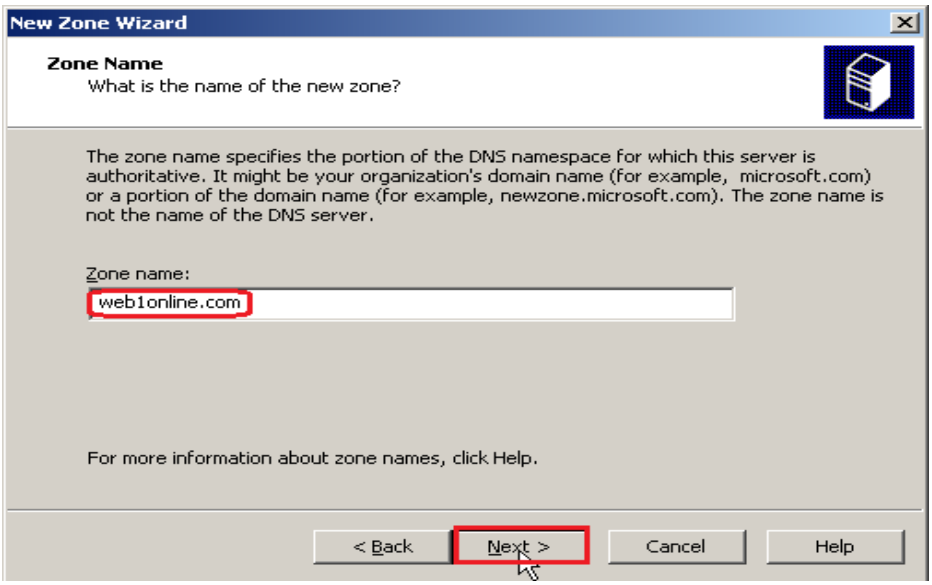
Click Next



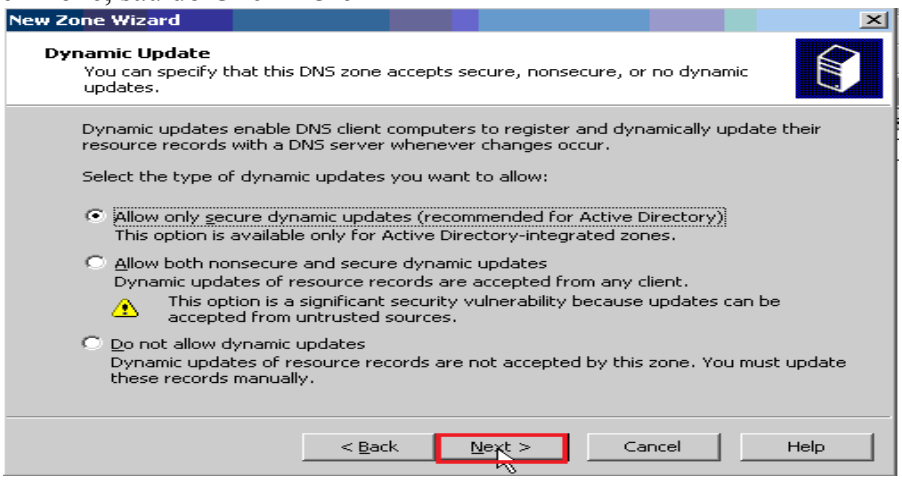
Chọn Primary zone, sau đó Click Next



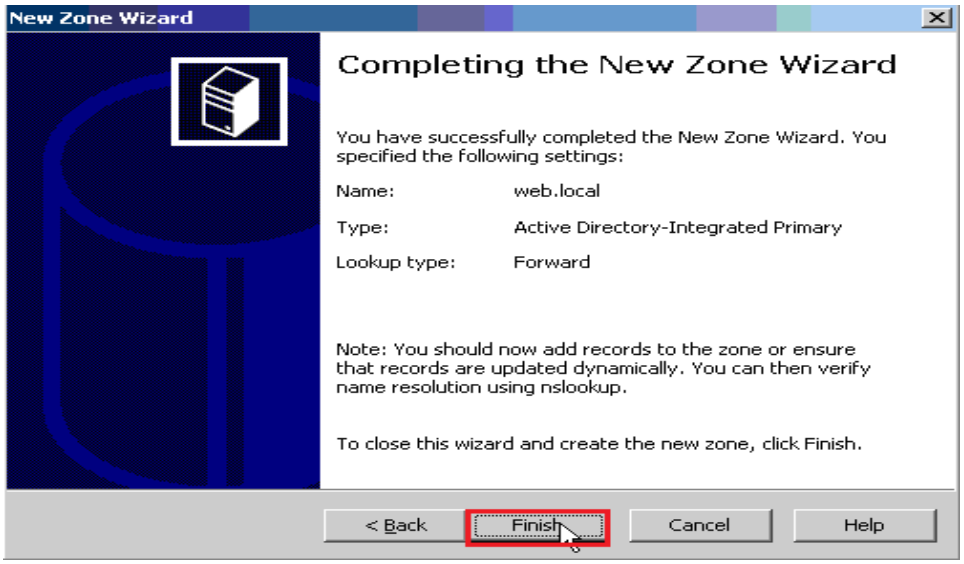
Chọn To all domain controlleras in the Active Directory domain dung.com, sau đó Click Next



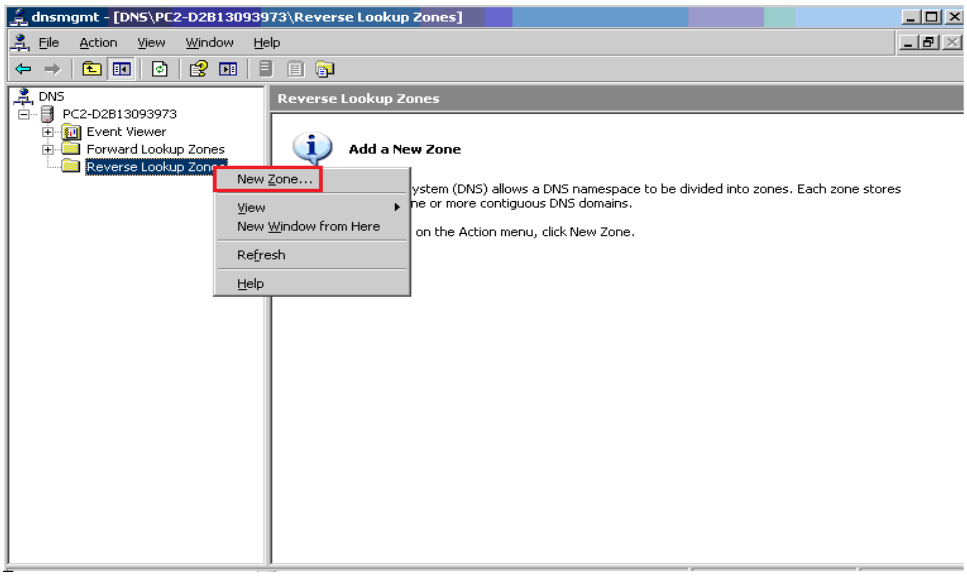
Điền tên Zone, sau đó Click Next



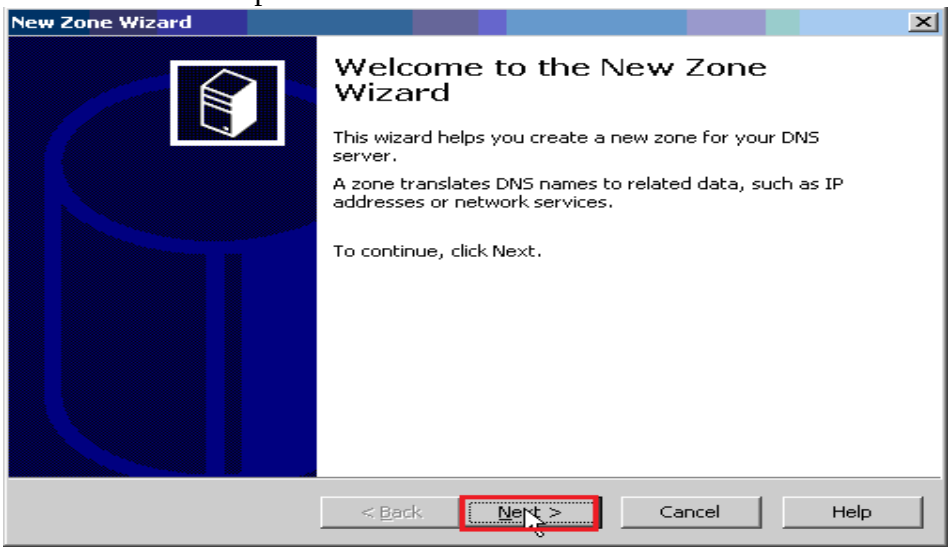
Chọn Allow only sercure dynamic updates(recommended for Active Diretory), sau đó Click Next



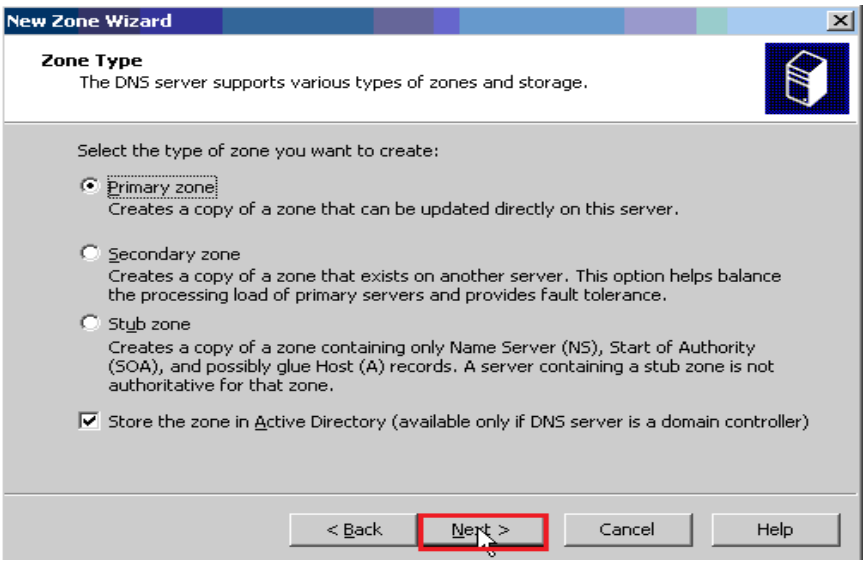
Click Finish



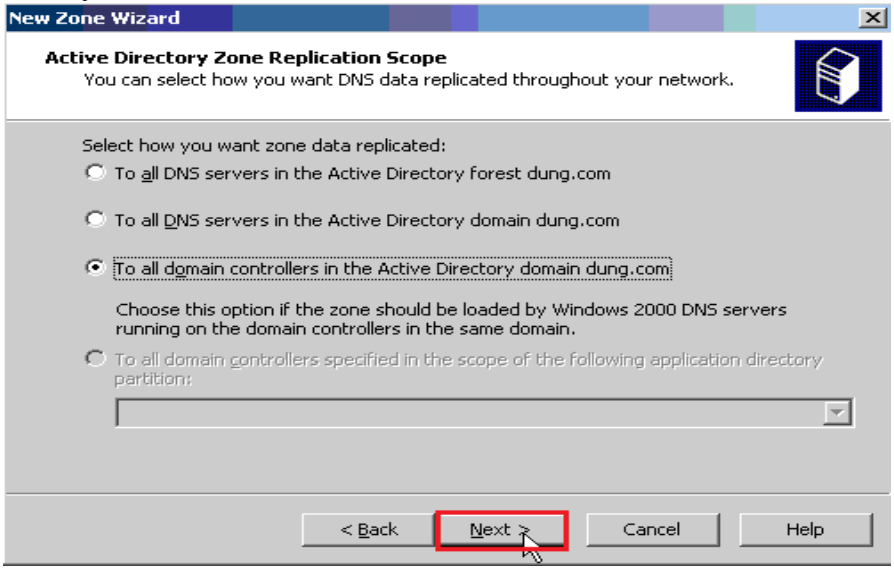
R_Click Reverse Lookup Zone\New Zone…



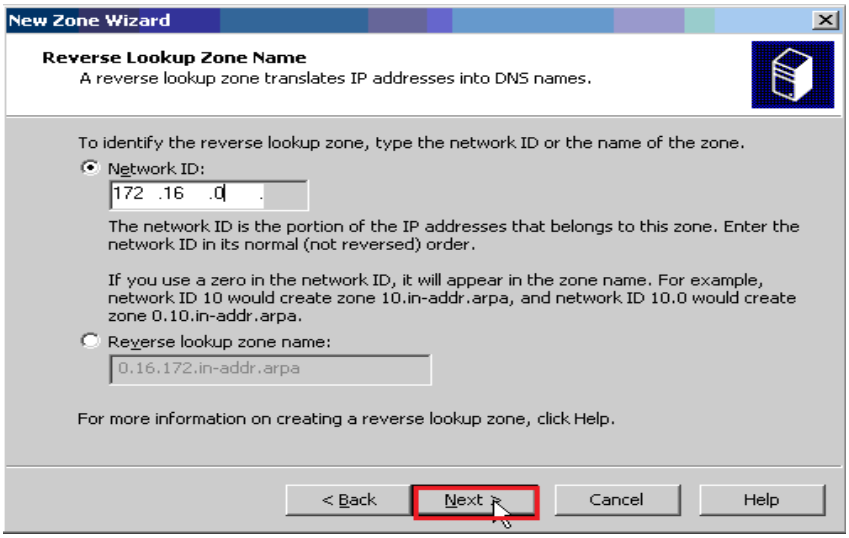
Click Next



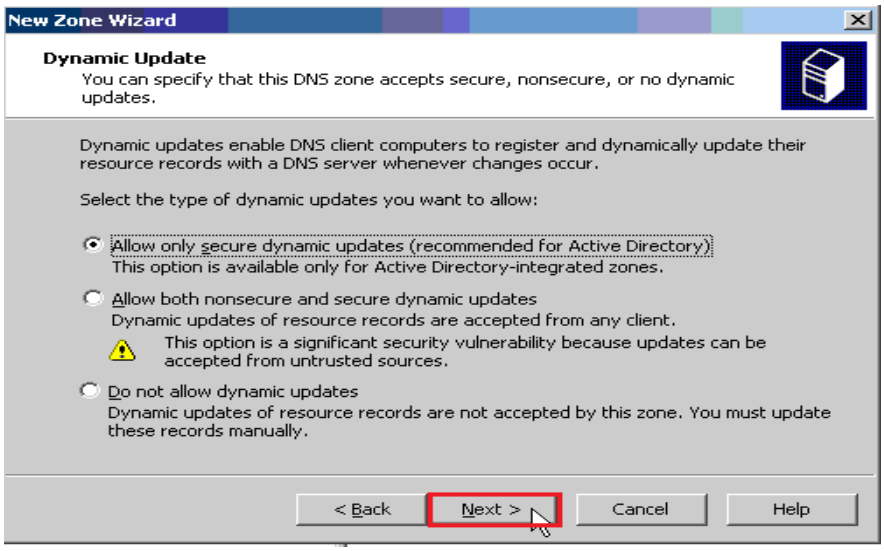
Chọn Primary zone,sau đó Click Next



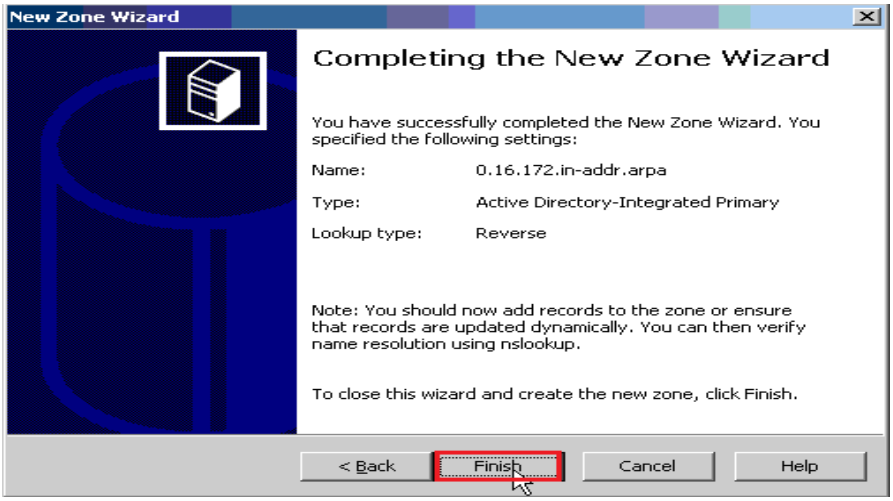
Chọn To all domain controlleras in the Active Directory domain dung.com , sau đó Click Next



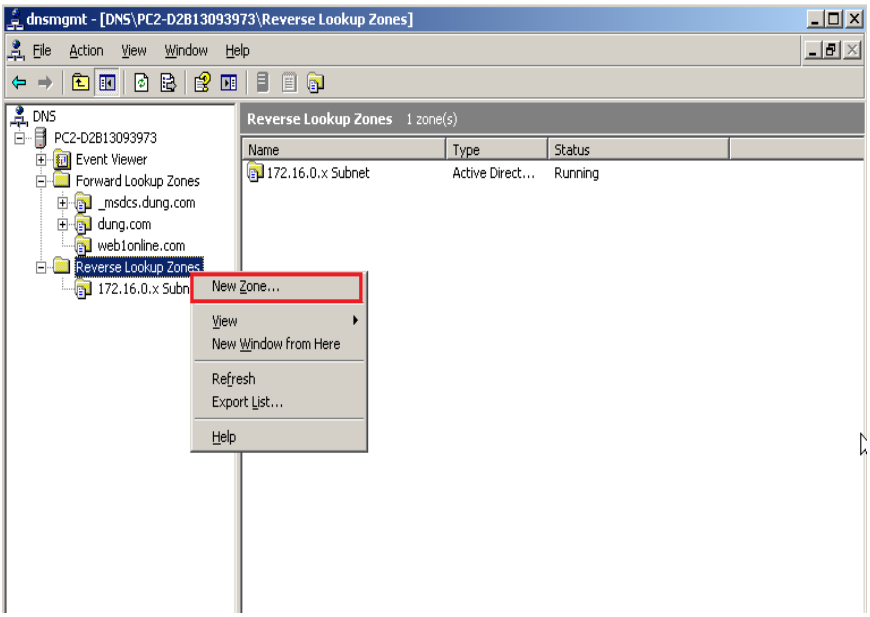
Điền Network ID, sau đó Click Next



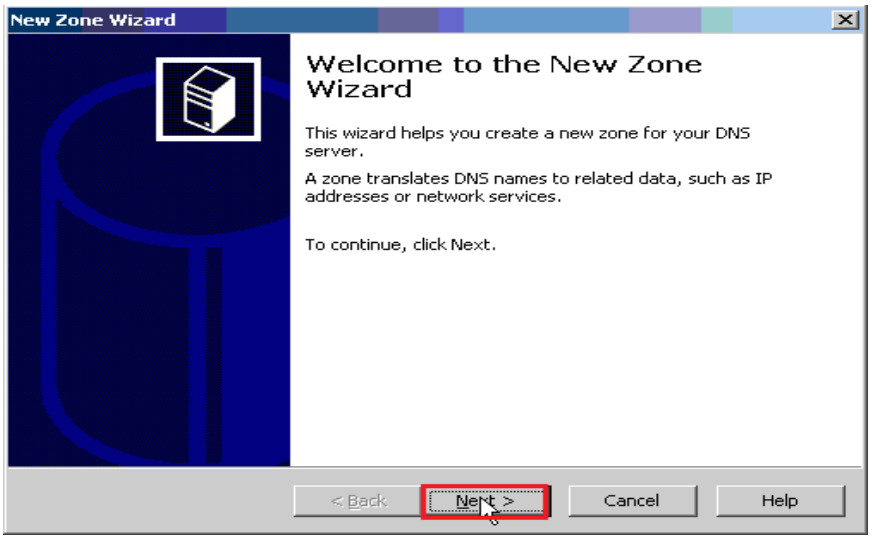
Chọn Allow only sercure dynamic updates(recommended for Active Diretory), sau đó Click Next



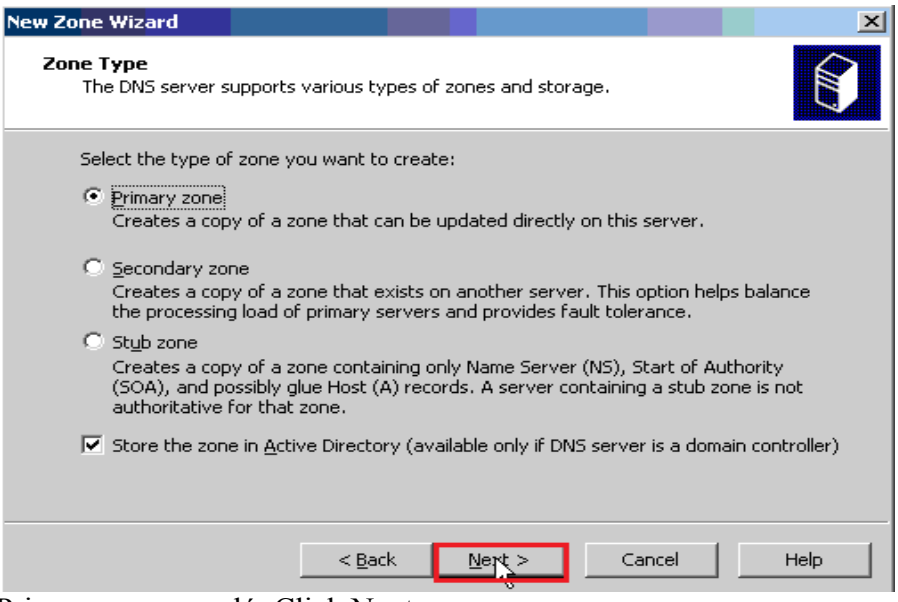
Click Finish



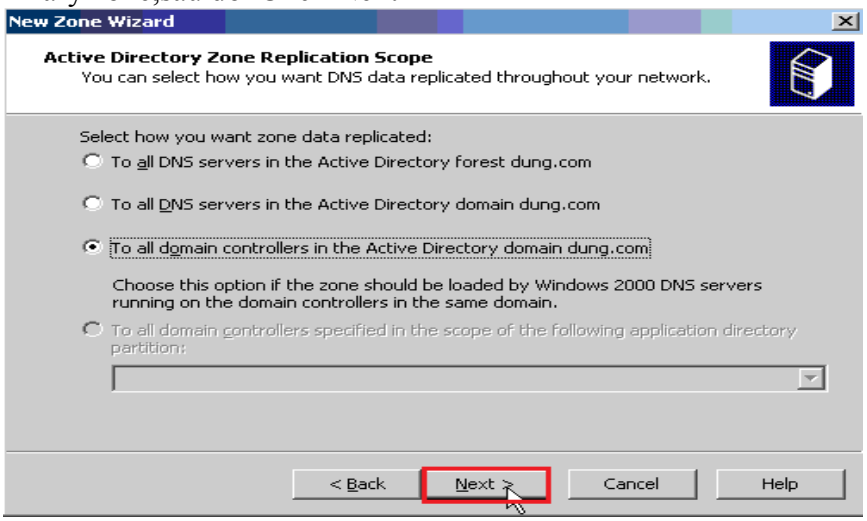
R_Click Reverse Lookup Zone\New Zone…



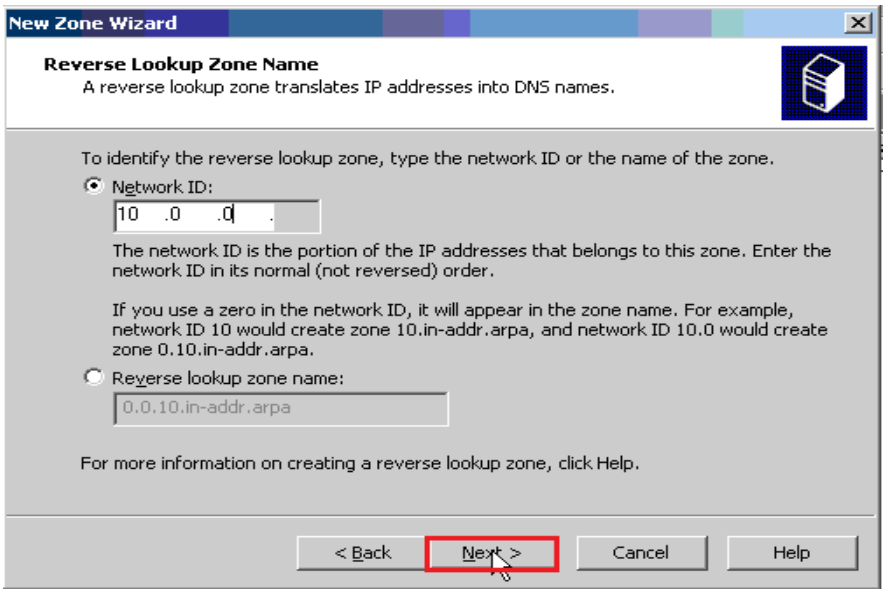
Click Next



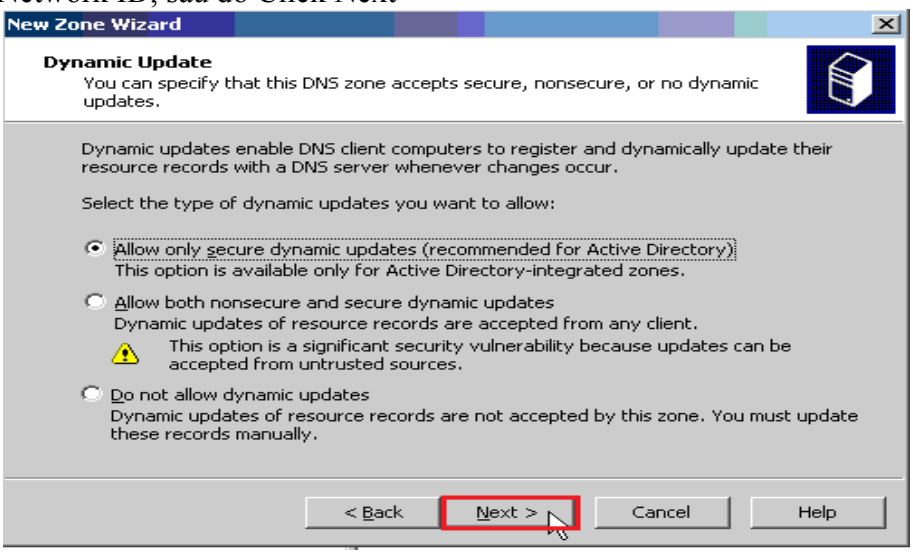
Chọn Primary zone,sau đó Click Next



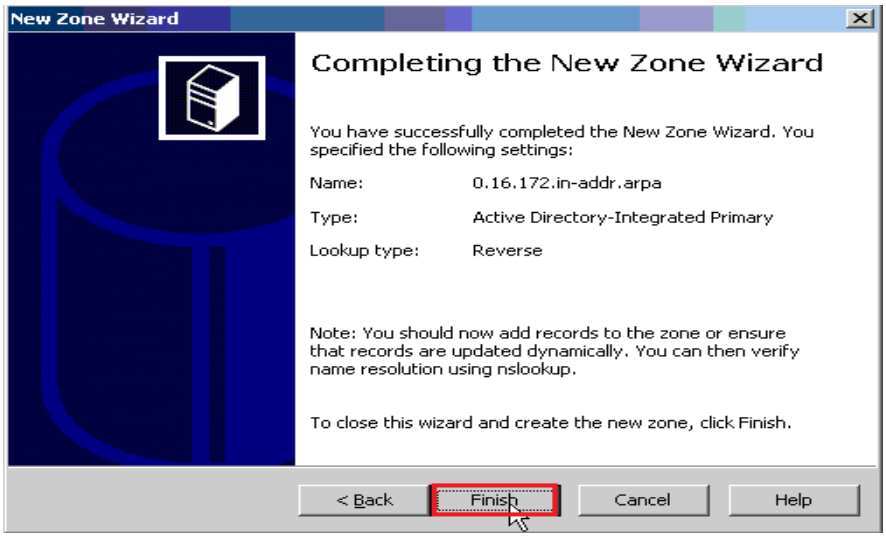
Chọn To all domain controlleras in the Active Directory domain dung.com , sau đó Click Next



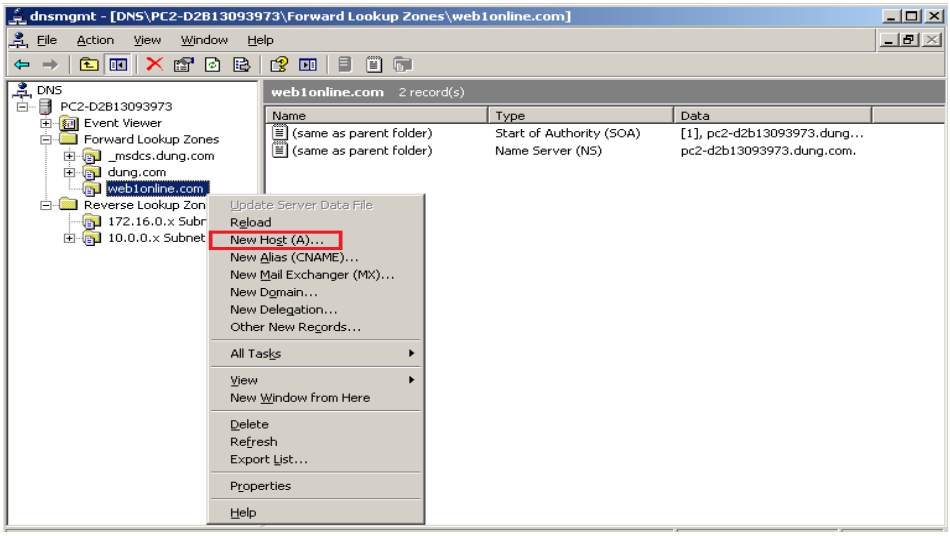
Điền Network ID, sau đó Click Next



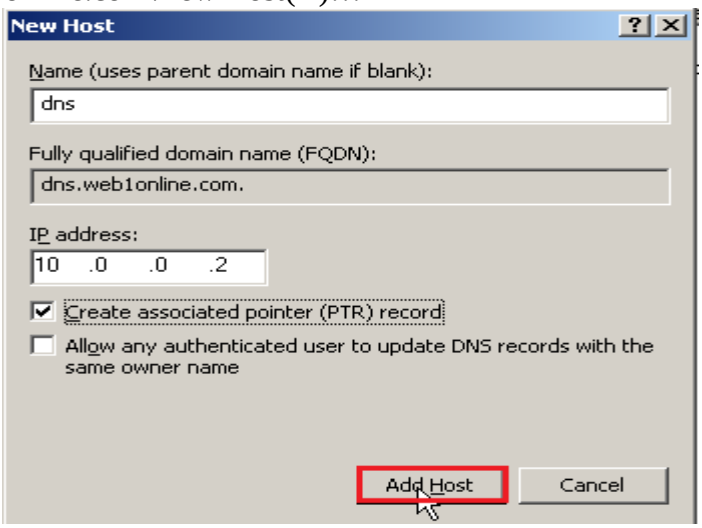
Chọn Allow only sercure dynamic updates(recommended for Active Diretory), sau đó Click Next



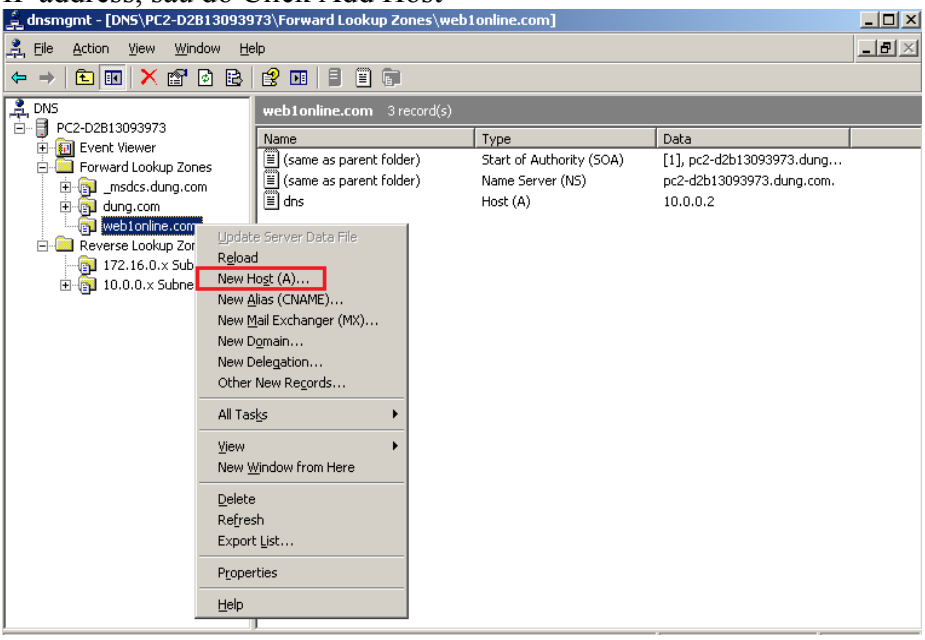
Click Finish



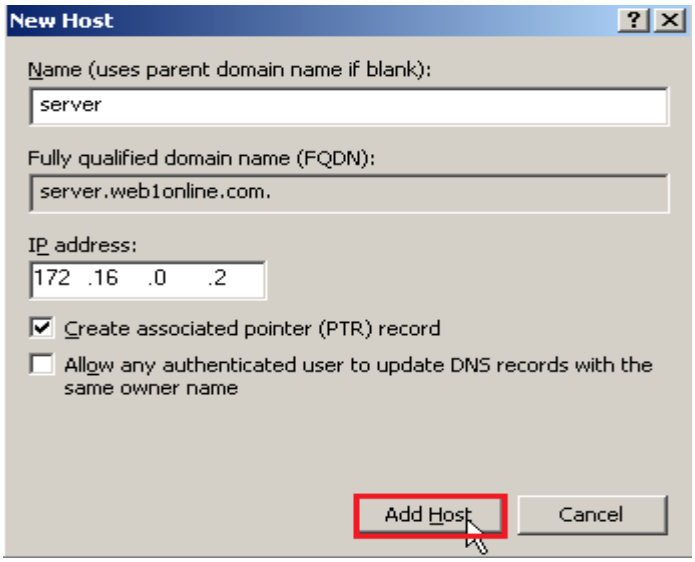
R_Click web1online.com\New Host(A)…



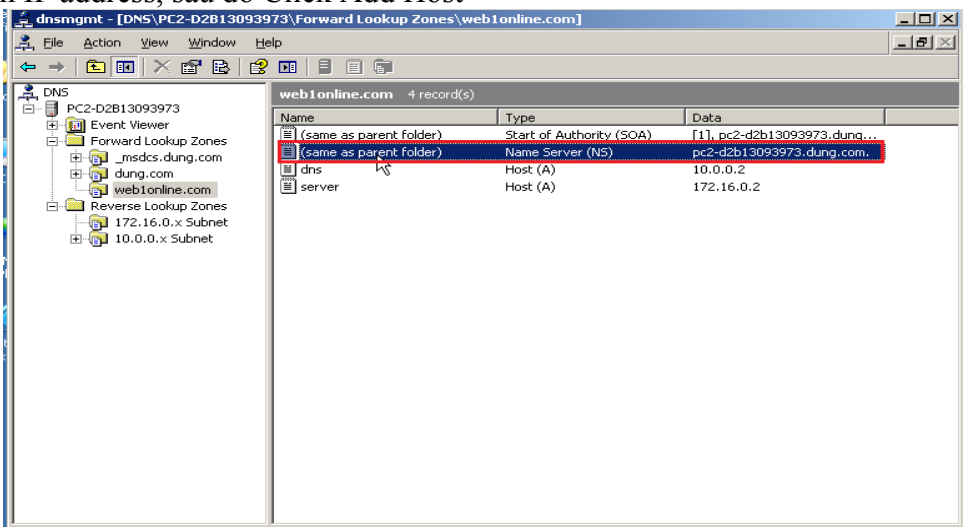
Điền IP address, sau đó Click Add Host



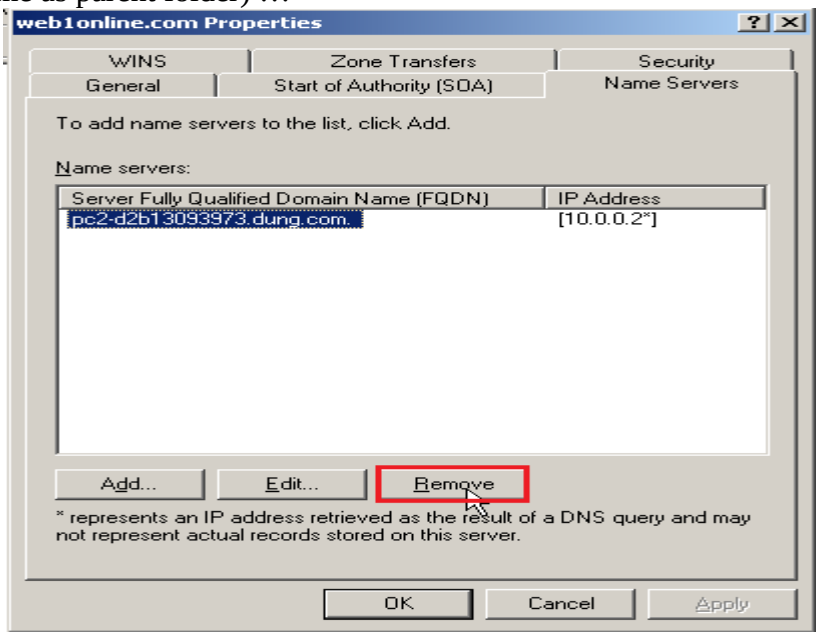
R_Click web1online.com\New Host(A)…



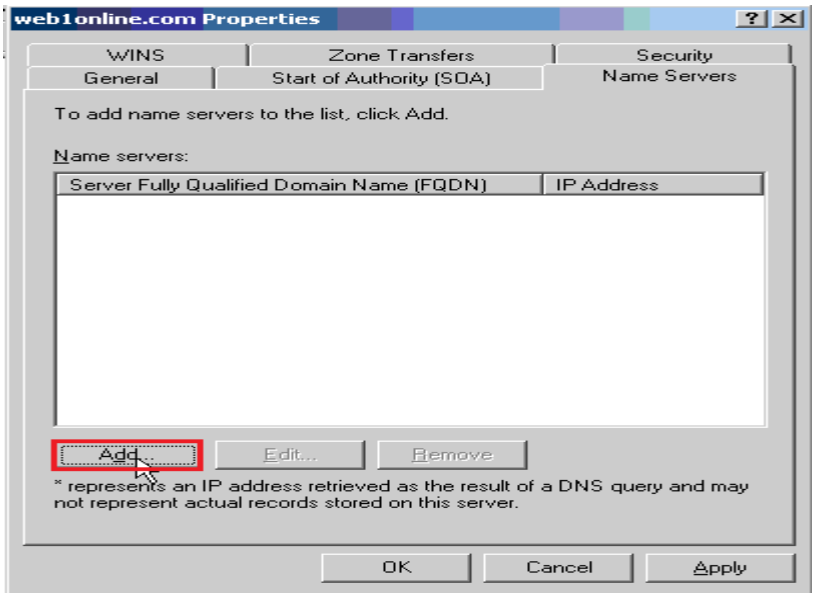
Điền IP address, sau đó Click Add Host



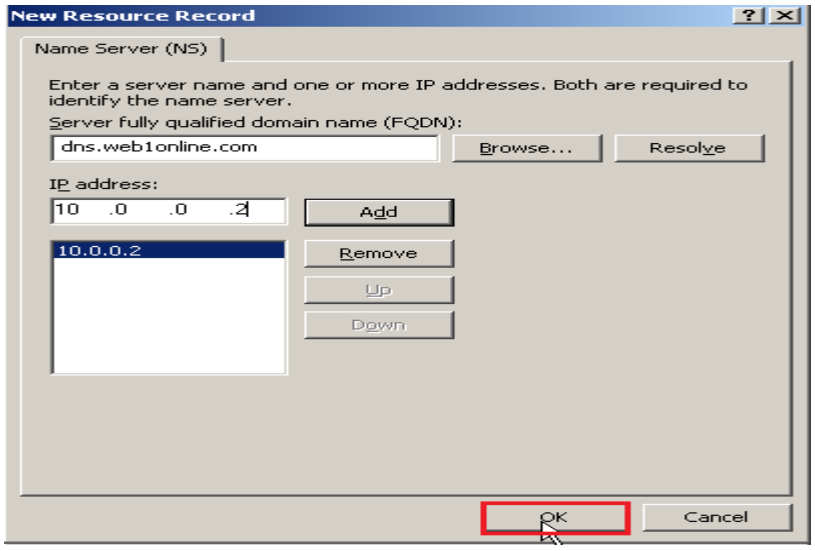
Click (same as parent folder) …



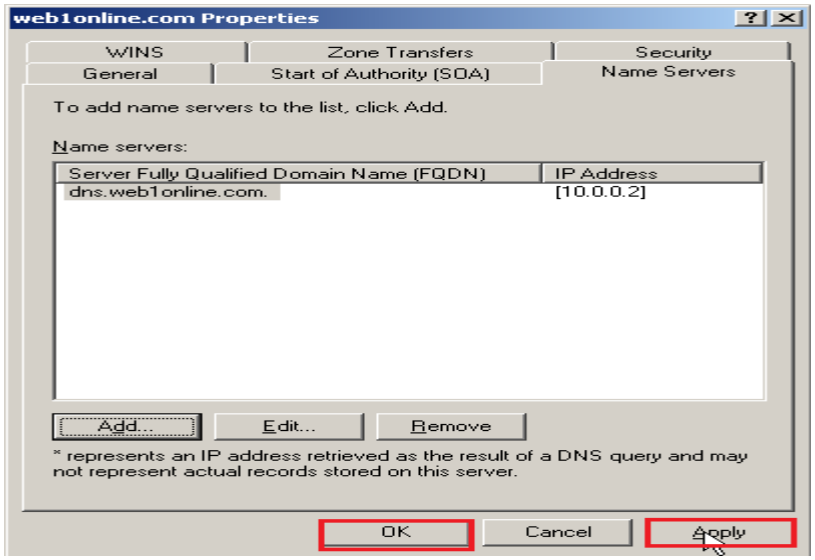
Click Remove



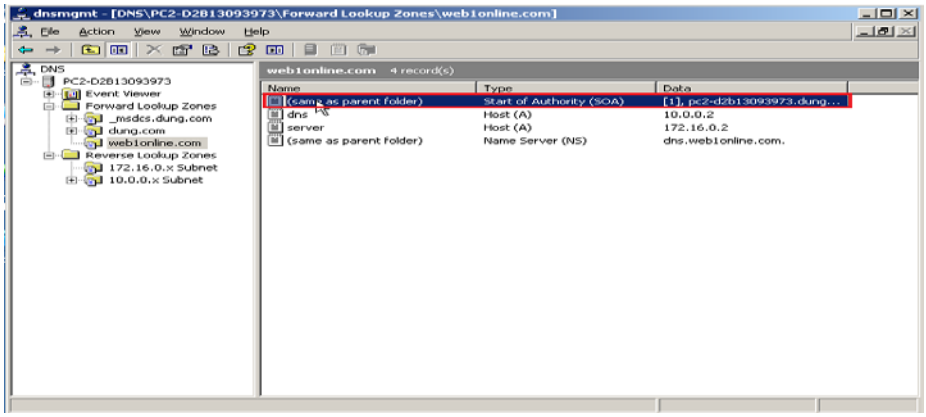
Click Add



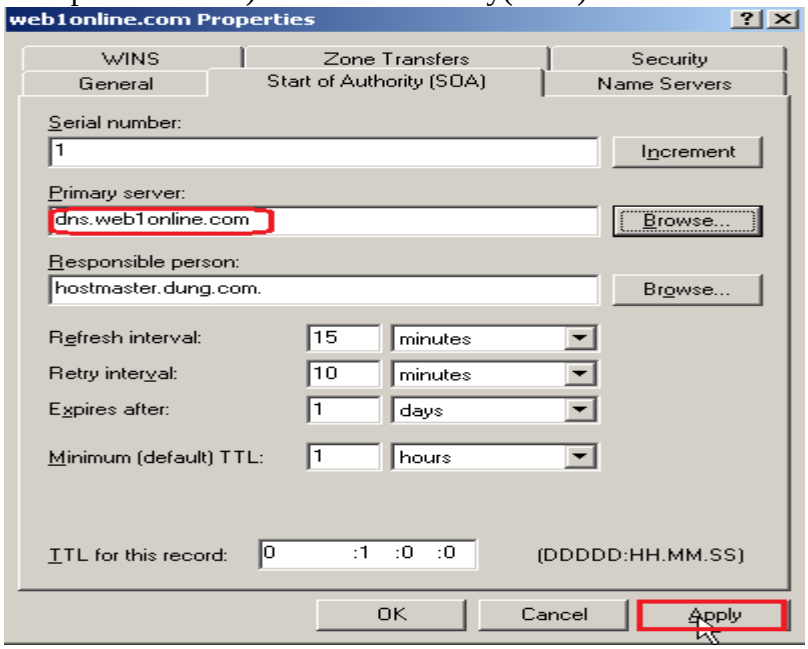
Click OK



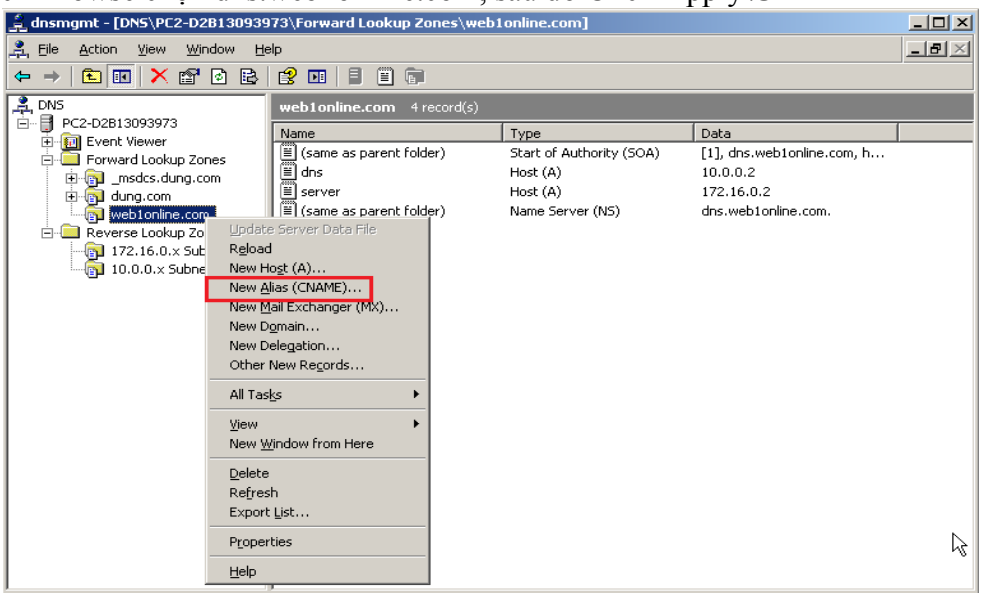
Click Apply\OK



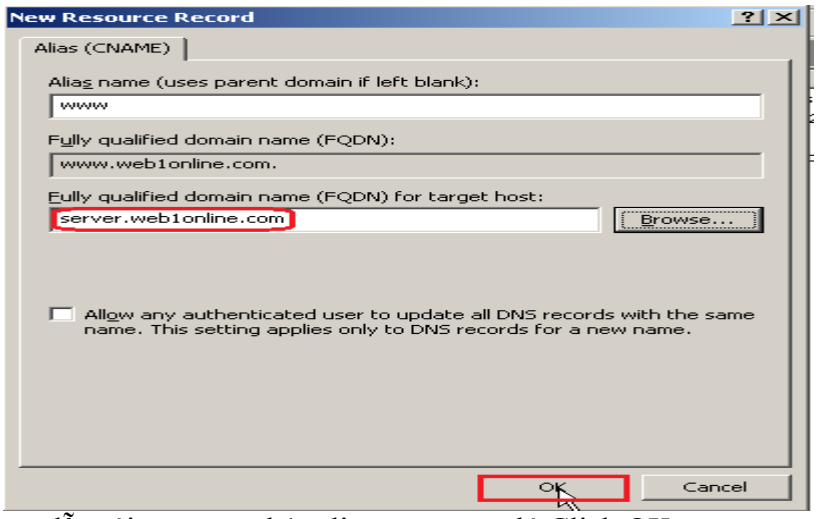
Click (same as parent forlder) start of Authority(SOA)…



Click Browse chọn dns.web1online.com, sau đó Click Apply\OK



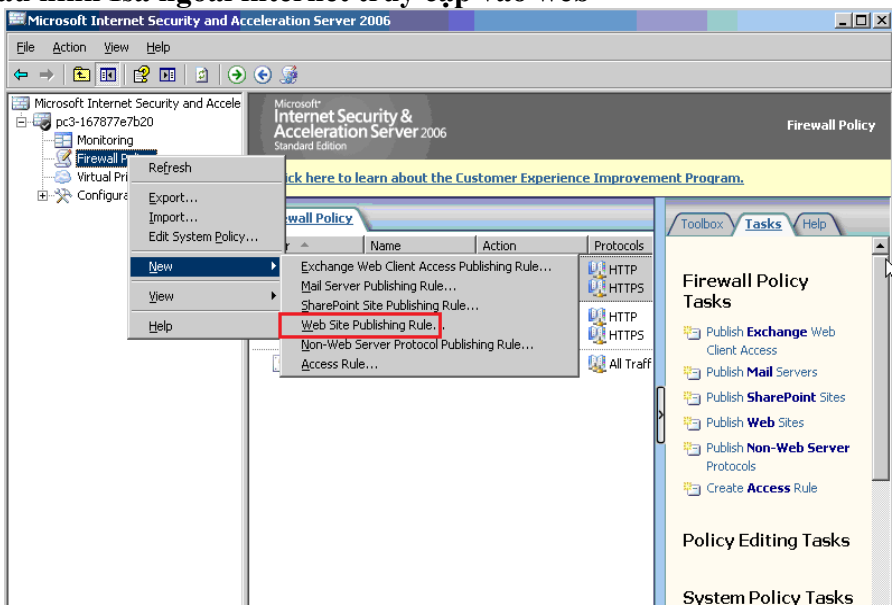
R_Click New Alias (CNAME)…



Chọn đường dẫn tới server.web1online.com, sau đó Click OK

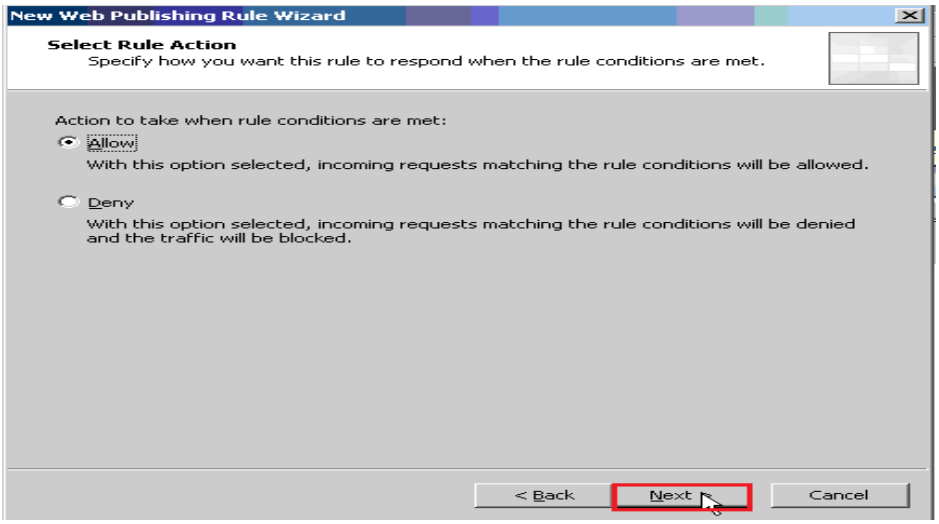
Trên thanh Address gõ địa chỉ http://www.web1online.com

6.5. Cấu hình Isa ngoài internet truy cập vào web

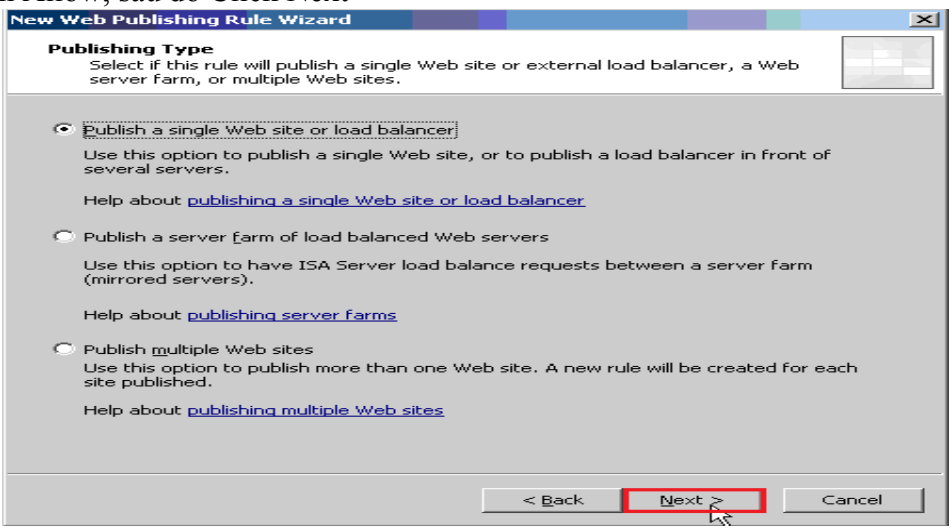


R_Click Firewall Polycy\New\Web Site Publishing Rule..

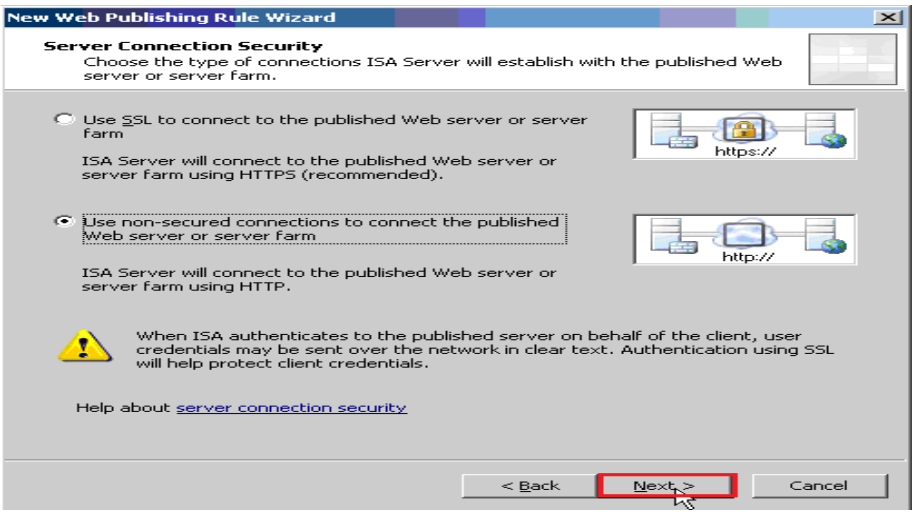
ClickNext



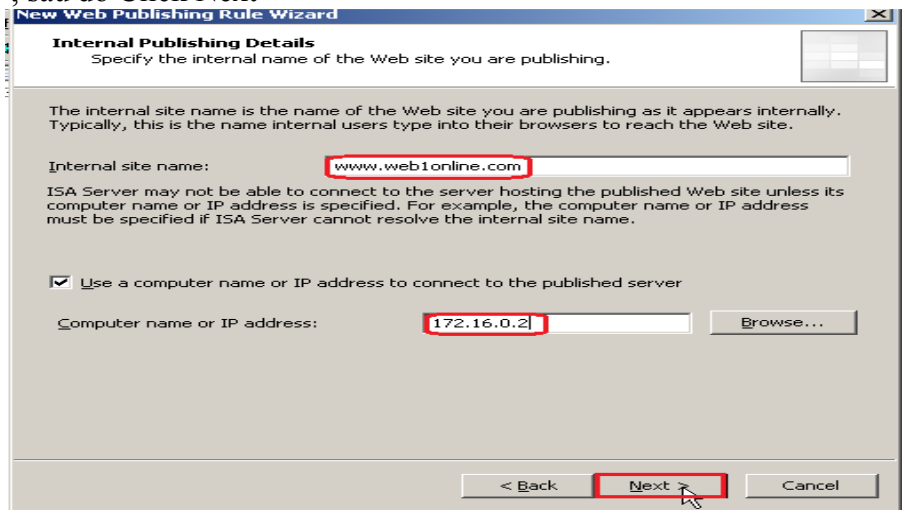
Chọn Allow, sau đó Click Next



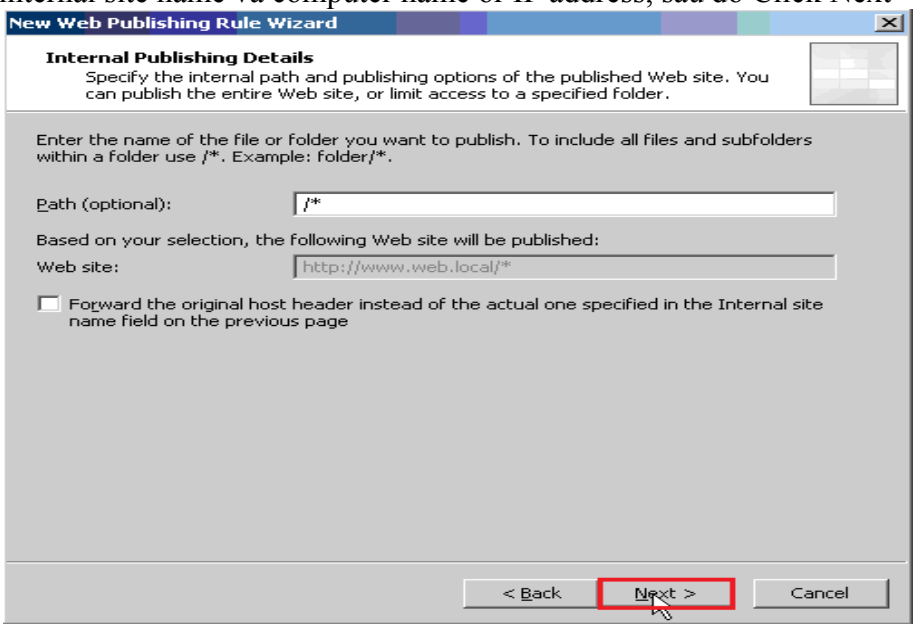
Chọn publish a single Web site or load balancer, sau đó Click Next



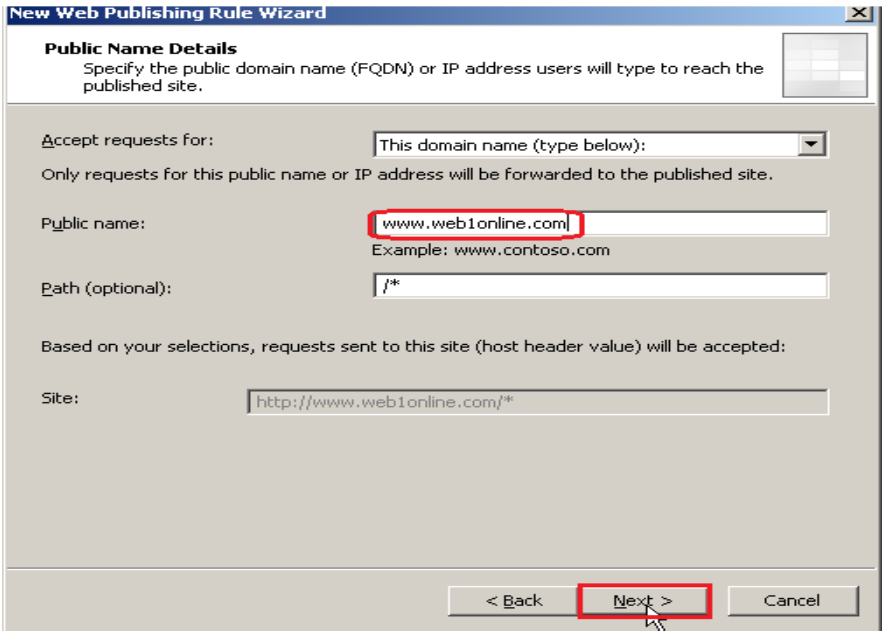
Chọn non-secured connetions to connect the published Web server or server using HTTP , sau đó Click Next



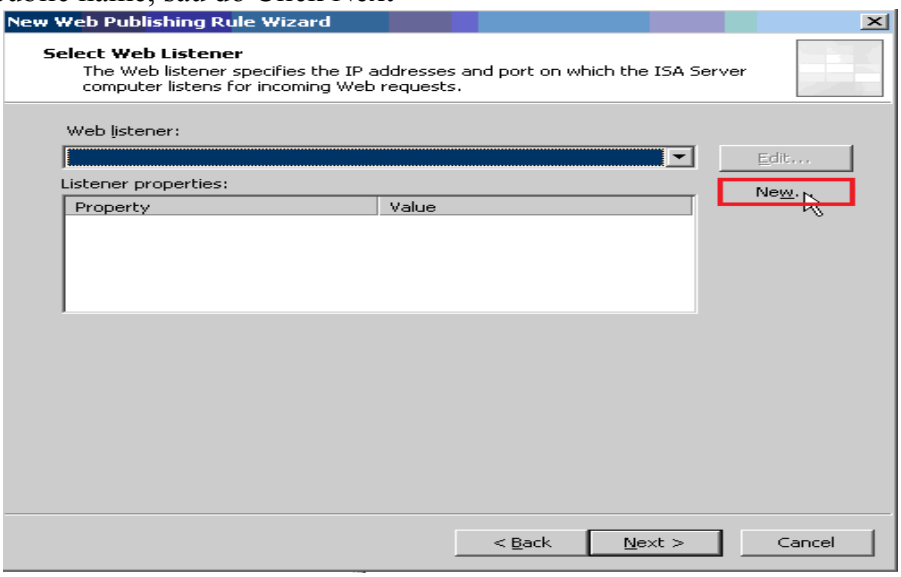
Điền internal site name và computer name or IP address, sau đó Click Next



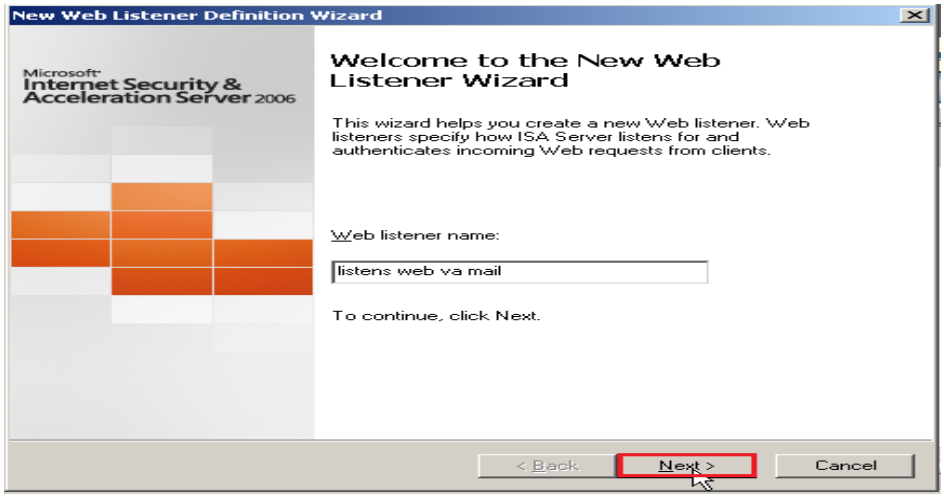
Điền path(optional), sau đó Click Next



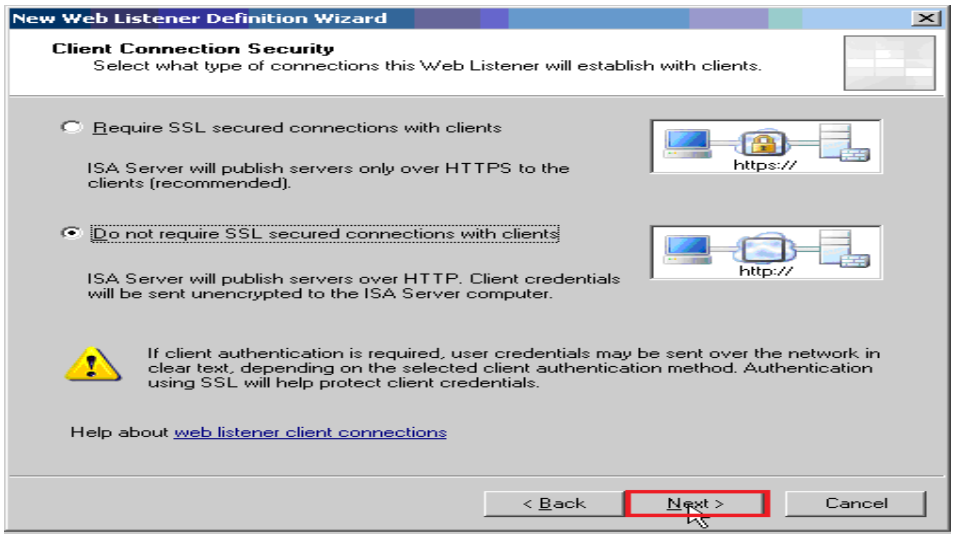
Điền public name, sau đó Click Next



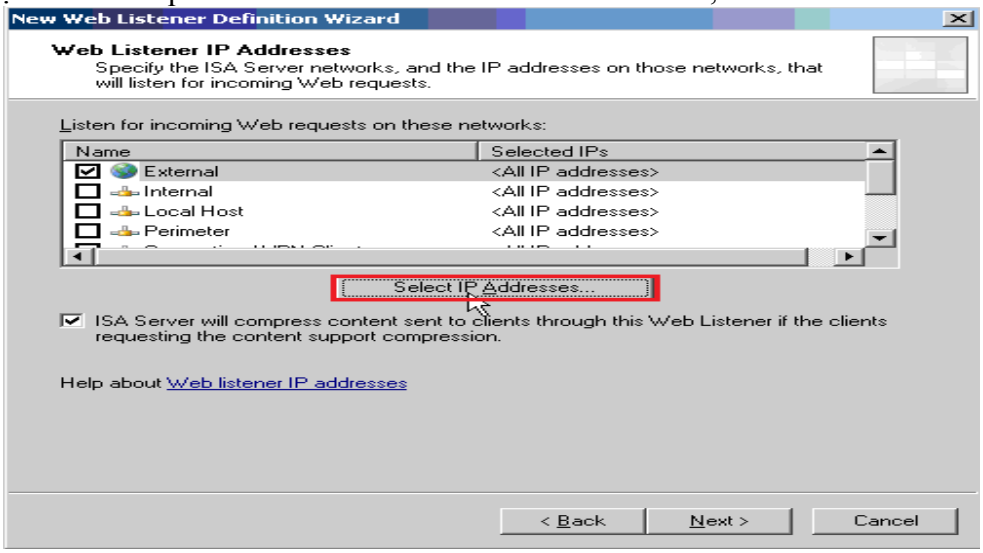
Click New



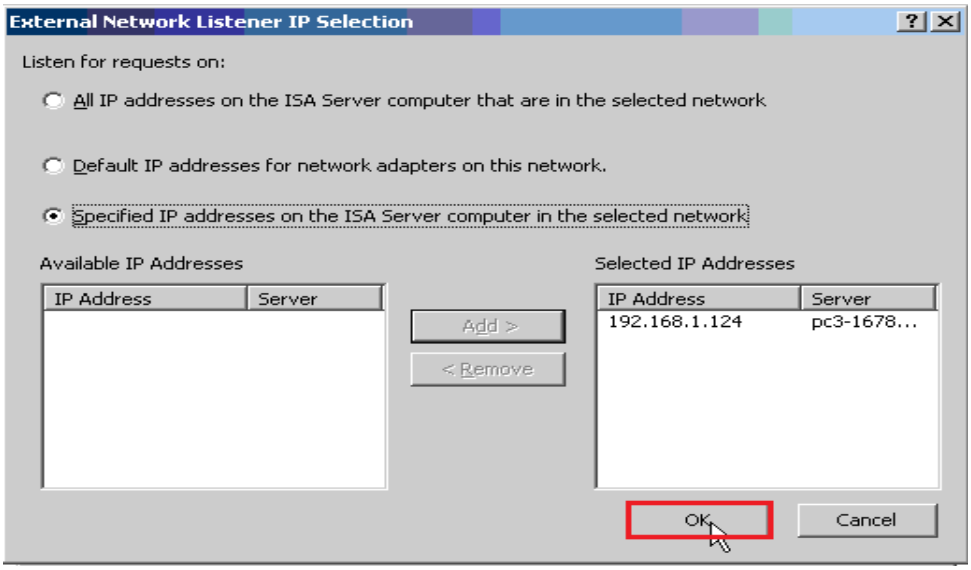
Click Next



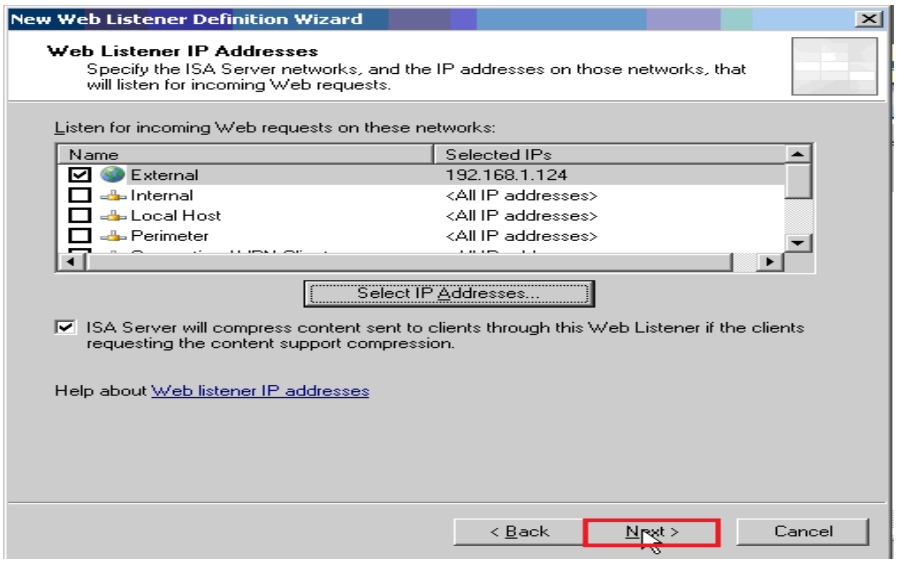
Chọn Do not require SSL sercured connection with clients, sau đó Click Next



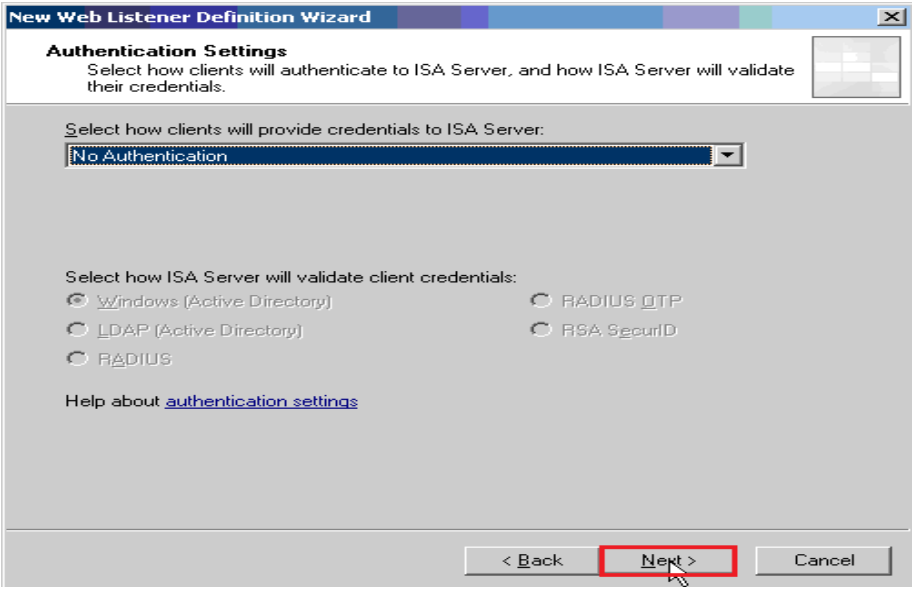
Click Select IP addresses…



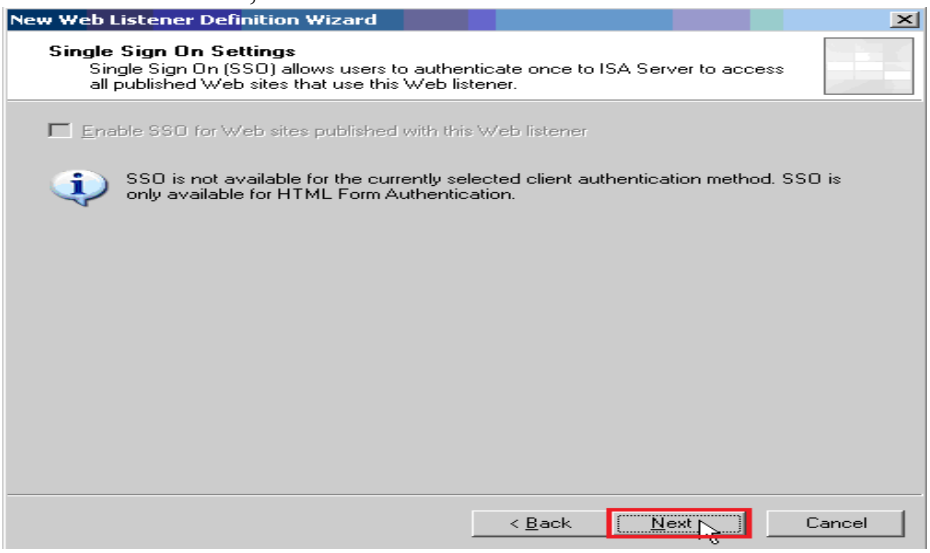
Click OK



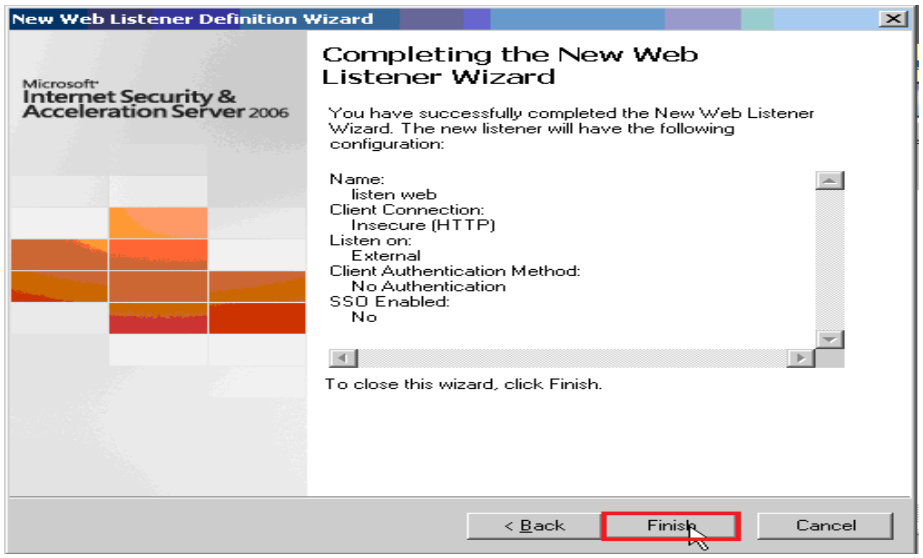
Click Next



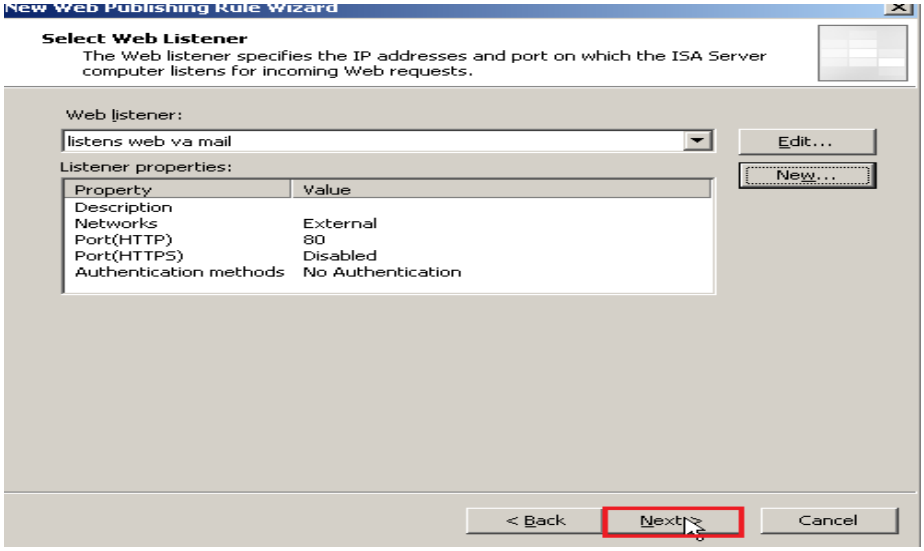
Chọn No Authentication, sau đó Click Next



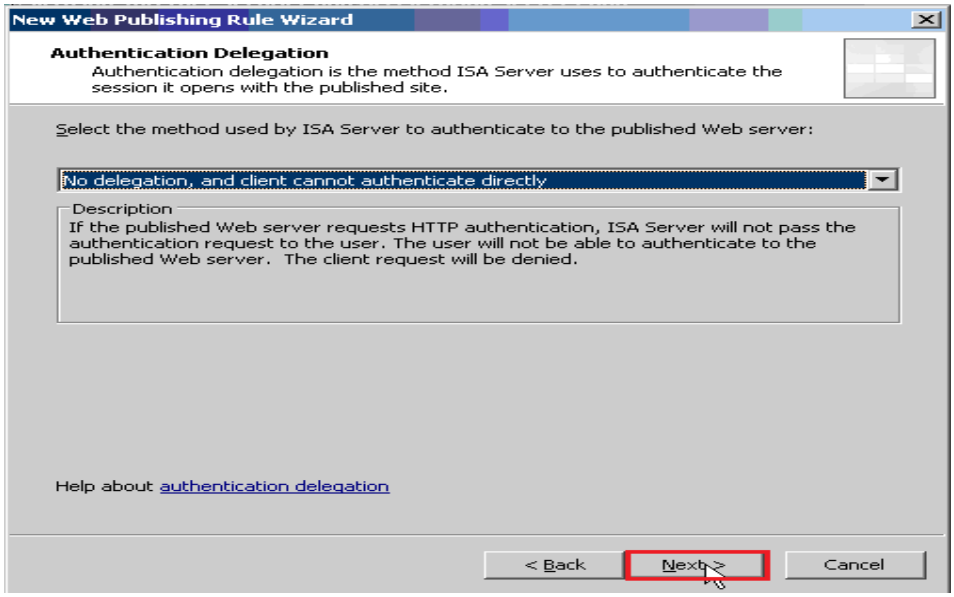
Click Next



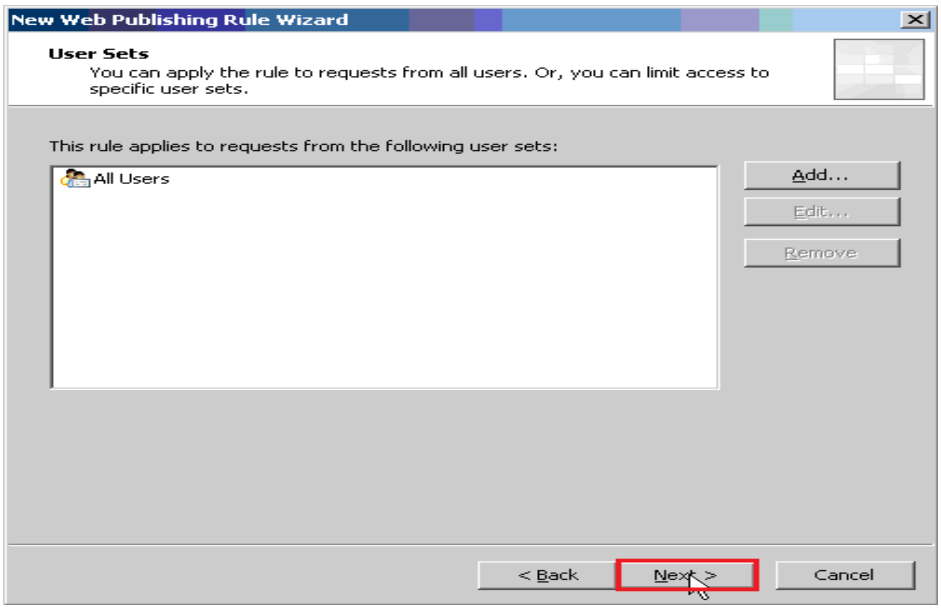
Click Finish



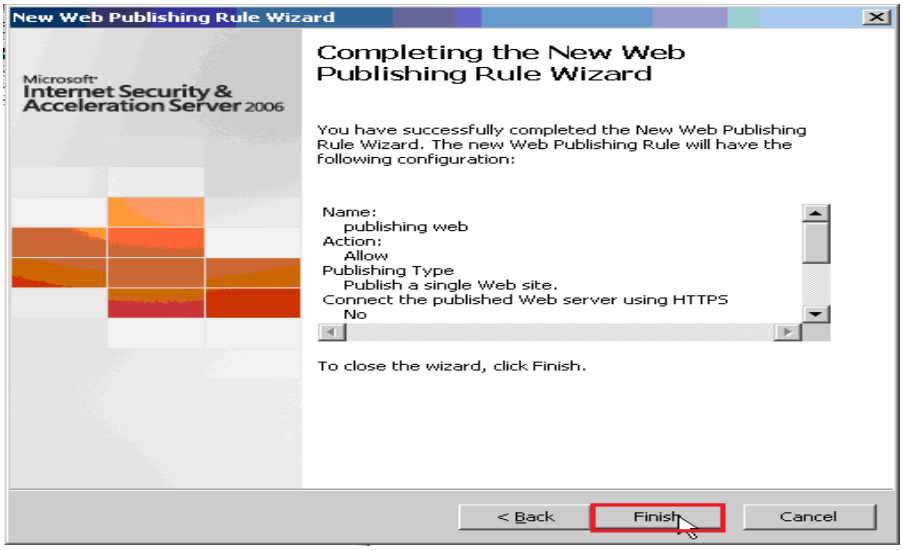
Click Next



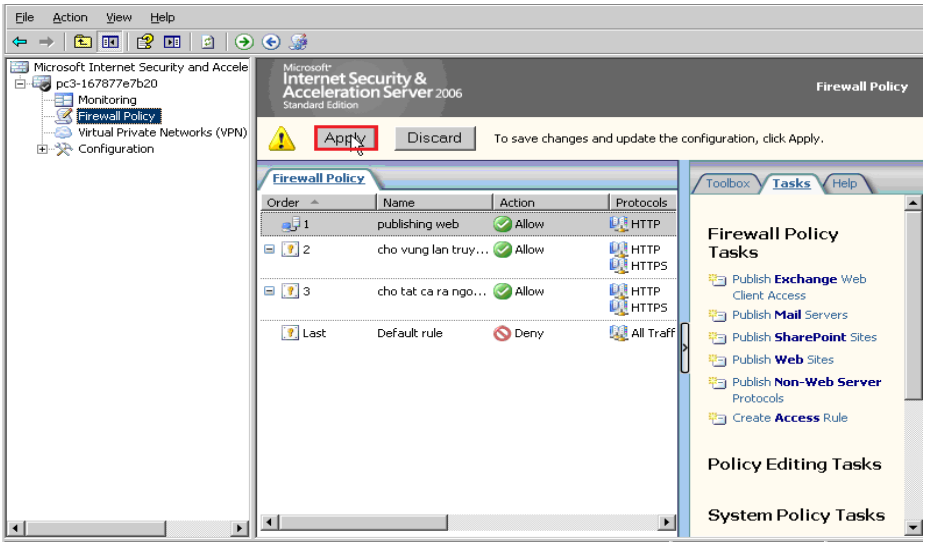
Click Next



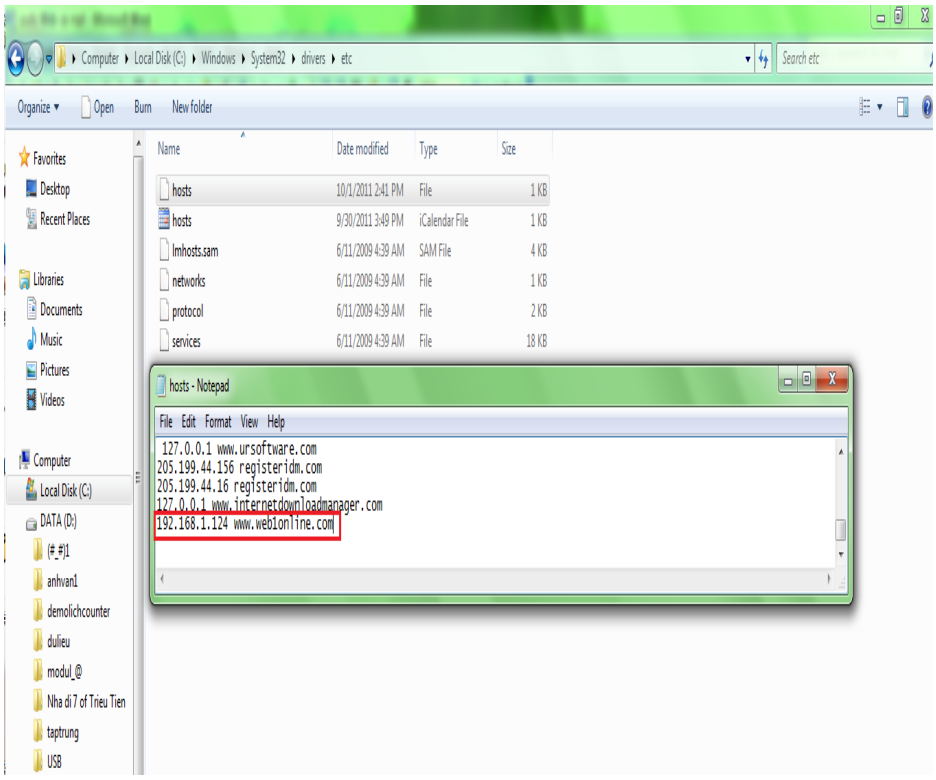
Click Next



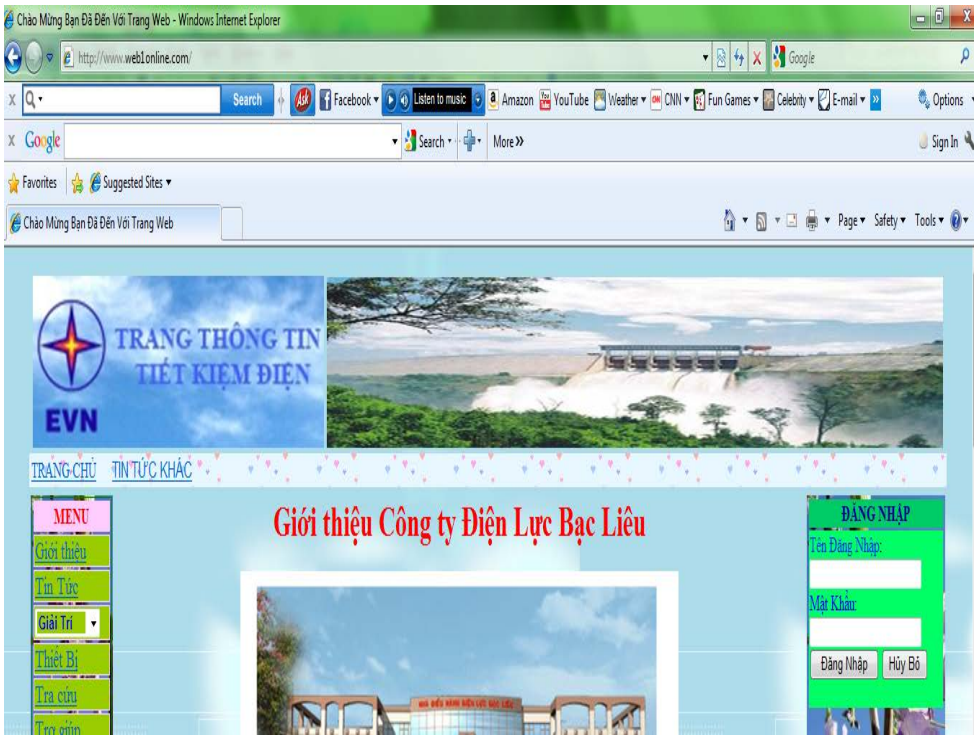
Click Finish



Click Apply



Vào File host phân giải tên miền 192.168.1.124 thành www.web1online.com

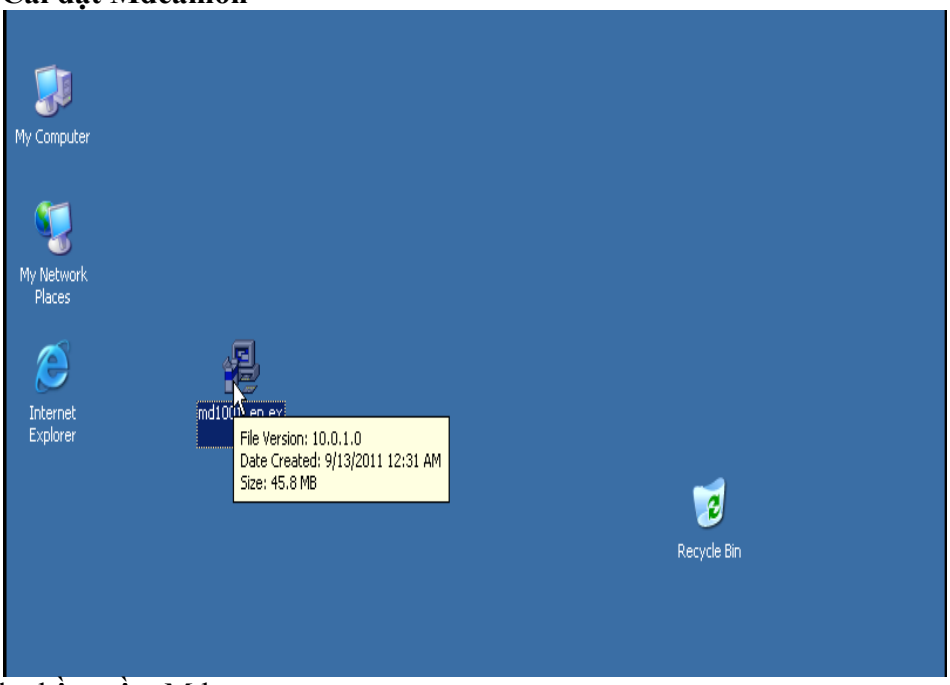


Trên thanh Address gõ địa chỉ http://www.web1online.com

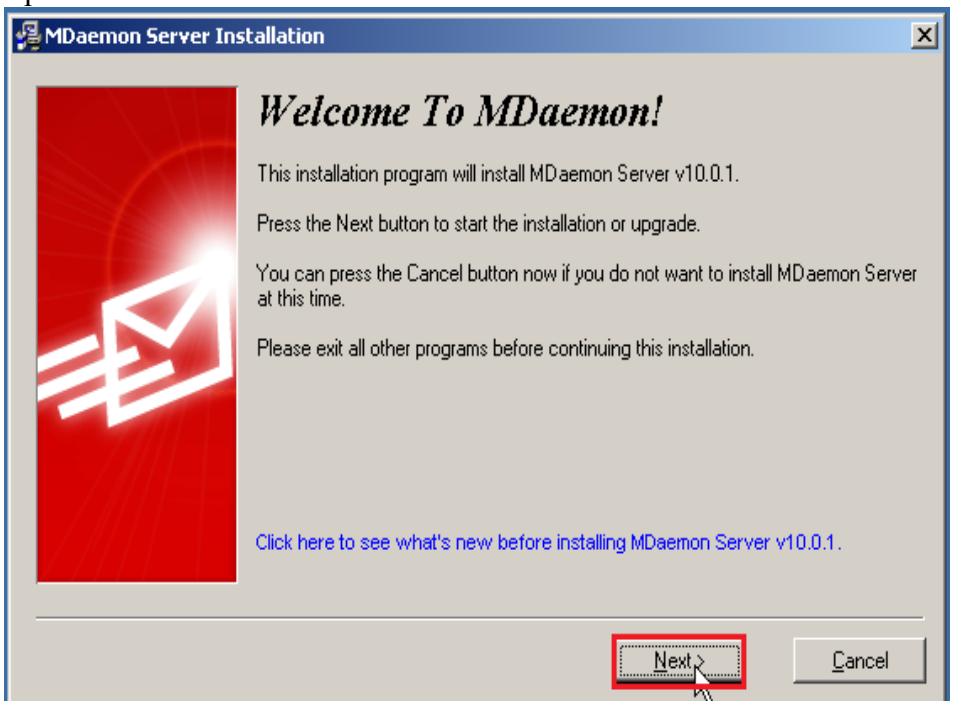
7. Public mail Mdeamon

Bảo vệ hệ thống Mail Server là một chức năng chính của ISA Server với một số công nghệ tập chung vào việc tăng cường bảo mật cho Mail Server khi xuất bản ra Internet, ISA đã trở thành giải pháp Firewall số một để triển khai dịch vụ mail của Microsoft. Trong phần này, chúng ta tiến hành cài đặt và public mail Mdeamon.

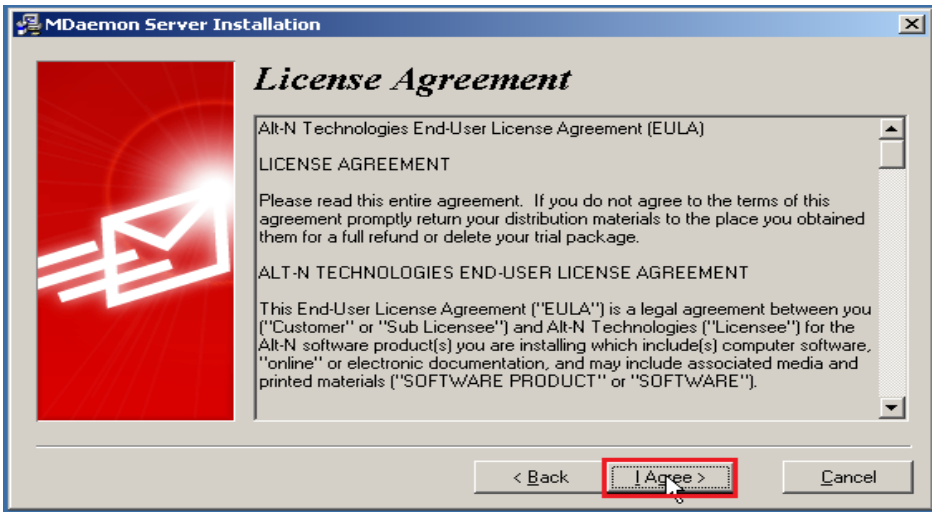
7.1. Cài đặt Mdeamon



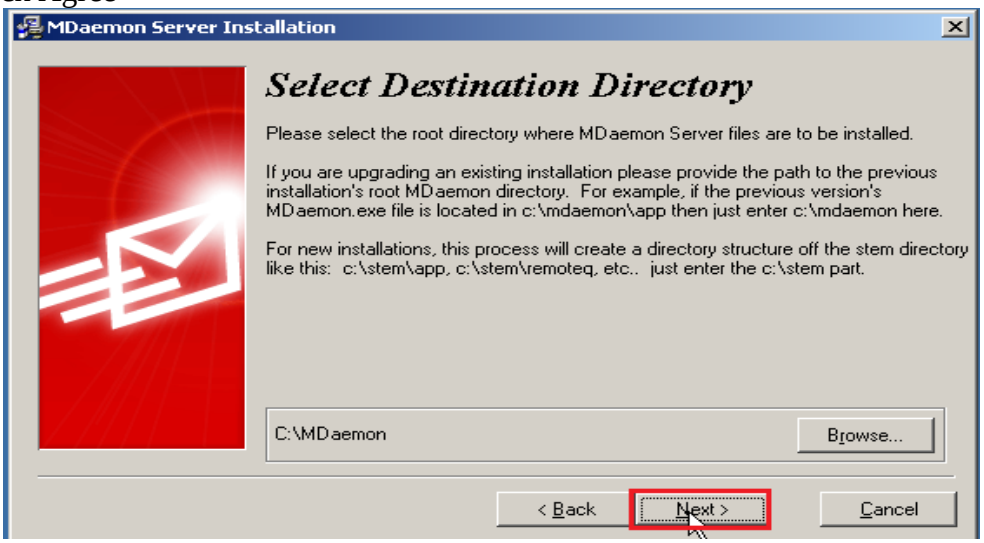
Click phần mềm Mdmeamon



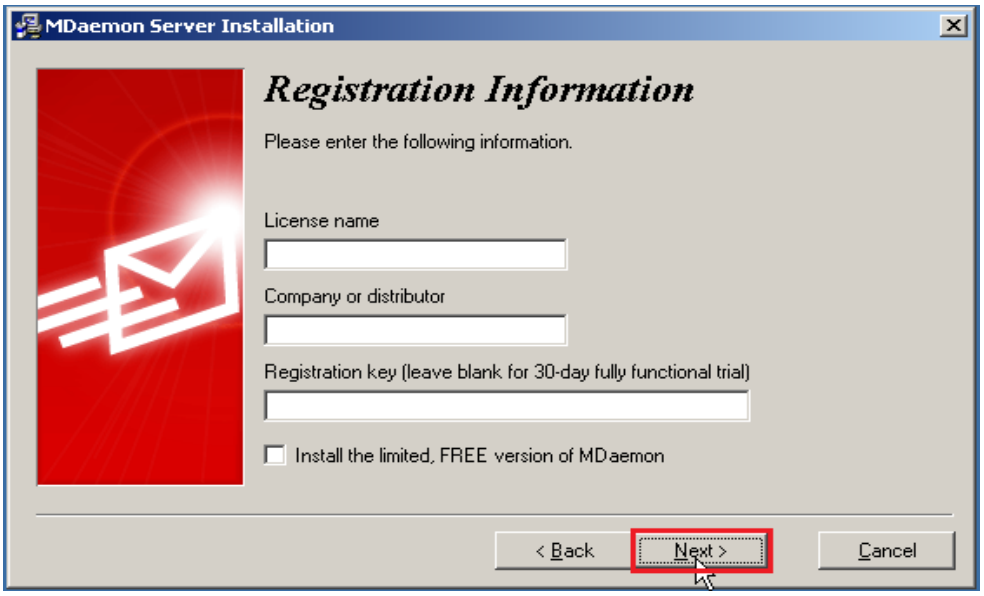
Click Next



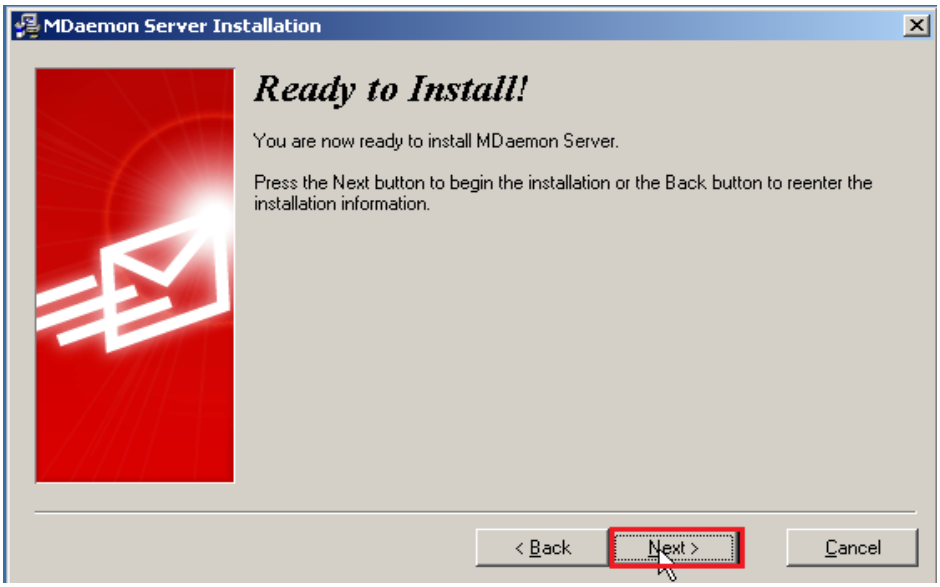
Click Agree



Click Next



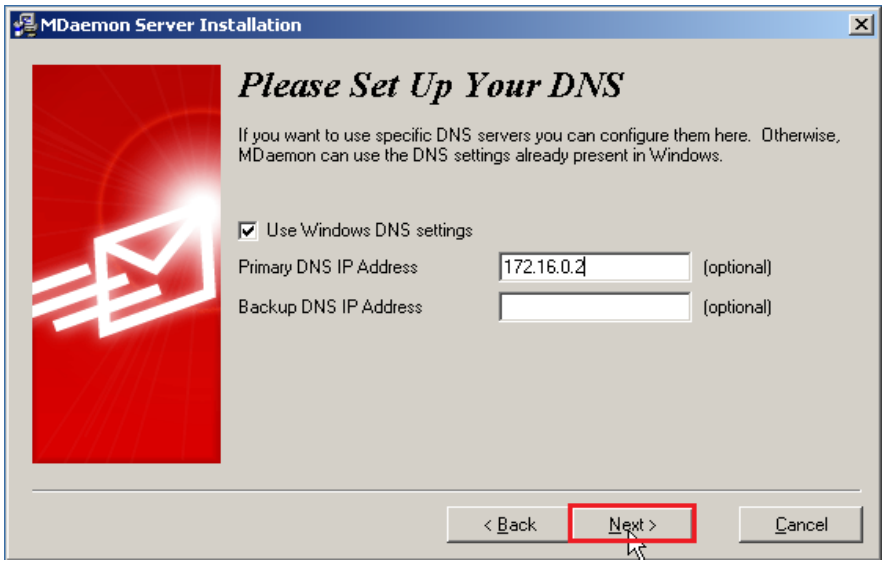
Click Next



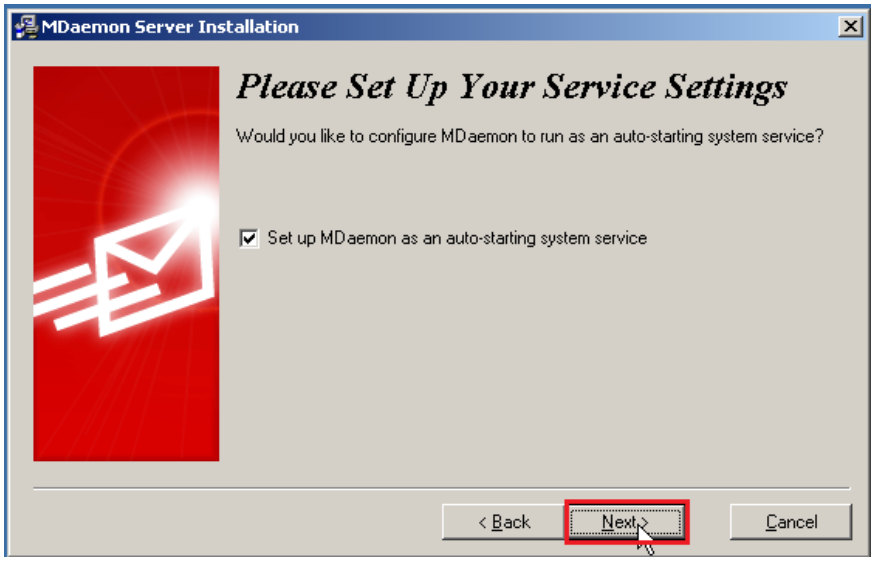
Click Next

Điền tên Domain, sau đó Click Next

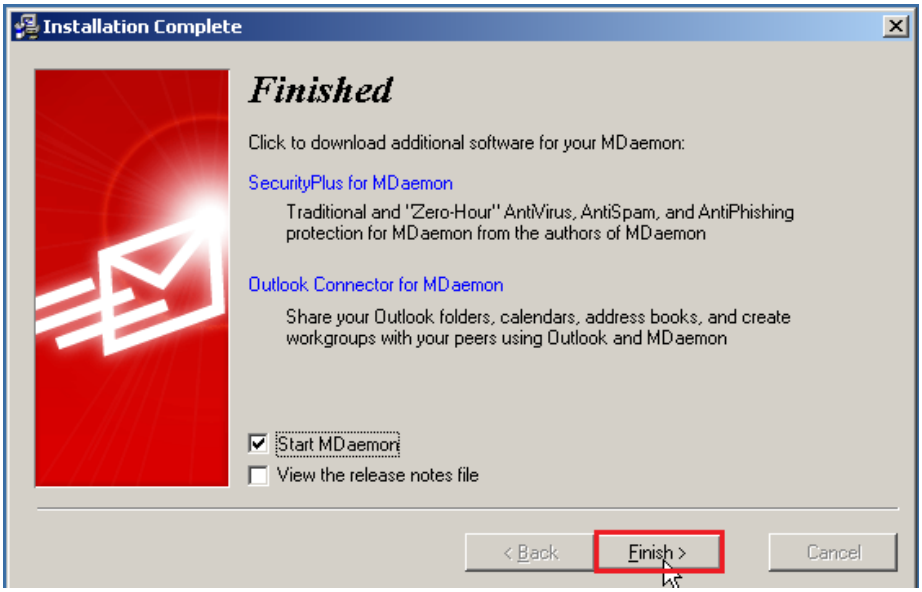
Click Next



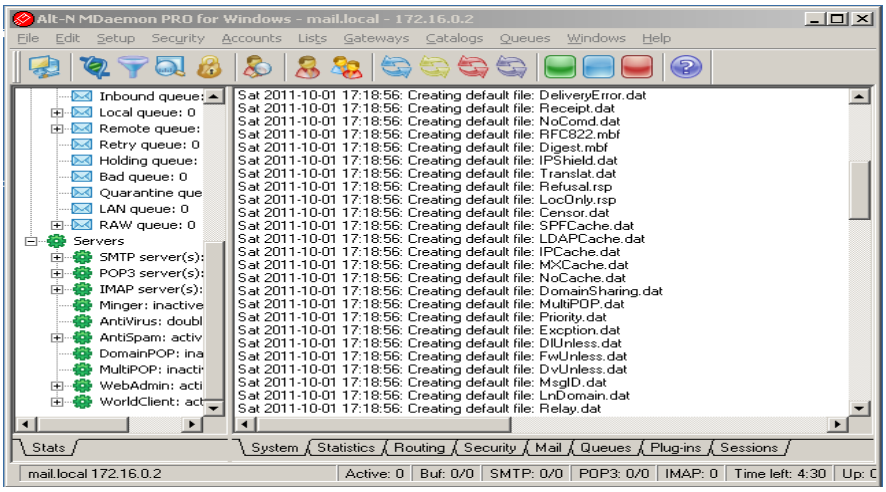
Click Next



Click Next

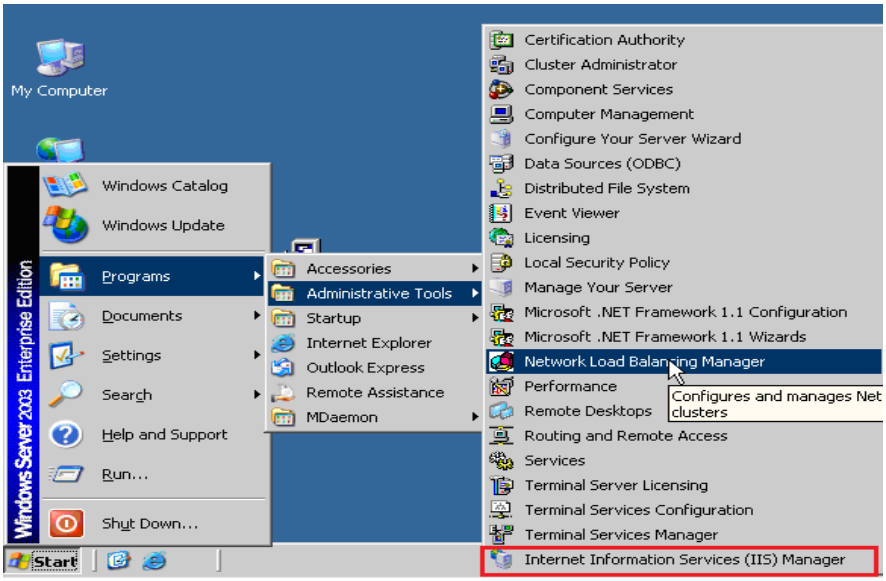


Click Finish

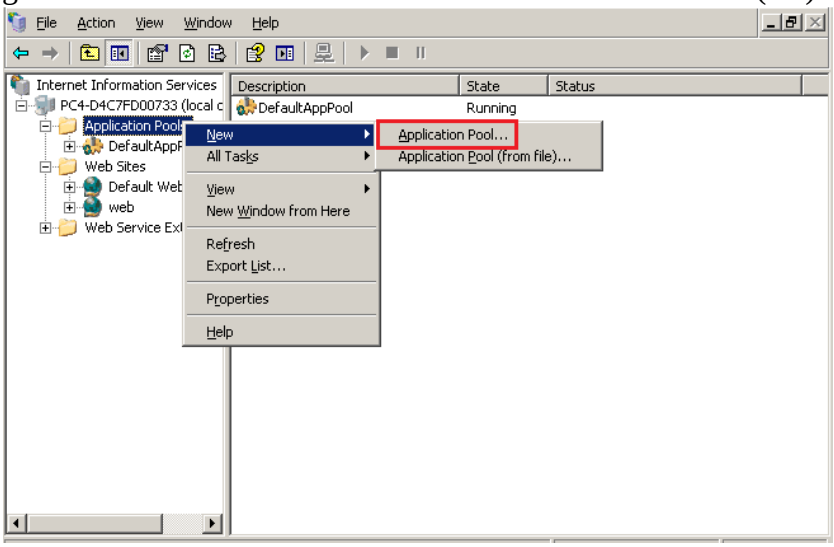


Bên trên là giao diên Mail Mdeamon

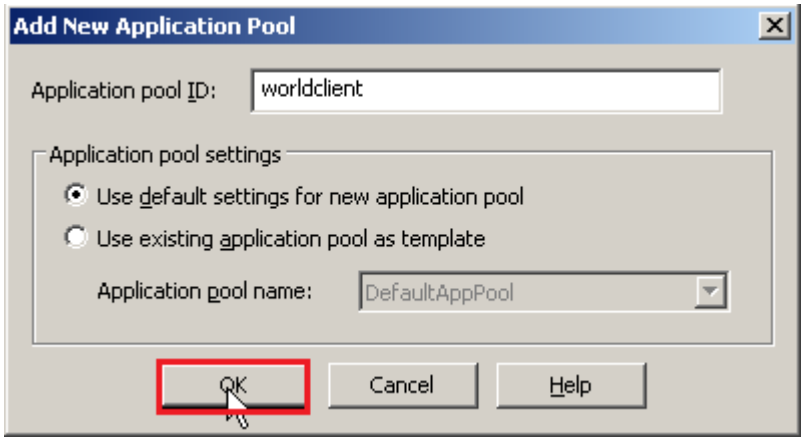
7.2. cấu hình WebMail



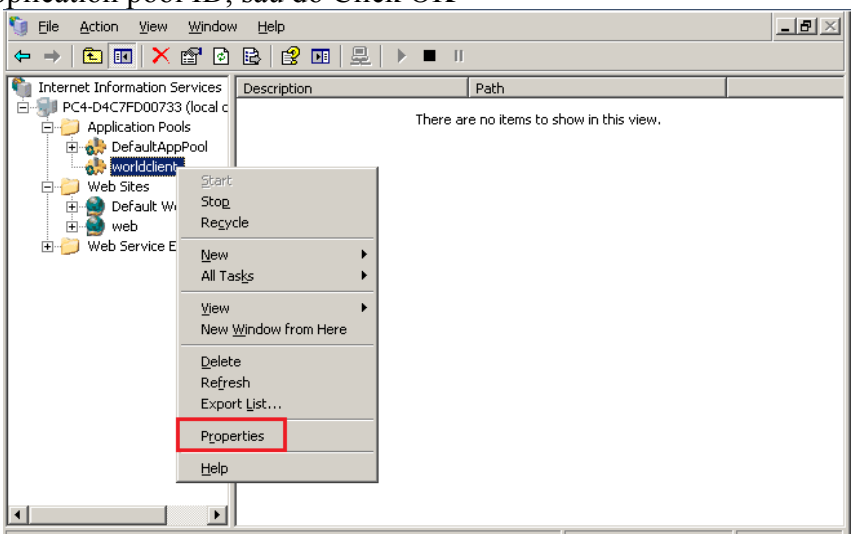
Start\Programs\Administrative Tools\ Internet Information Services(IIS)Manager



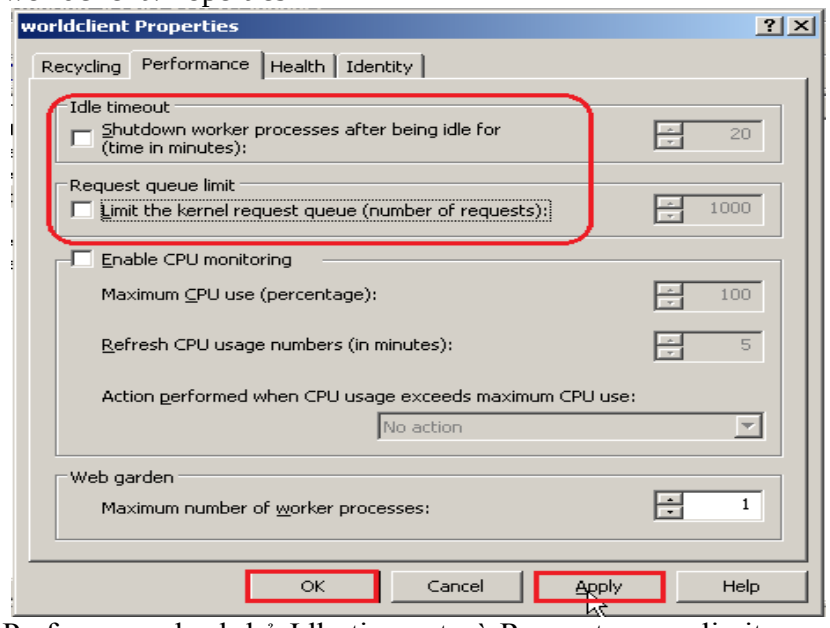
R_Click Application Pools\New\Application Pool…



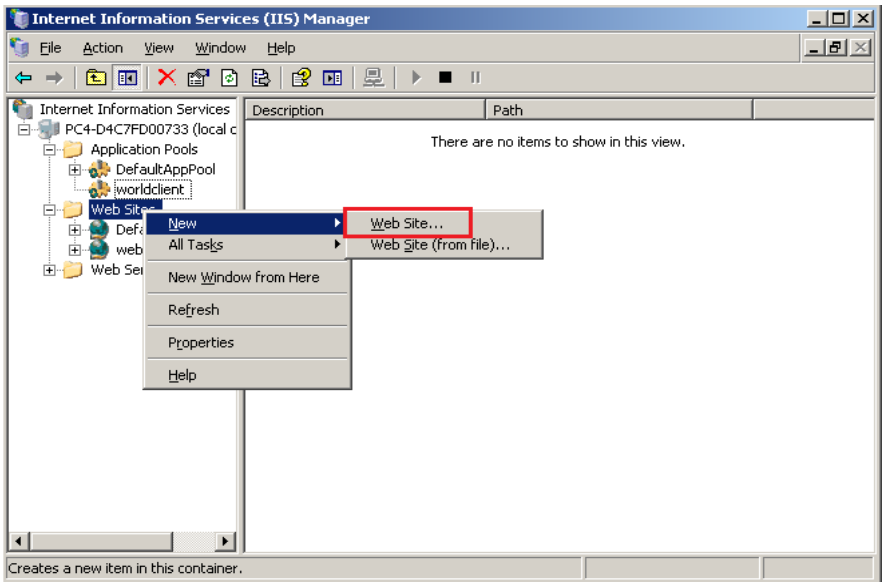
Điền Application pool ID, sau đó Click OK



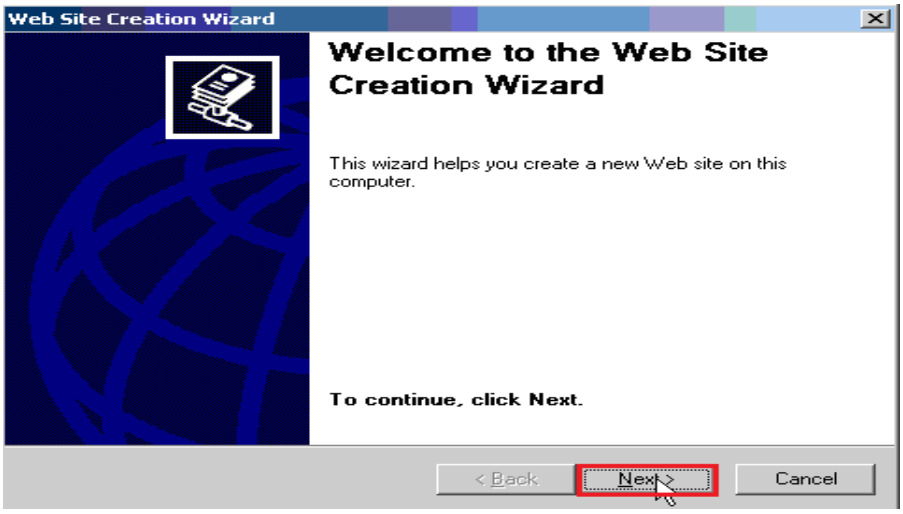
R_Click worldclient\Properties



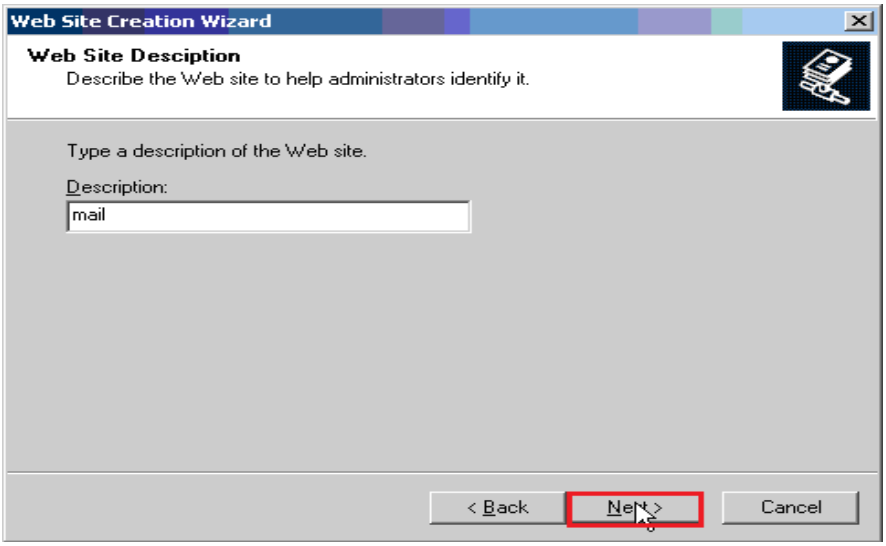
Vào tab Performace check bỏ Idle timeout và Request queue limit, sau đó Click Apply\OK



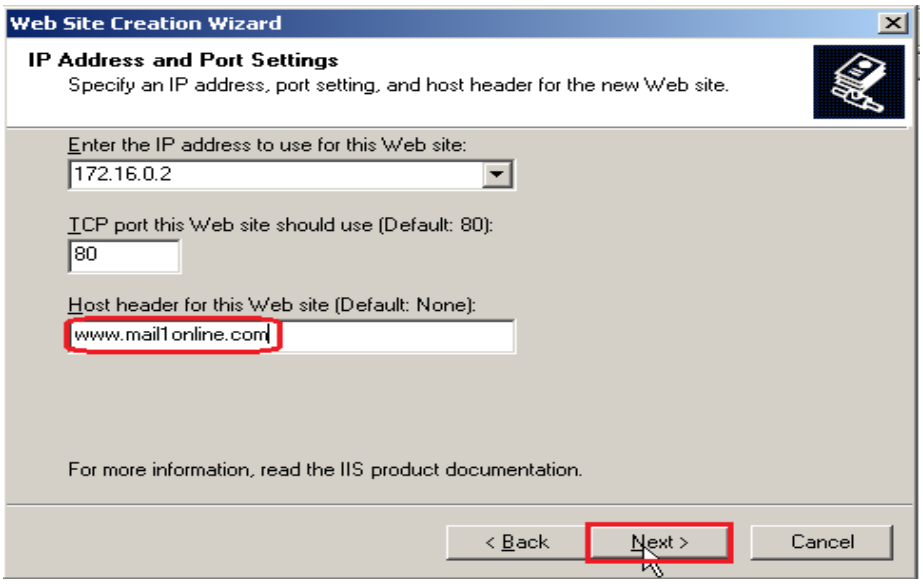
R_Click Web Sites\New\Web Site…



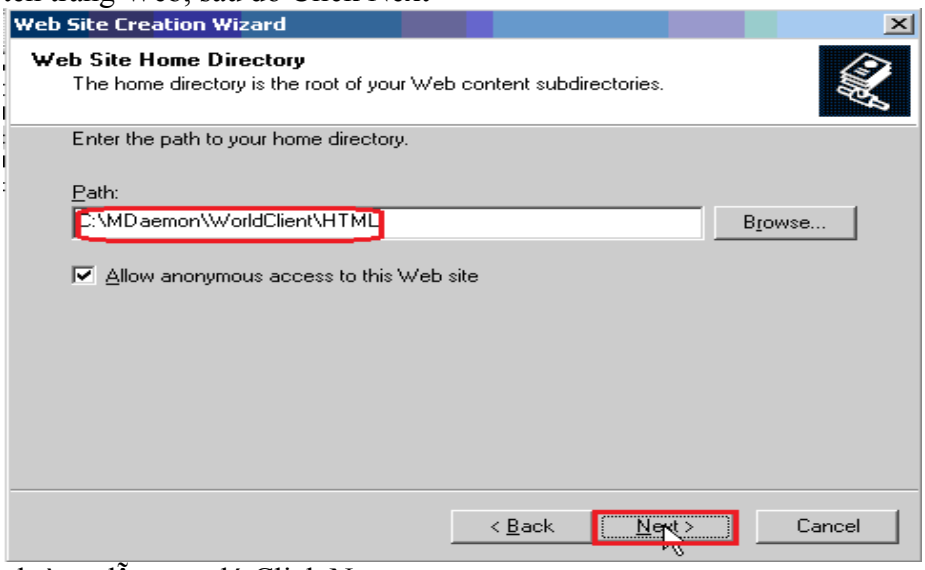
Click Next



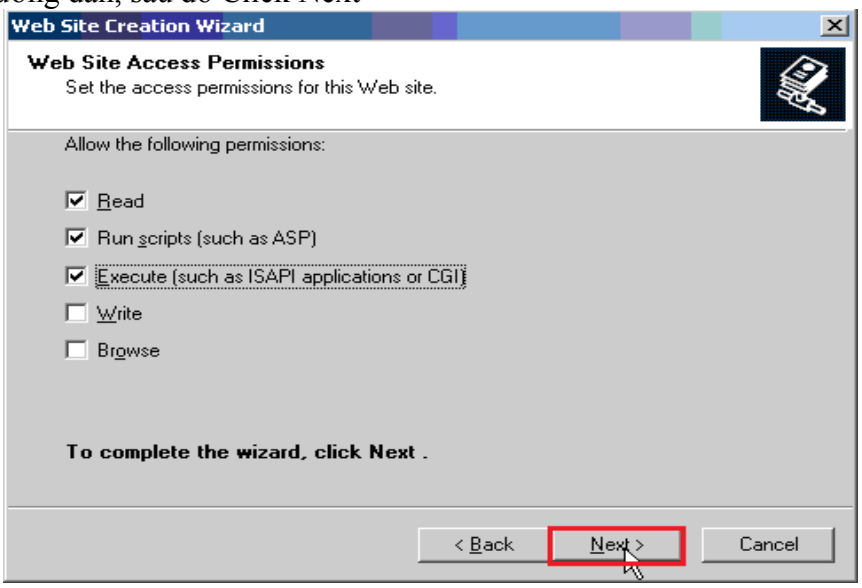
Click Next



Điền tên trang Web, sau đó Click Next

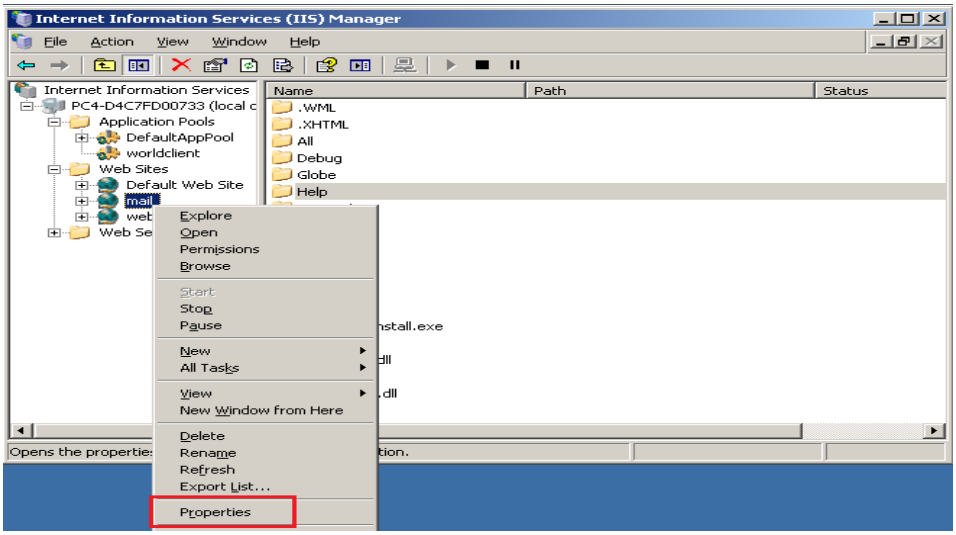


Chọn đường dẫn, sau đó Click Next

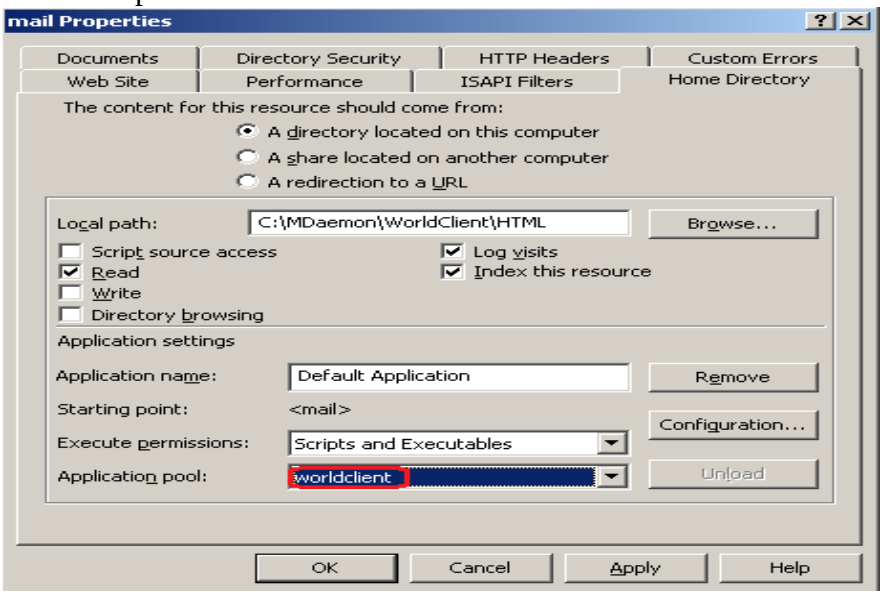


Click Next

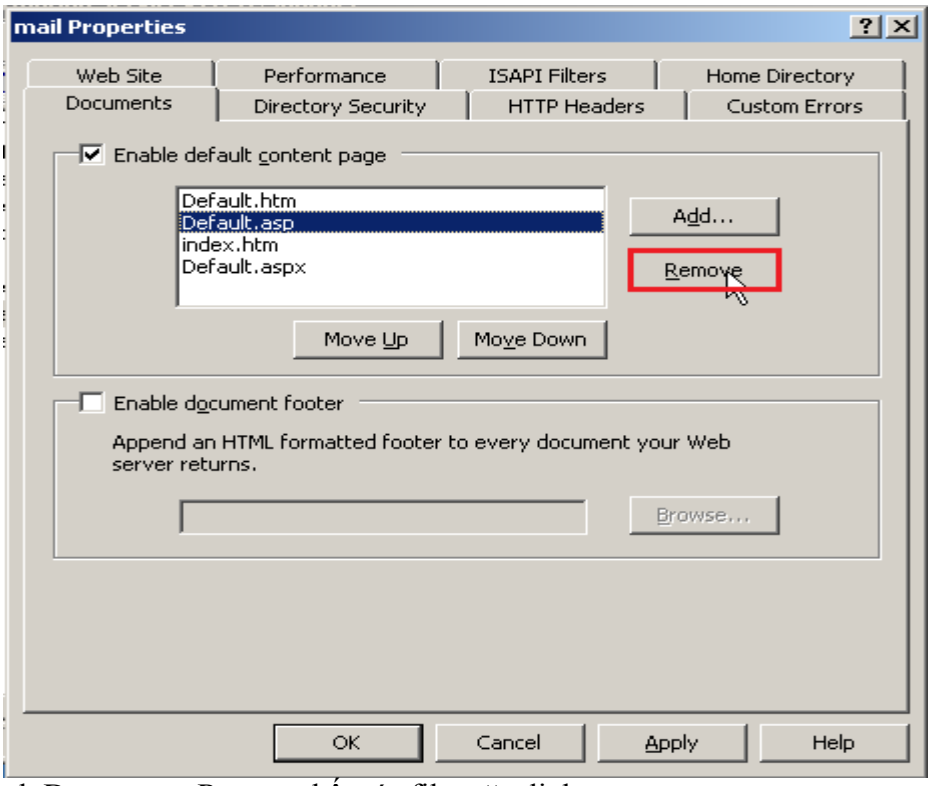
Click Finish



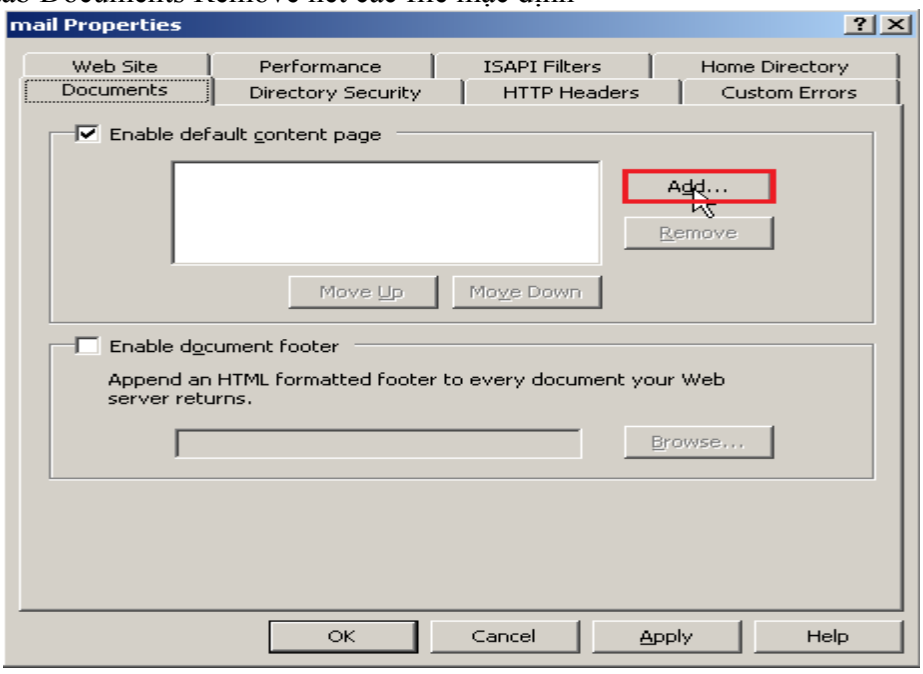
R_Click mail\Properties



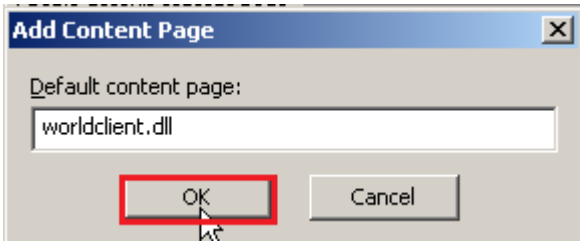
Vào tab Home Directory chọn wordclient



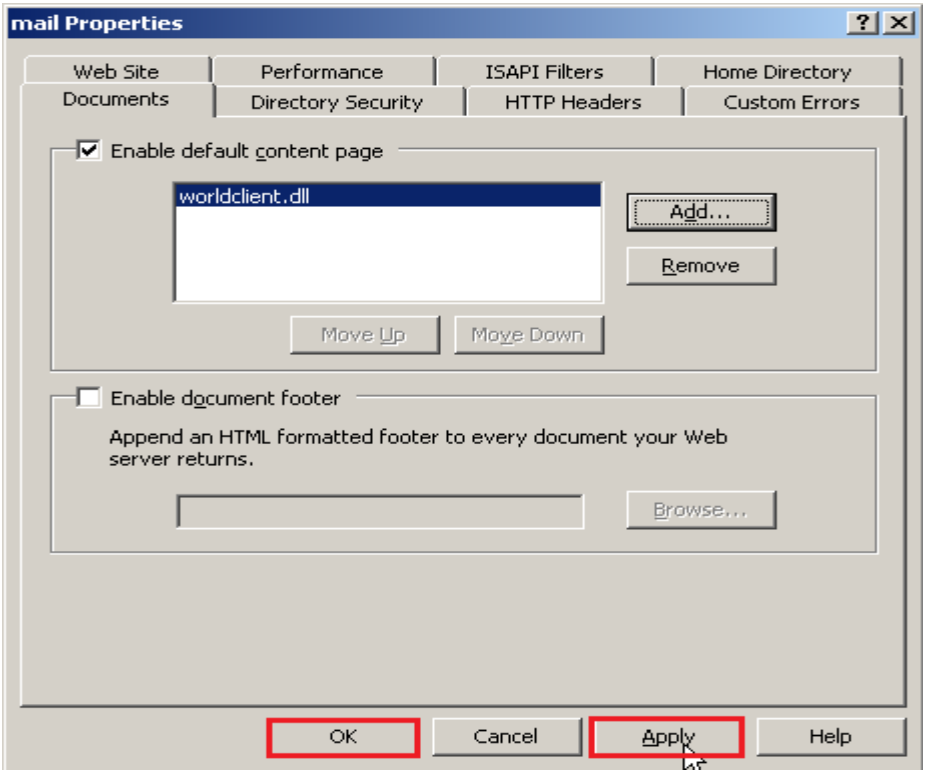
Vào tab Documents Remove hết các file mặc định



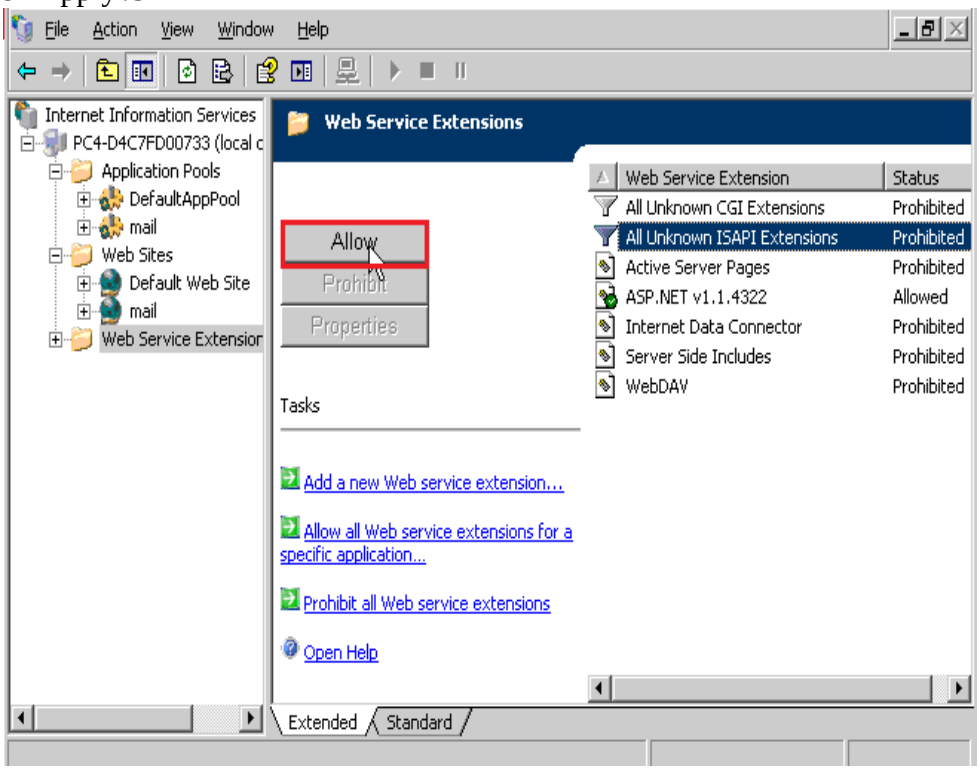
Click Add



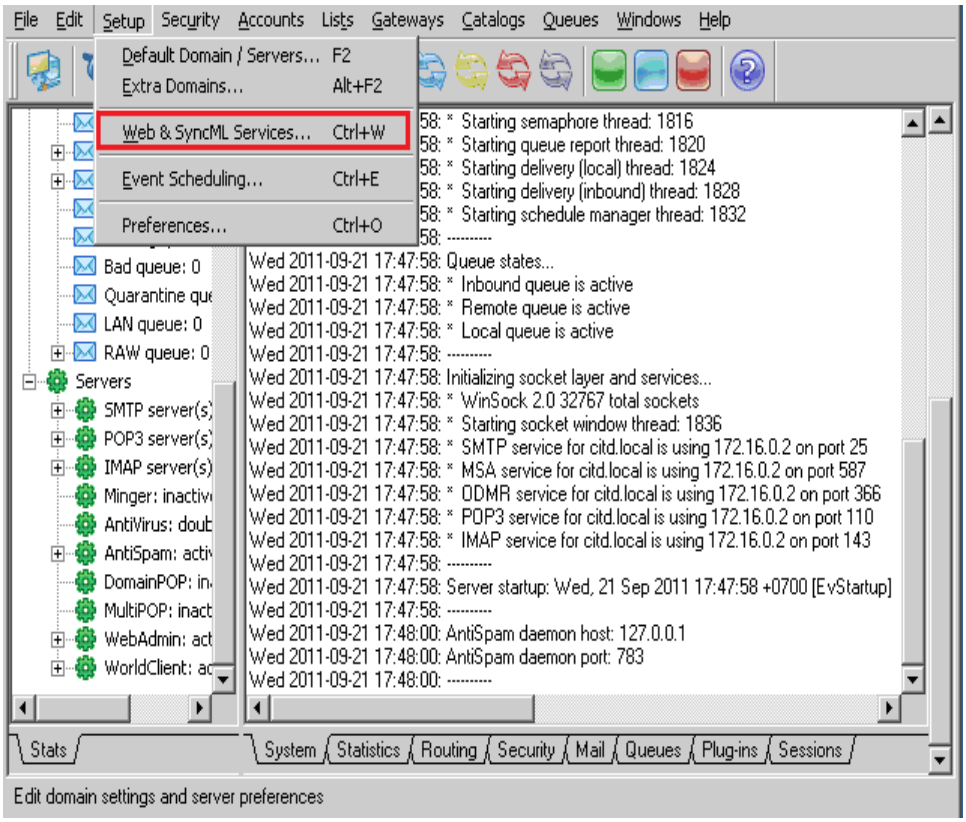
Click OK



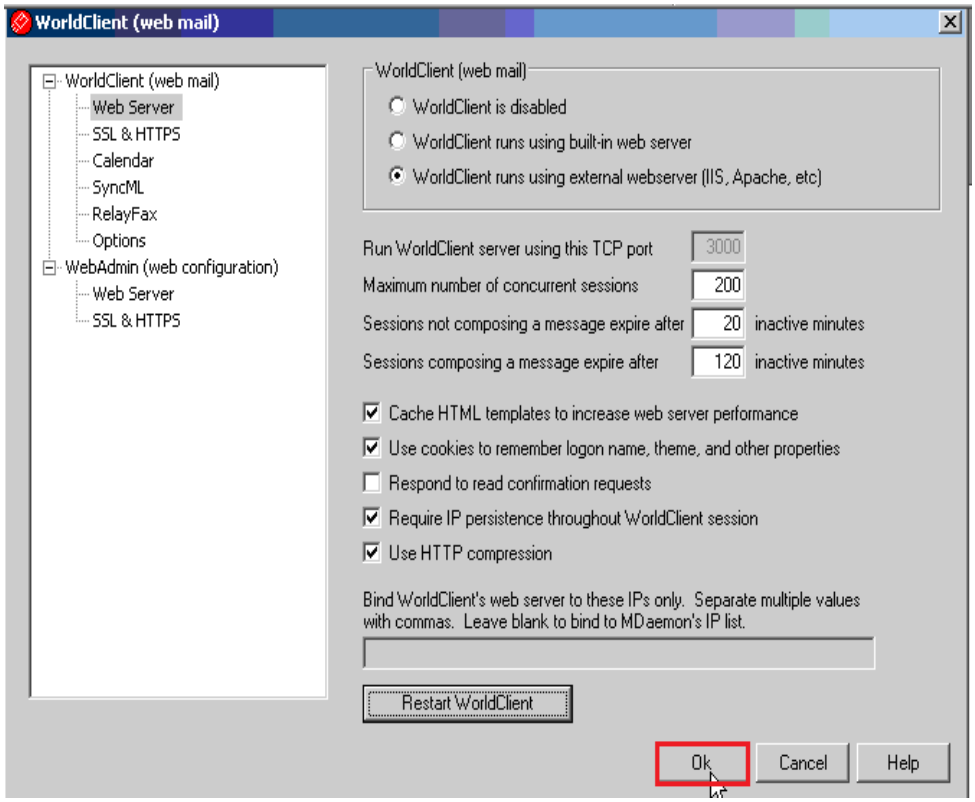
Click Apply\OK



Web service Extension\All Unknown ISAPI Extensions\ Click Allow

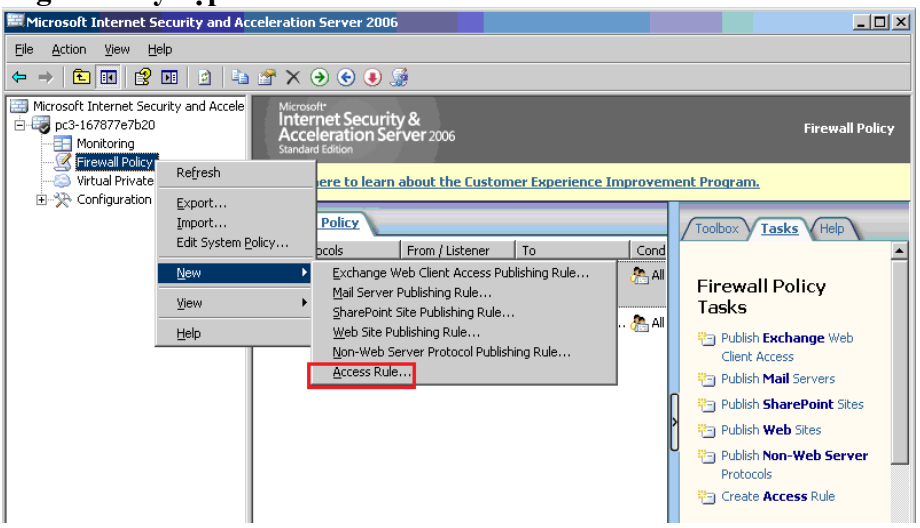


Setup\Web & SynML Servies

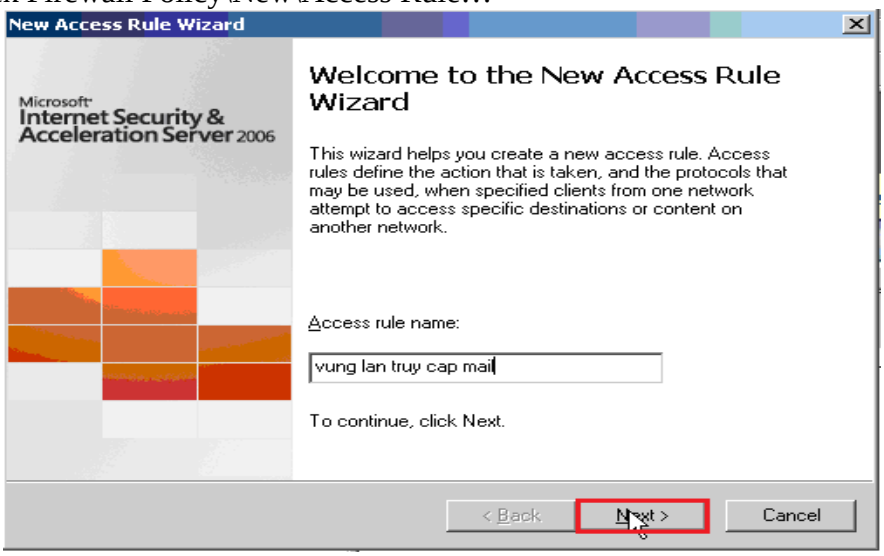


Chọn worldClient runs using external webserver (IIS, Apache, etc), sau đó Click OK

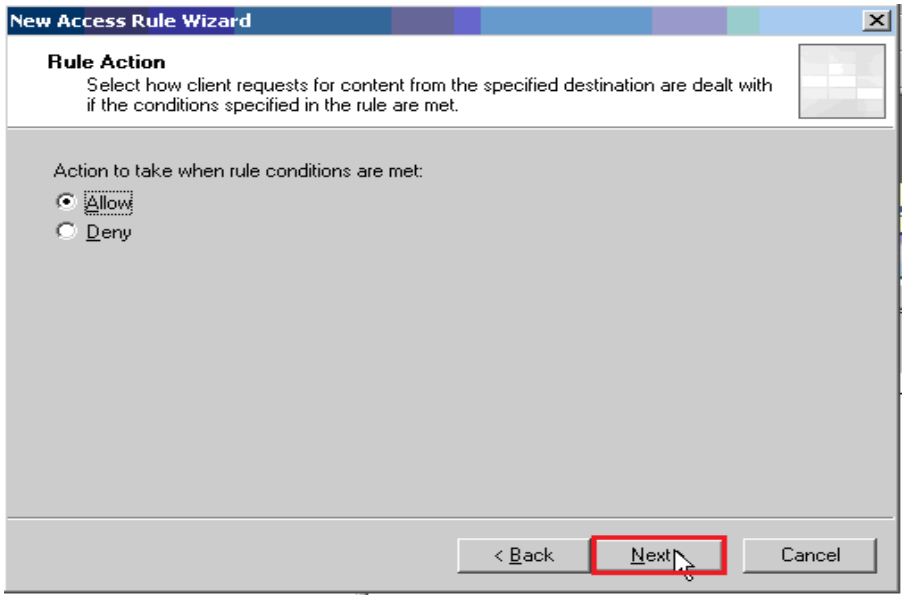
7.3.Vùng lan truy cập mail



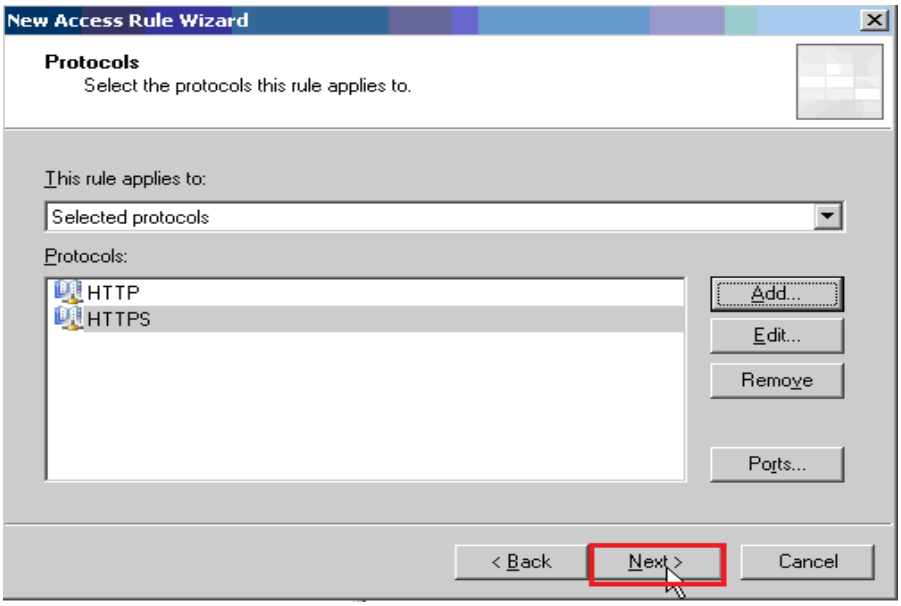
R_Click Firewall Policy\New\Access Rule…



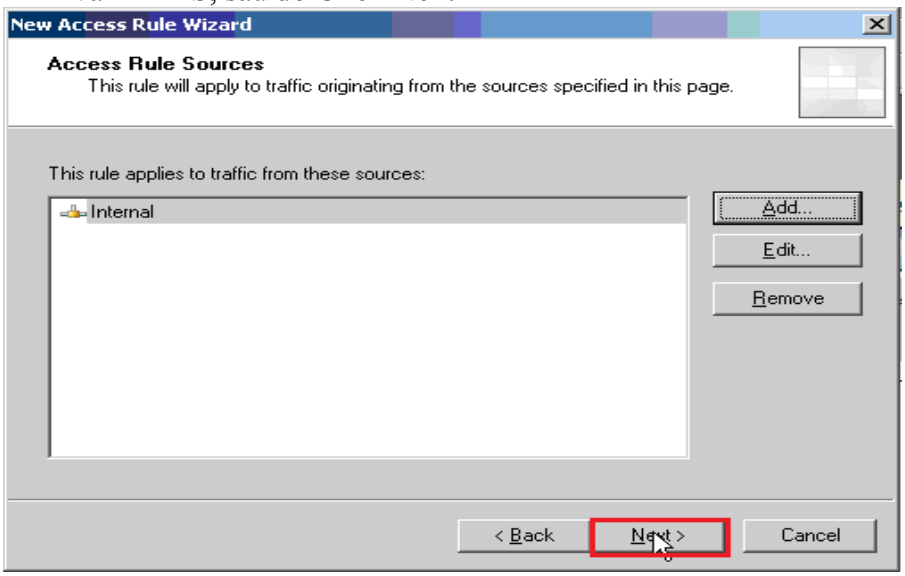
Next



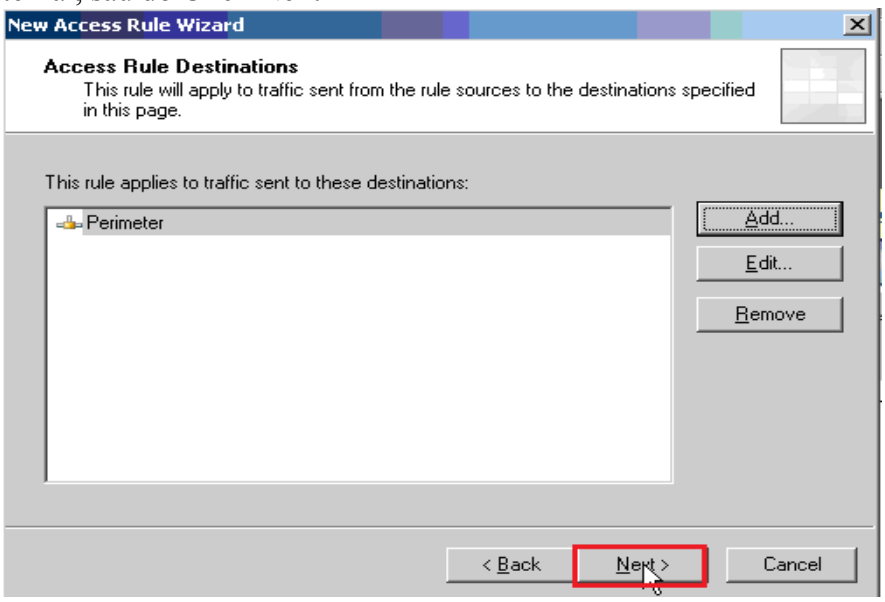
Next



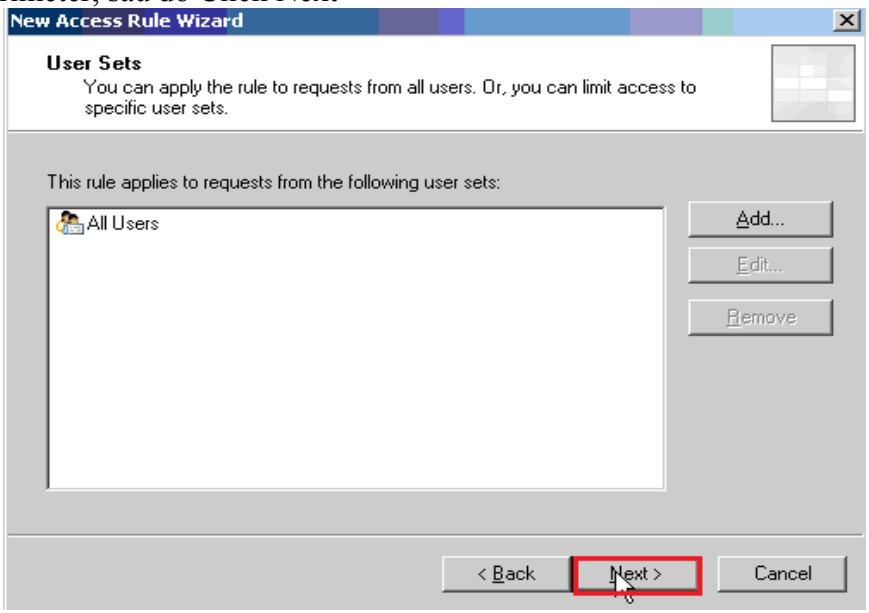
Add HTTP và HTTPS, sau đó Click Next



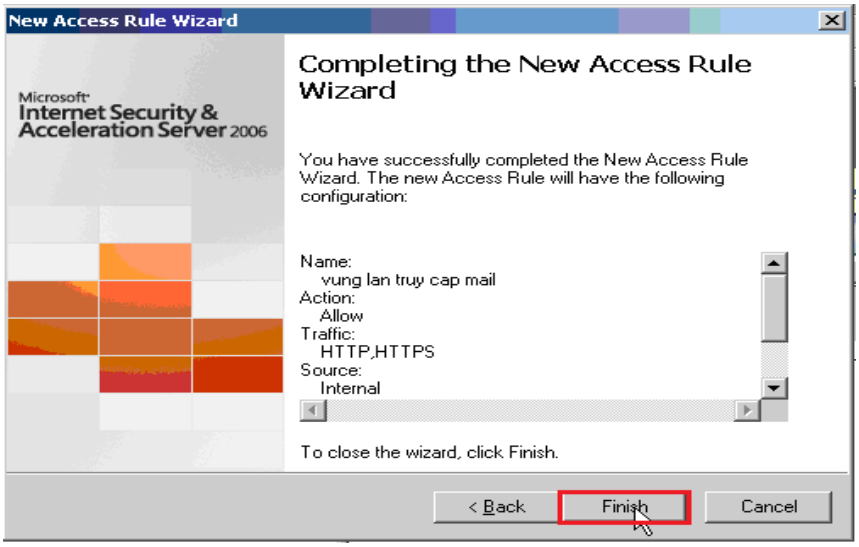
Add Internal, sau đó Click Next



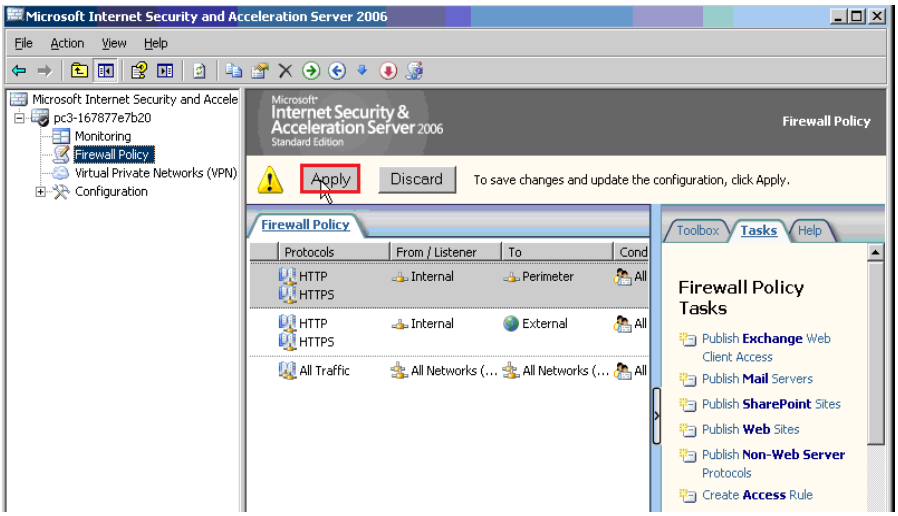
Add Perimeter, sau đó Click Next



Next

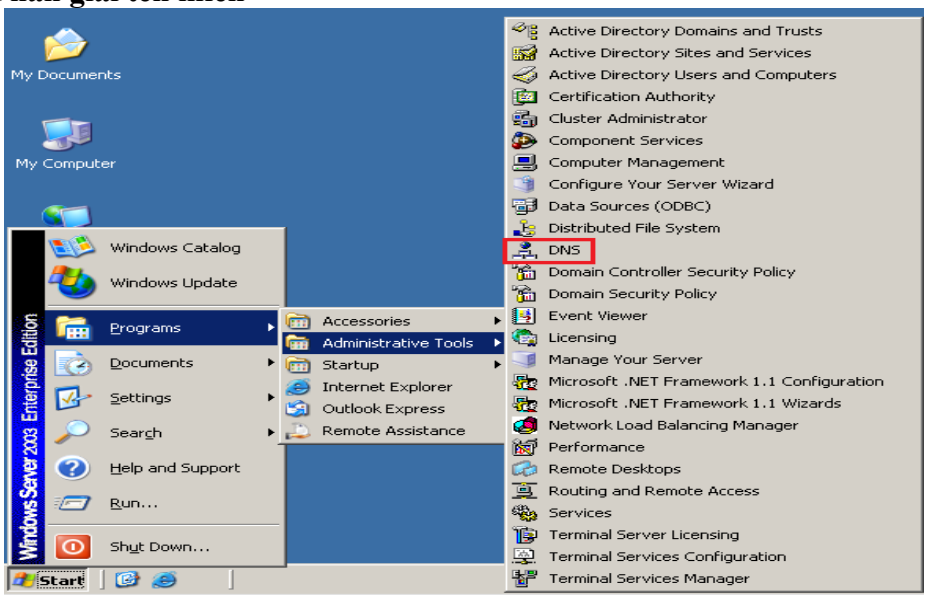


Click Finish

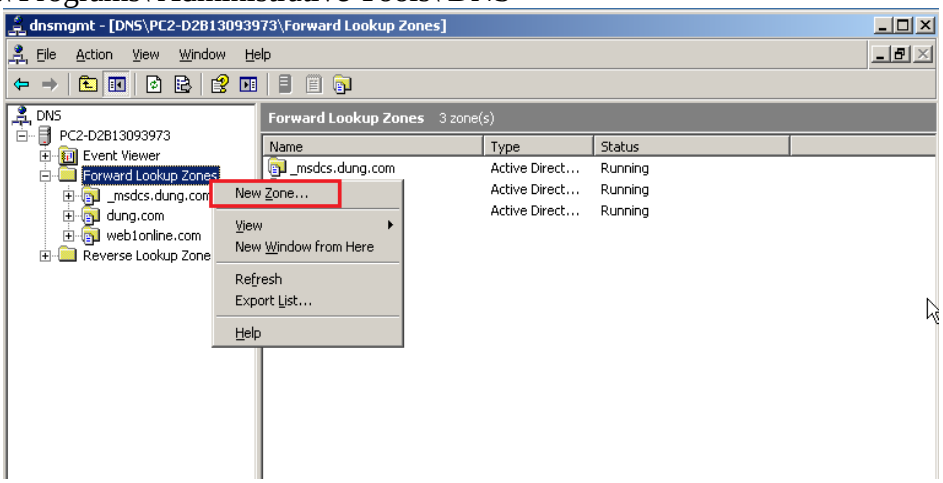


Click Apply

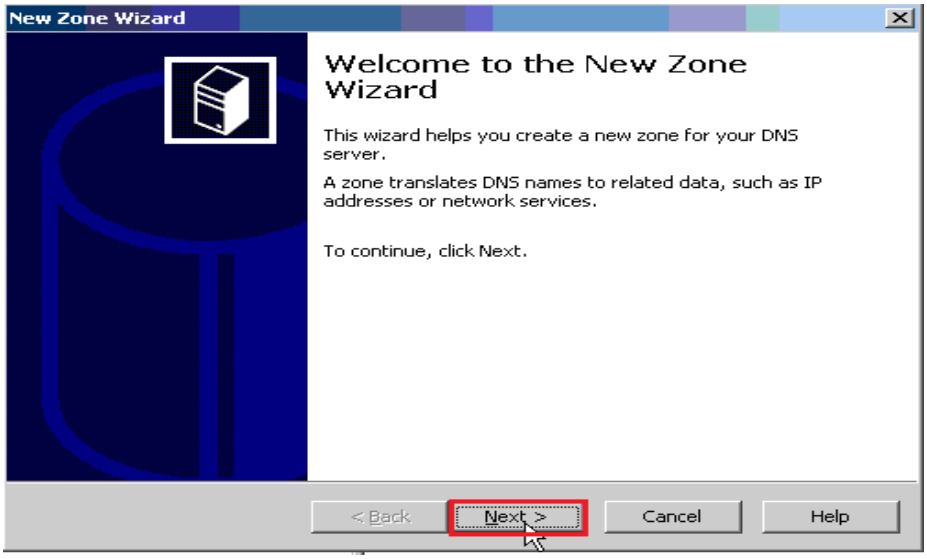
7.4. Phân giải tên miền



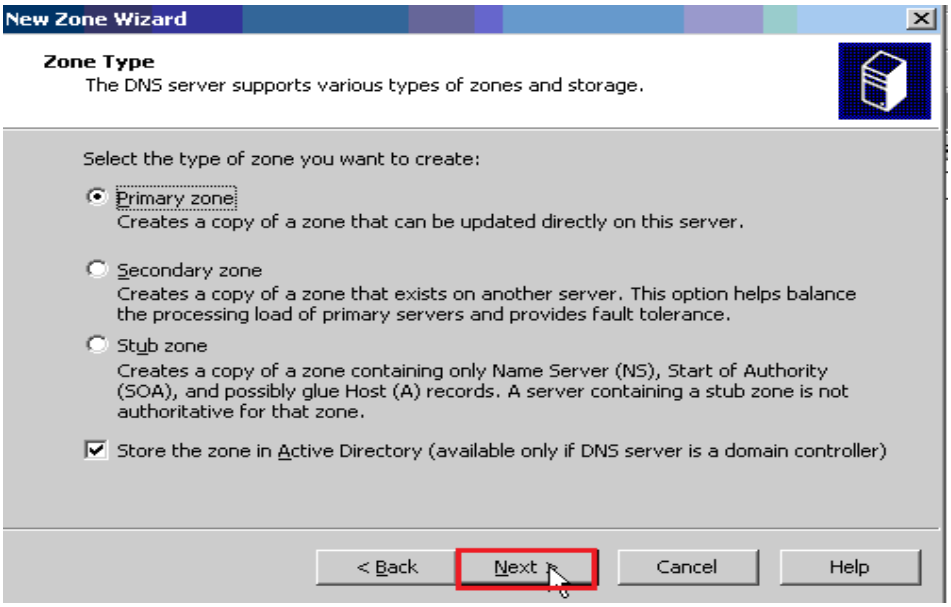
Start\ Programs\ Administrative Tools\ DNS



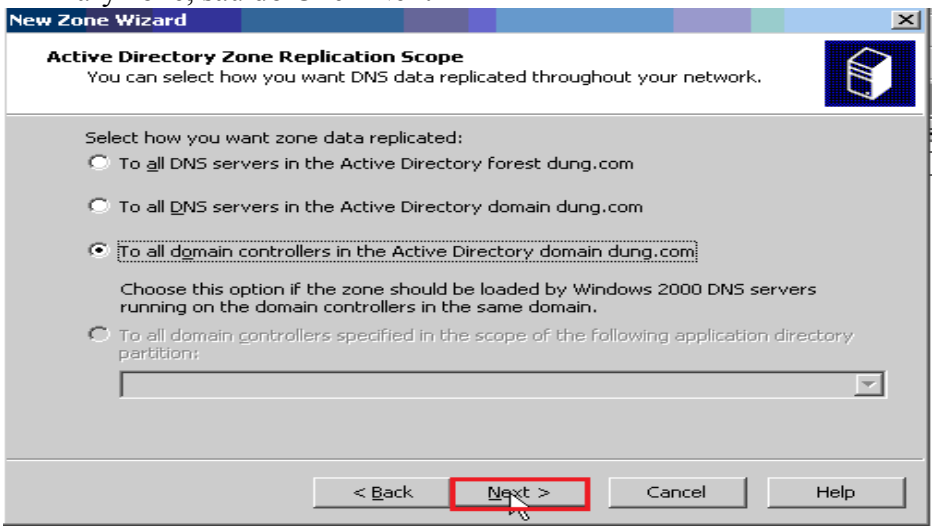
R_Click Forward Lookup Zones\ Click New Zone…



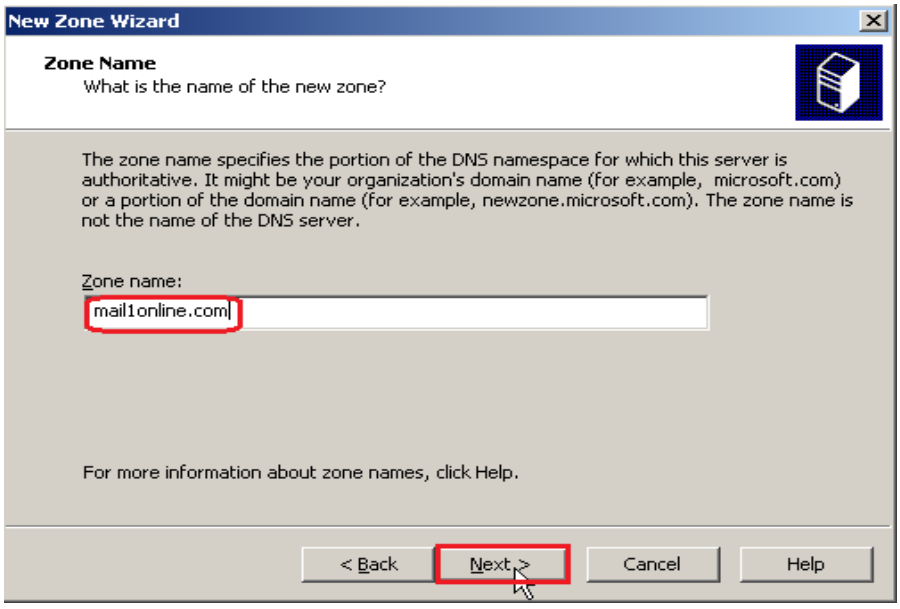
Click Next



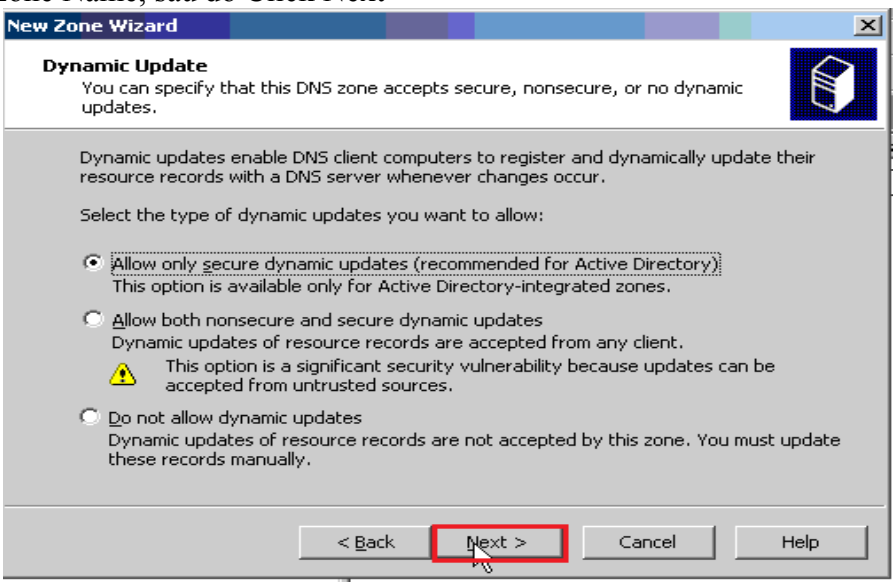
Chọn Primary zone, sau đó Click Next



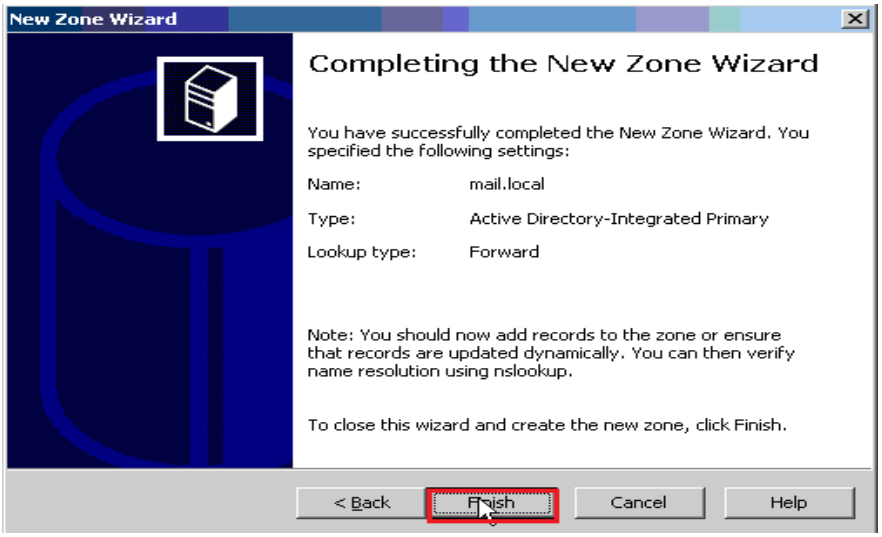
Chọn To all domain controllers in the Active Diretory domain dung.com, sau đó Click Next



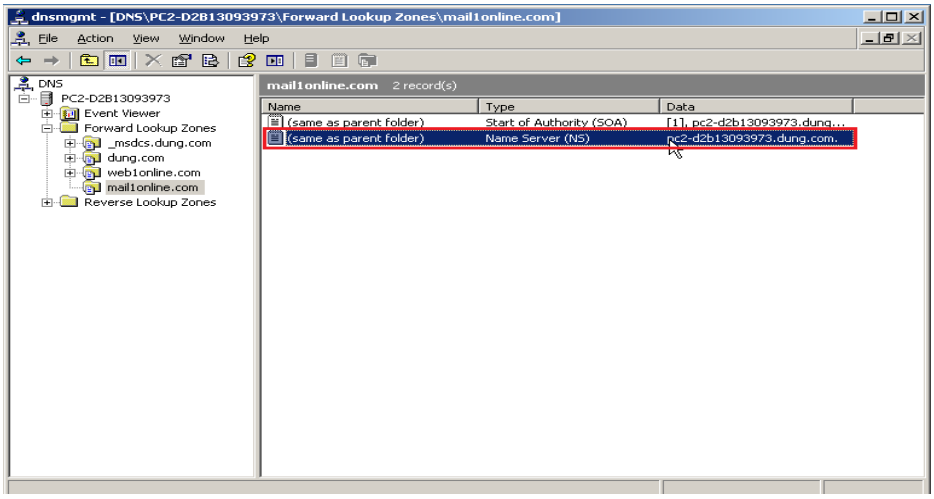
Điền Zone Name, sau đó Click Next



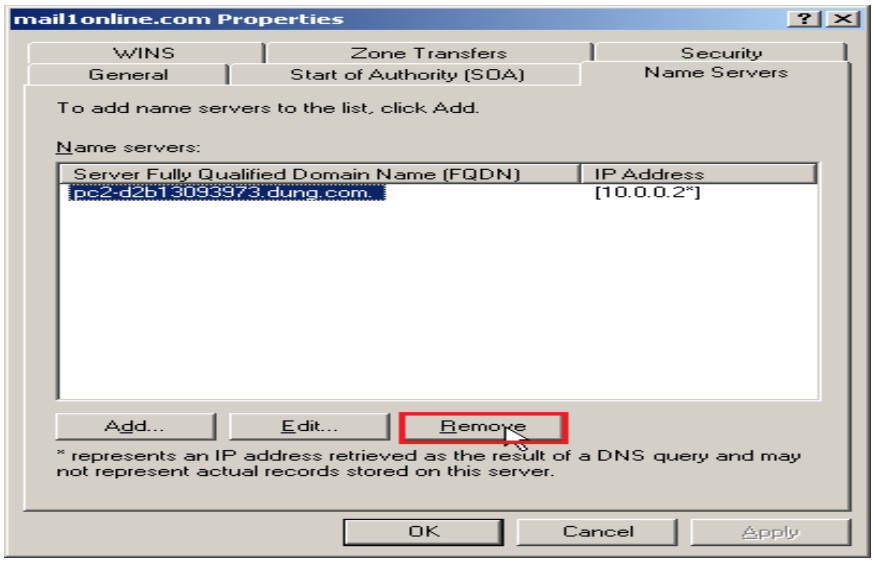
Chọn Allow only secure dynamic update(recommended for Active Directory), sau đó Click Next



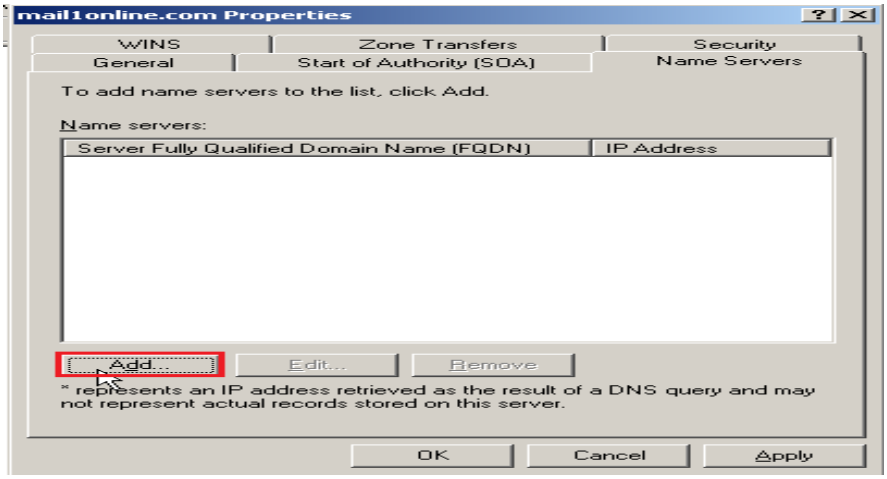
Click Finish



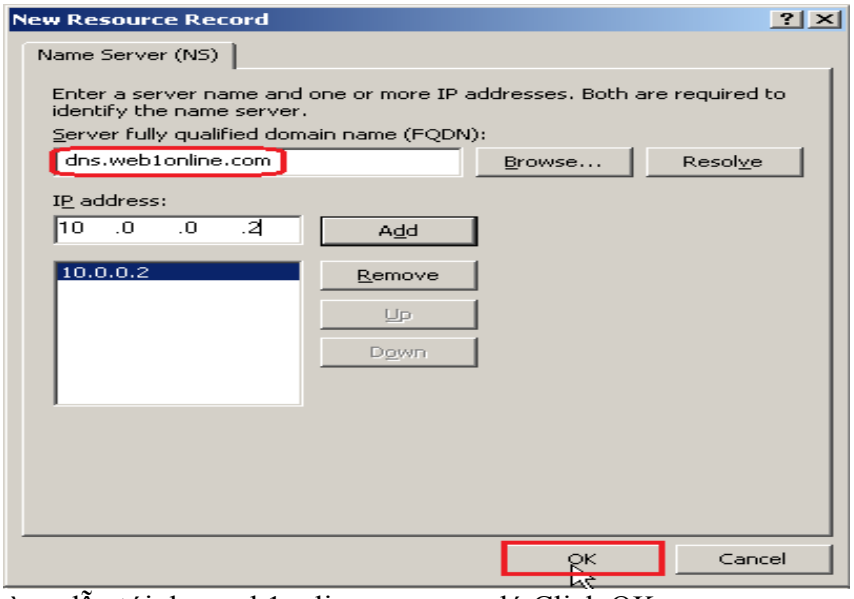
Click (same as parent folder) name server(NS)….



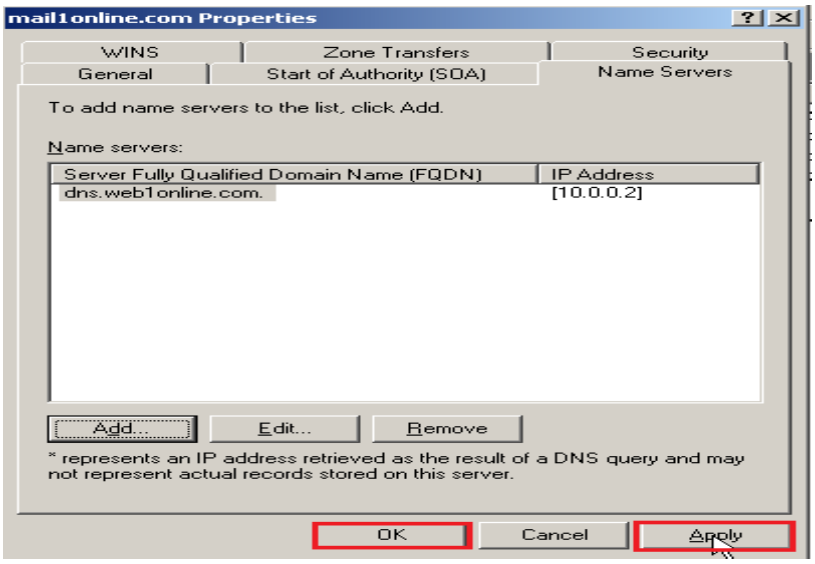
Click Remove



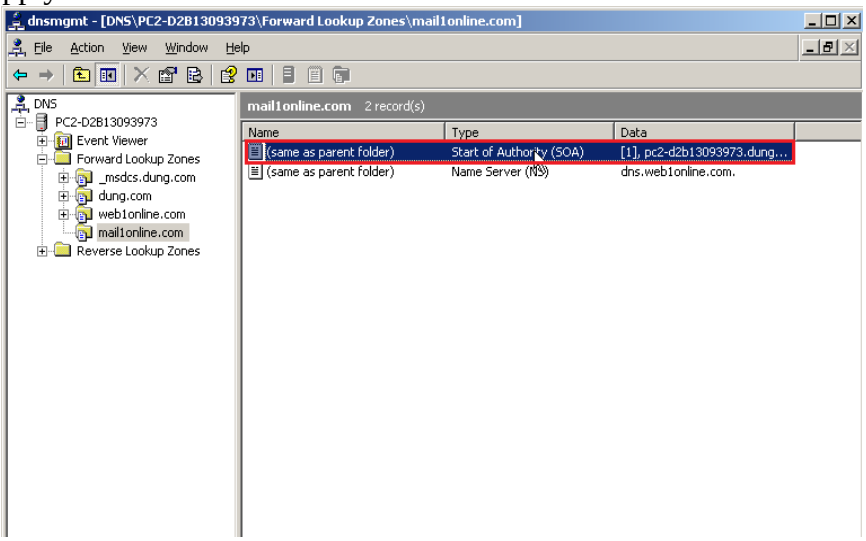
Click Add



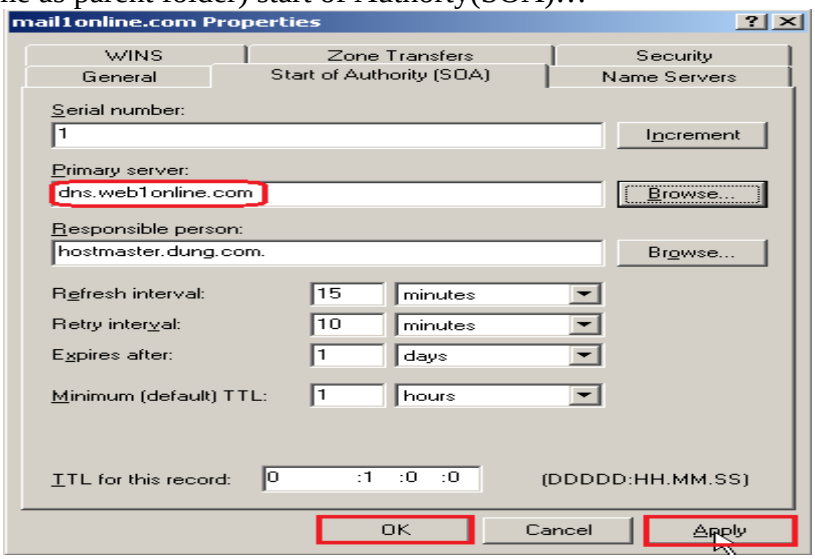
Chọn đường dẫn tới dns.web1online.com, sau đó Click OK



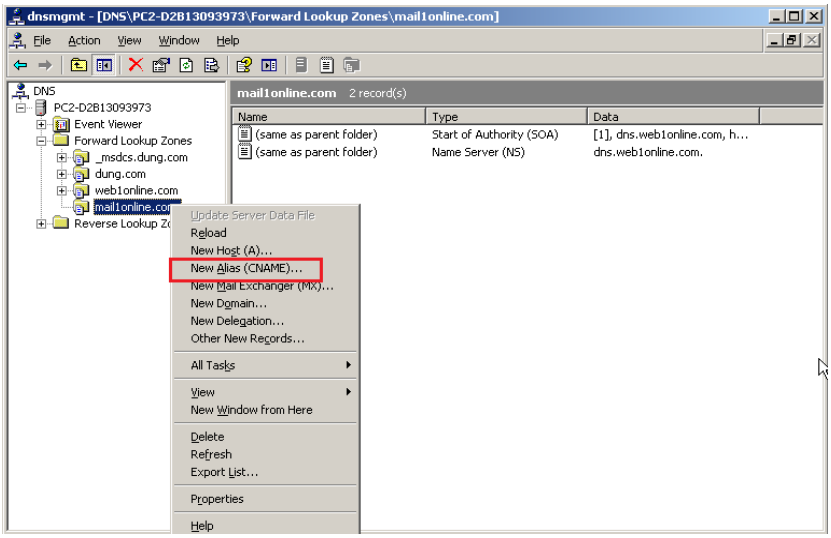
Click Apply\OK



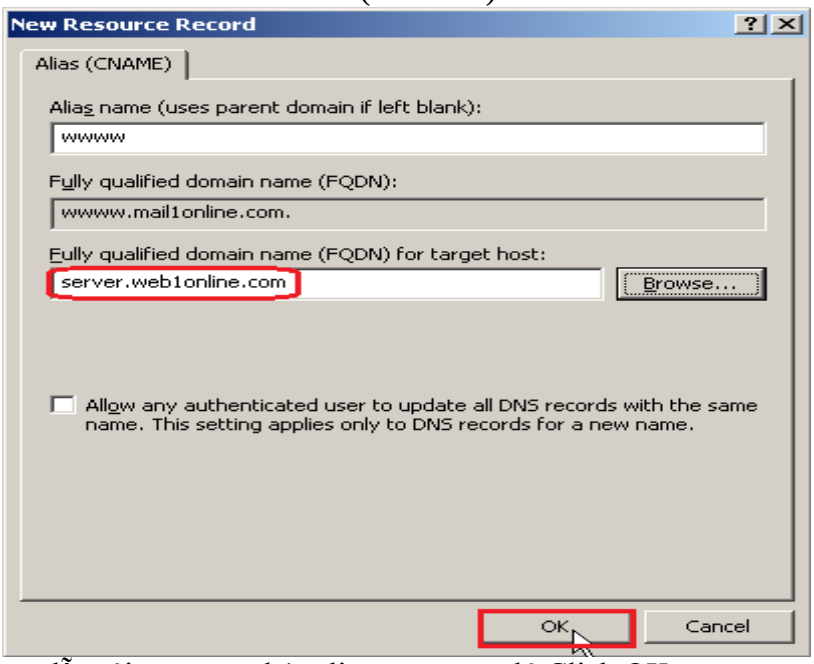
Click (same as parent folder) start of Authorty(SOA)…



Chọn dns.web1online.com, sau đó Click Apply\OK



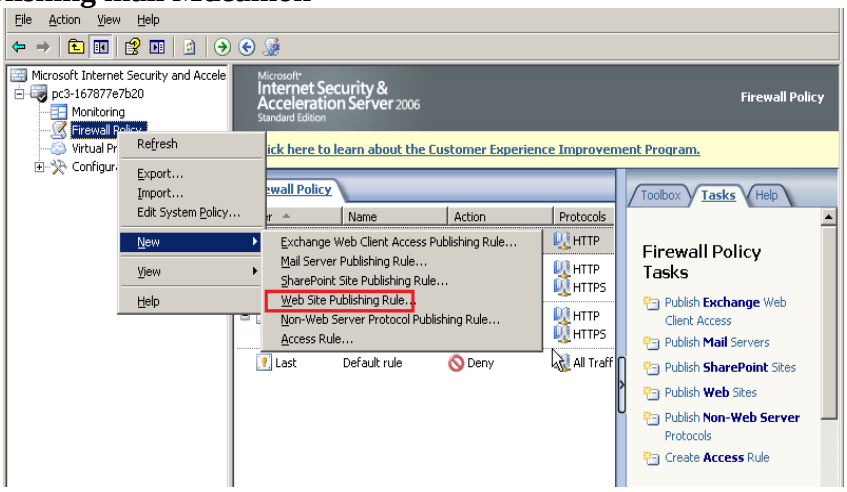
R_Click mail1online.com\New Alias (CNAME)…



Chọn đường dẫn tới server.web1online.com, sau đó Click OK

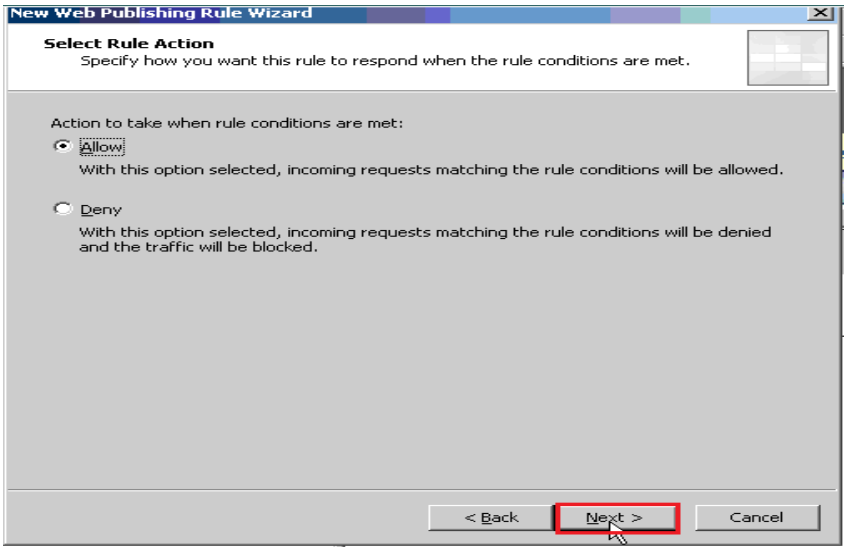
Trên thanh Address gõ http://www.mail1.online.com

7.5. Publishing mail Mdeamon

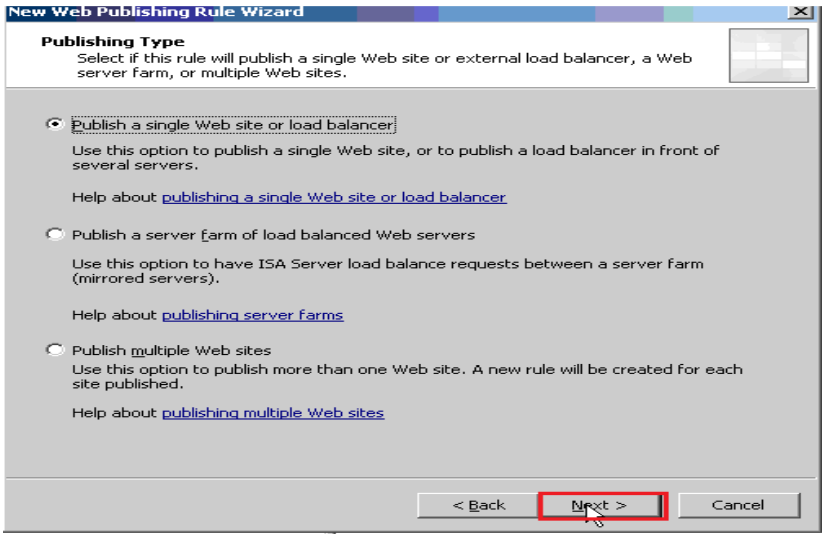


R_Click Firewall Polycy\New\Web Site Publishing Rule..

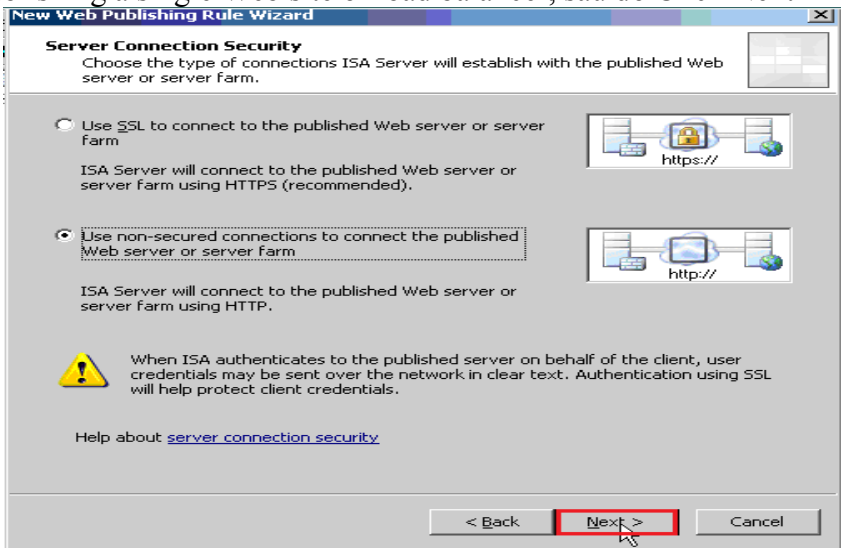
Điền Web Publishing rule name, sau đó Click Next



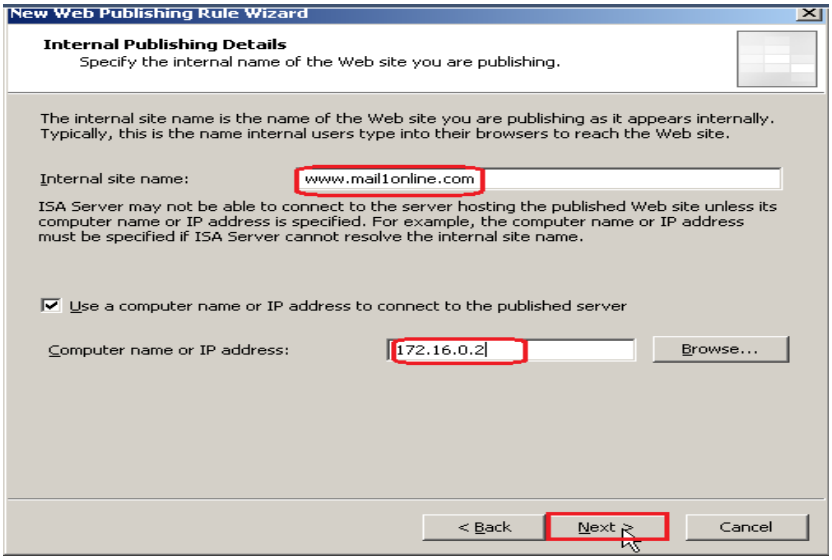
Chọn Allow, sau đó Click Next



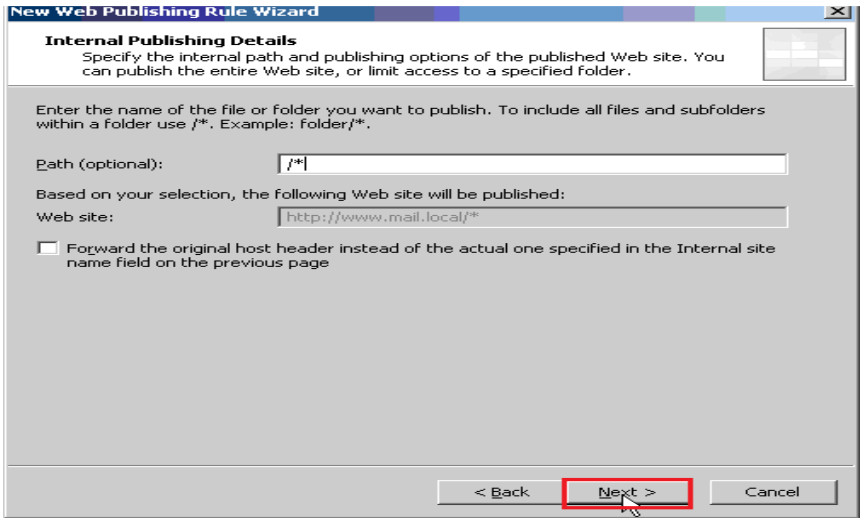
Chọn Publishing a single Web site or load balancer, sau đó Click Next



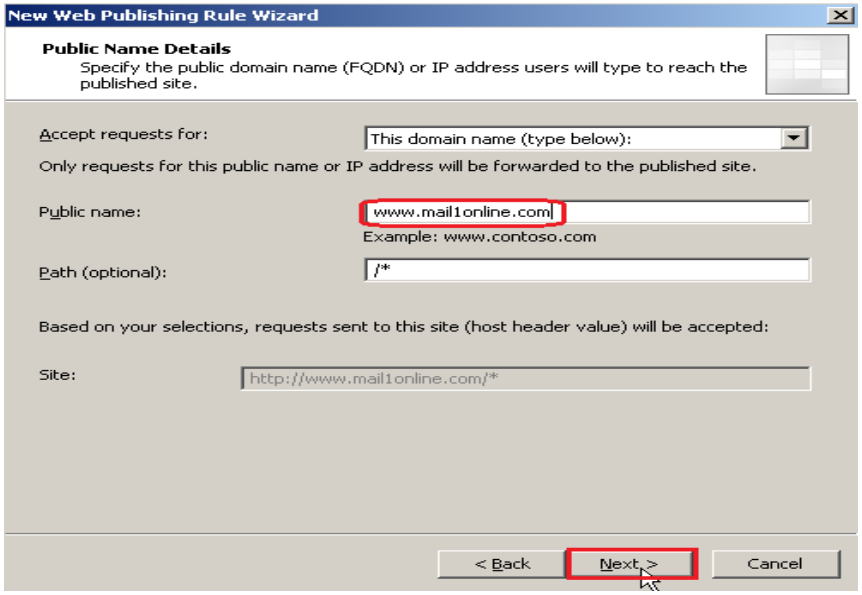
Chọn use non-secured connections to connect the published Web server or server farm, sau đó Click Next



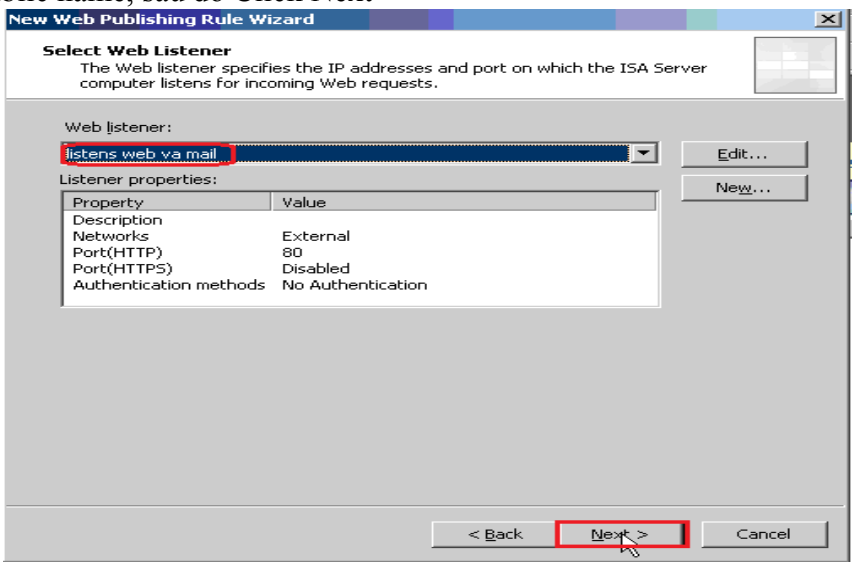
Điền Internal site name và Computer name or IP address, sau đó Click Next



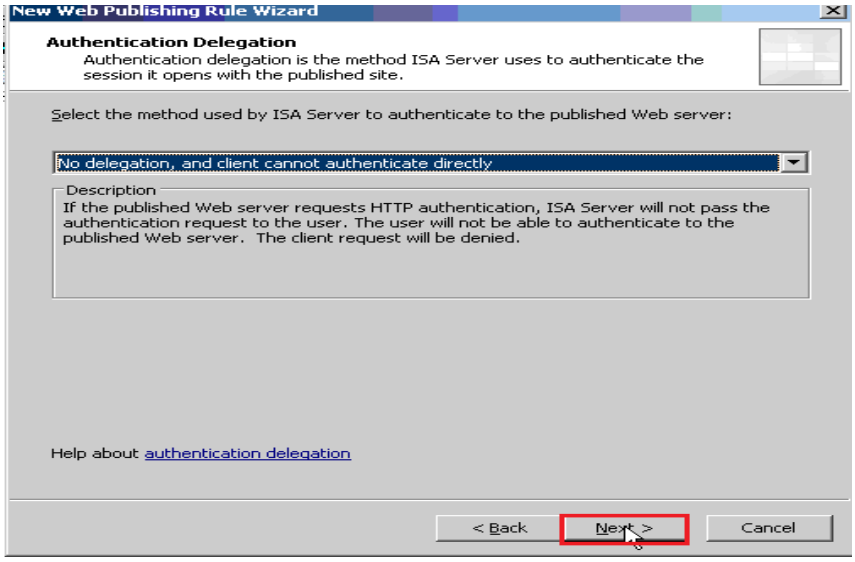
Click Next



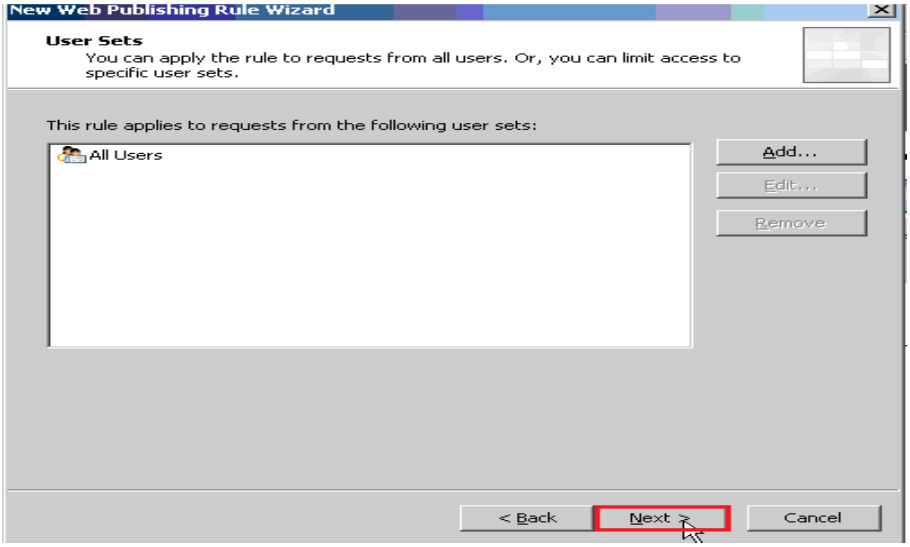
Điền Public name, sau đó Click Next



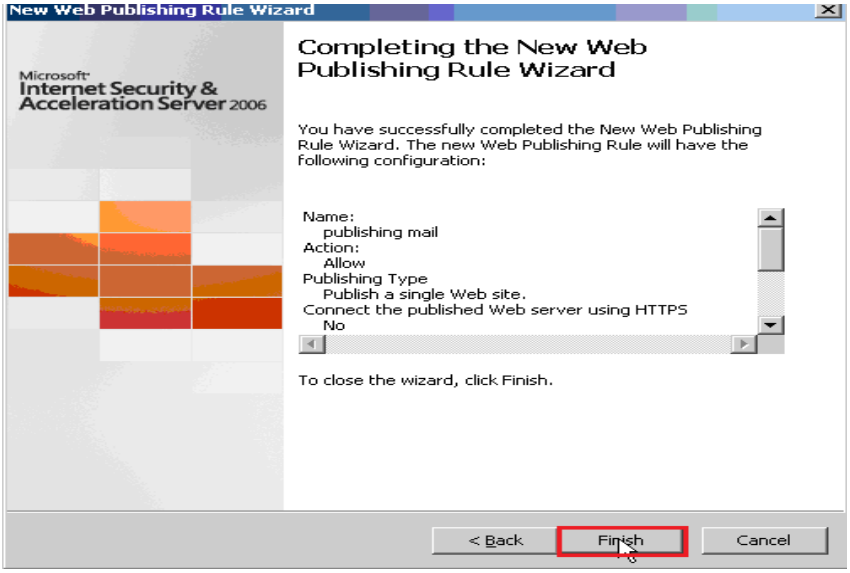
Chọn listens web va mail, sau đó Click Next



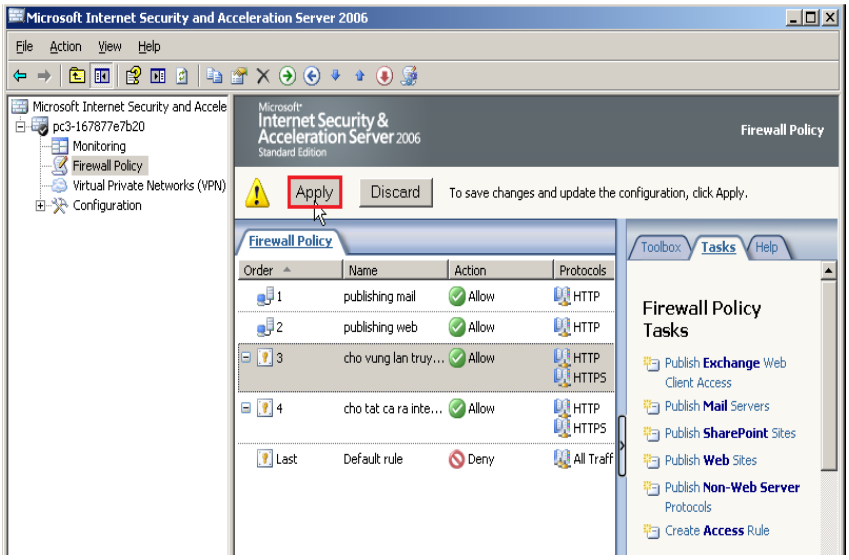
Click Next



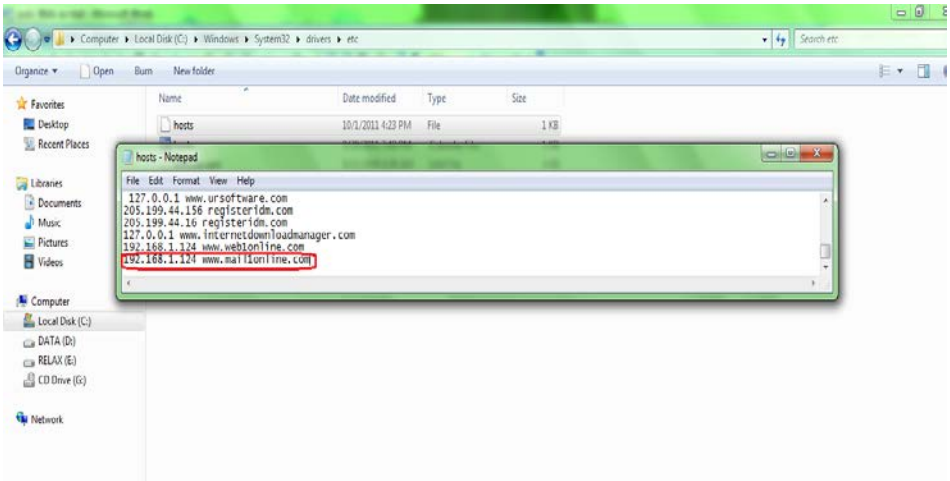
Click Next



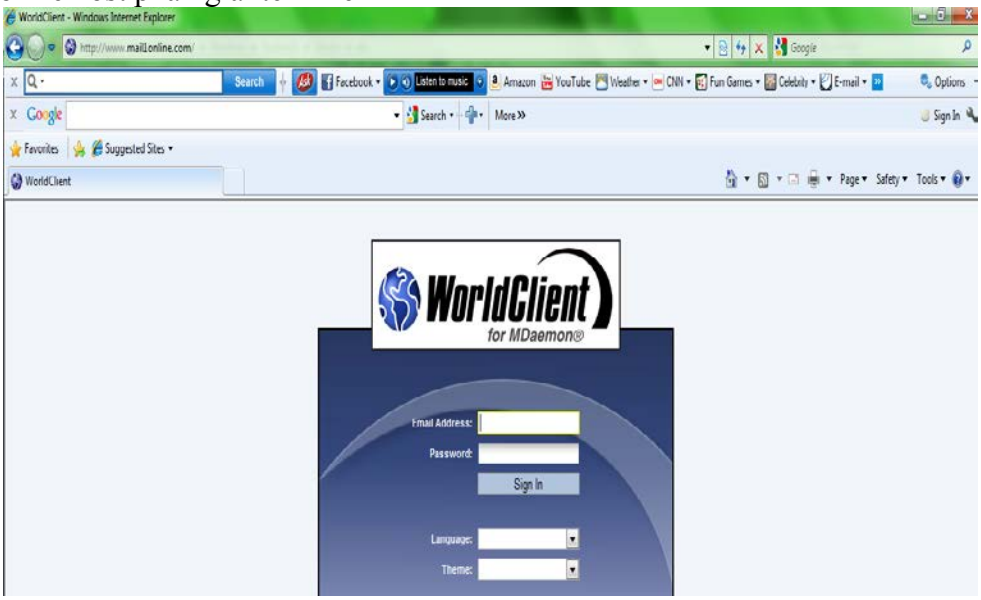
Click Finish



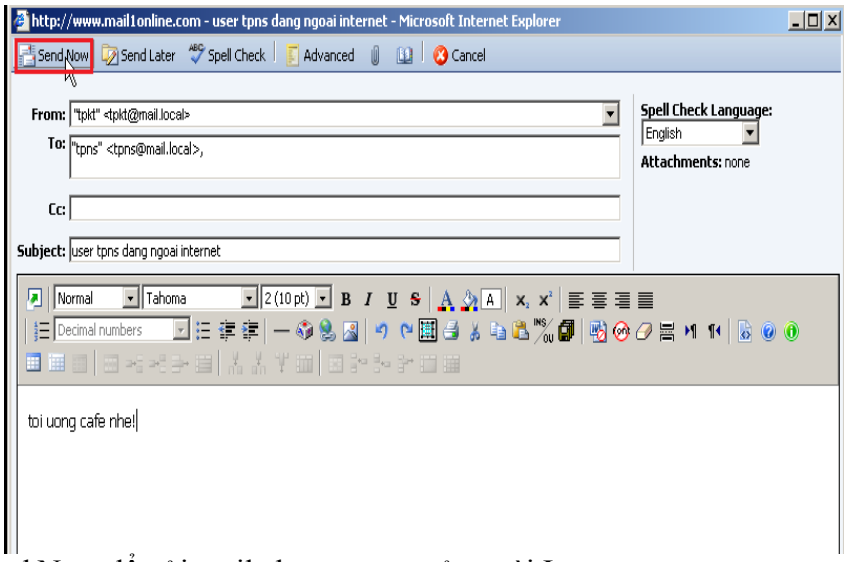
Click Apply



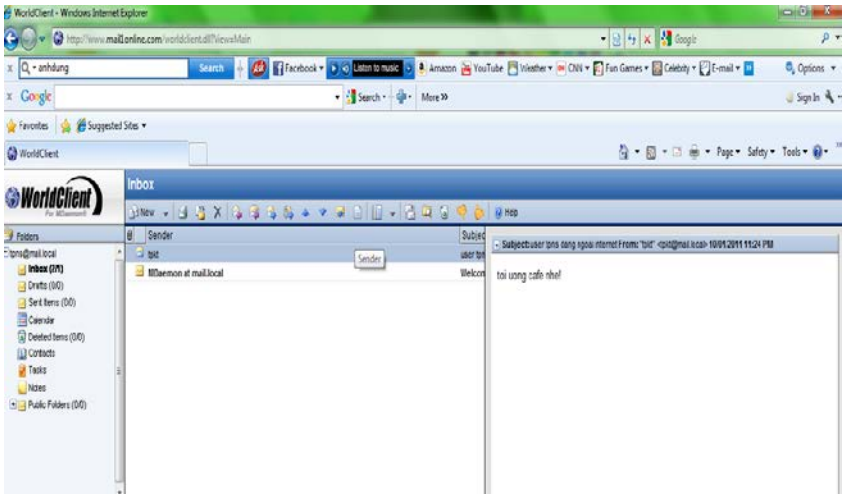
Vào file host phân giải tên miền



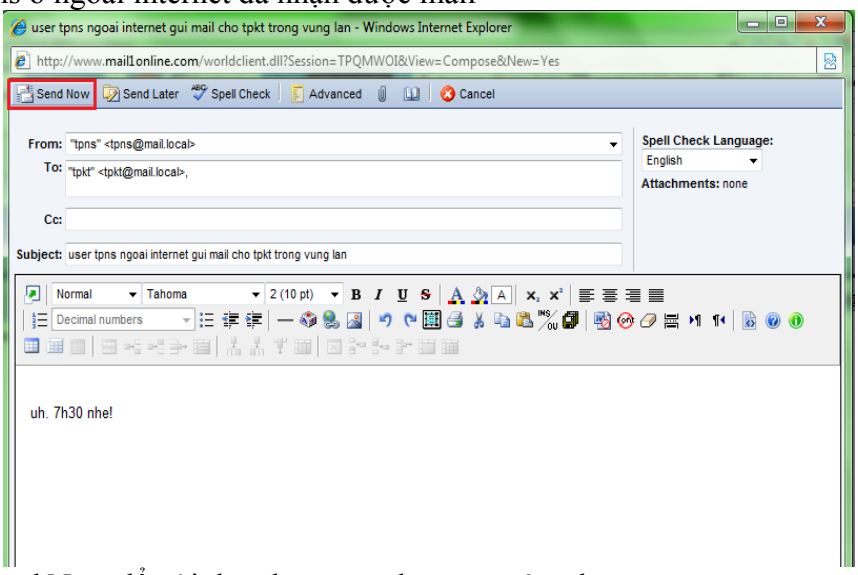
Trên thanh Address gõ http://www.mail1online.com
Gửi mail qua lại từ vùng lan ra ngoài Internet và ngược lại



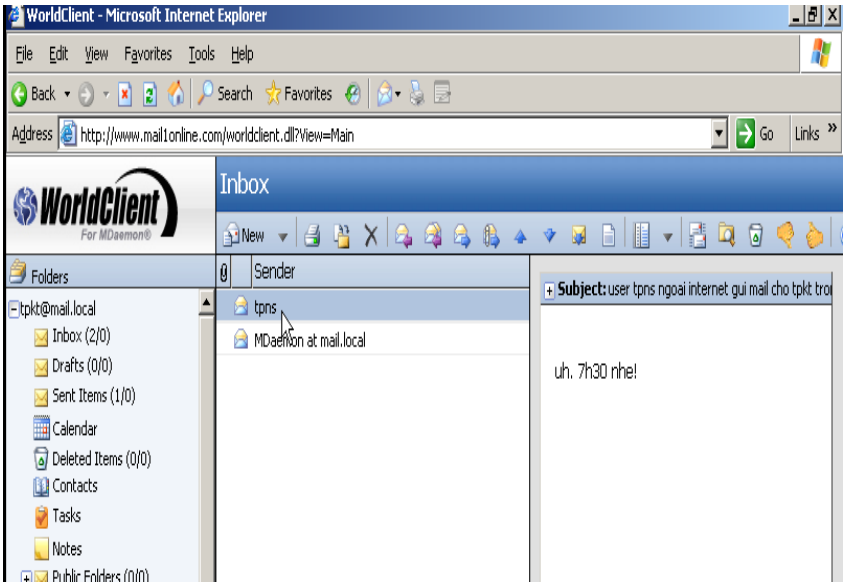
Click send Now để gửi mail cho user tpns ở ngoài Internet



User tpns ở ngoài internet đã nhận được mail



Click Send Now để gửi thư cho user tpkt trong vùng lan



User tpkt đã nhận được mail

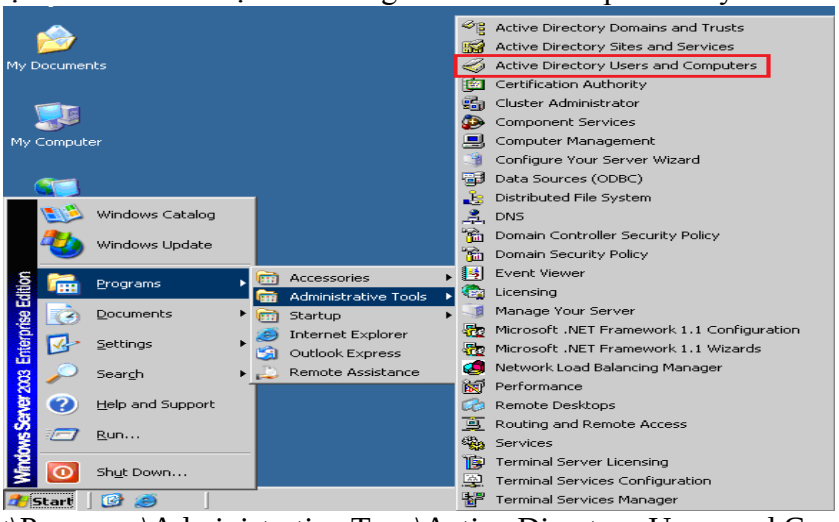
8. Vpn client - to - site

VPN Server cho phép các máy trạm VPN Client kết nối đến thông qua Internet, và giao tiếp với các máy tính trong mạng nội bộ. Trong khi các VPN Server trên những nền tảng khác cho phép máy trạm có tất cả các quyền để giao tiếp với mạng nội bộ một khi đã kết nối, thì VPN Server trên ISA Server giúp bạn chỉ định rõ những giao thức cụ thể để các máy trạm giao tiếp với mạng nội bộ. Bằng cách này ISA Server giúp bạn nâng cao độ bảo mật cho các hệ thống mạng VPN

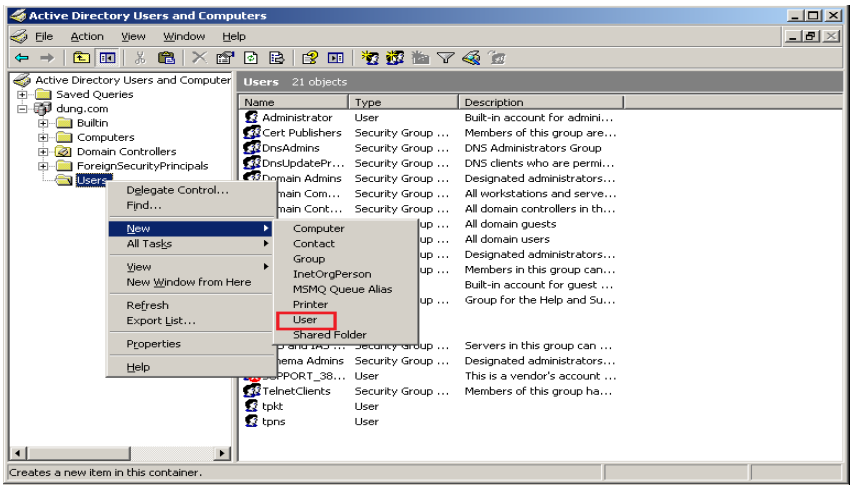
Bên cạnh đó ISA Server cho phép bạn xây dựng mạng VPN dưới dạng Site-To- Site. Một Site-To-Site VPN cho phép hai hay nhiều mạng có thể kết nối với nhau thông qua Internet.

Trong phần này, chúng ta sẽ sử dụng ISA Server 2006 để triển khai VPN Client-To-Site

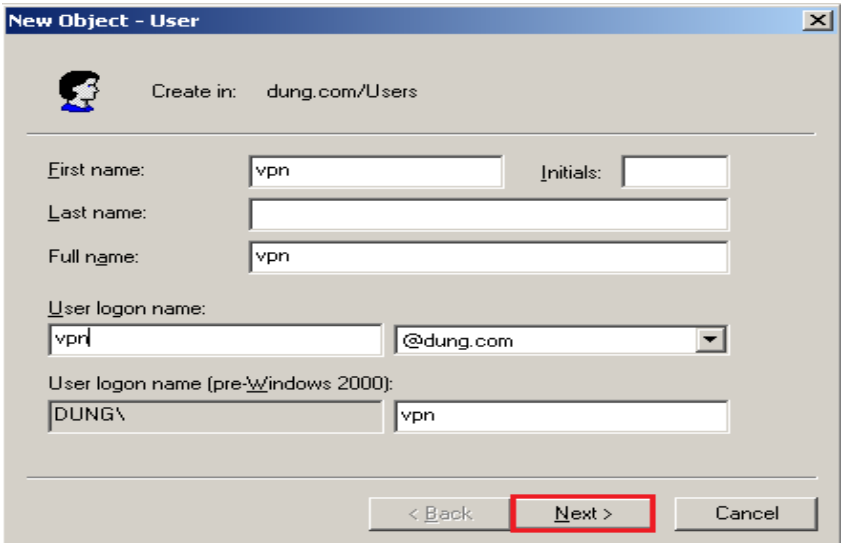
Bước 1: tạo user VPN và bật chức năng Remote Desktop của máy DC



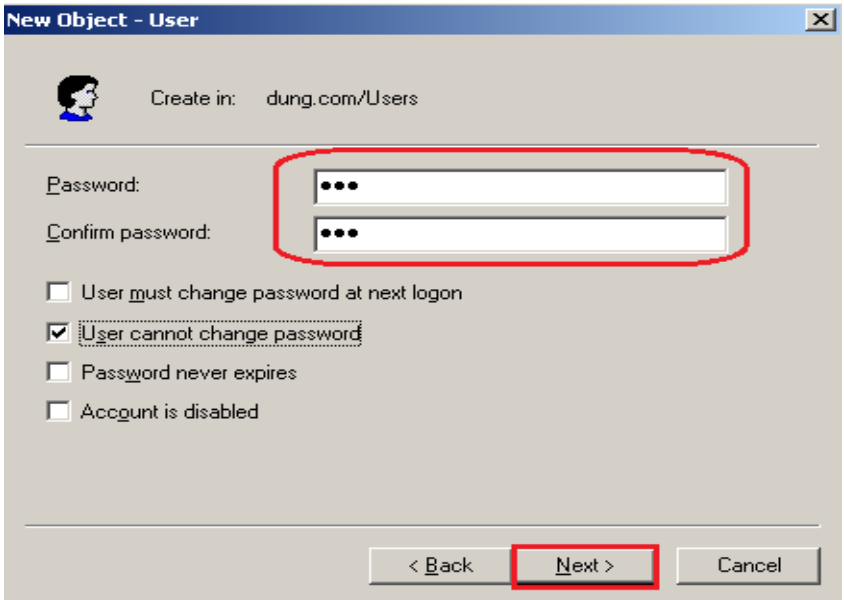
Vào Start\Programs\Administrative Toos\Active Directory Users and Computers



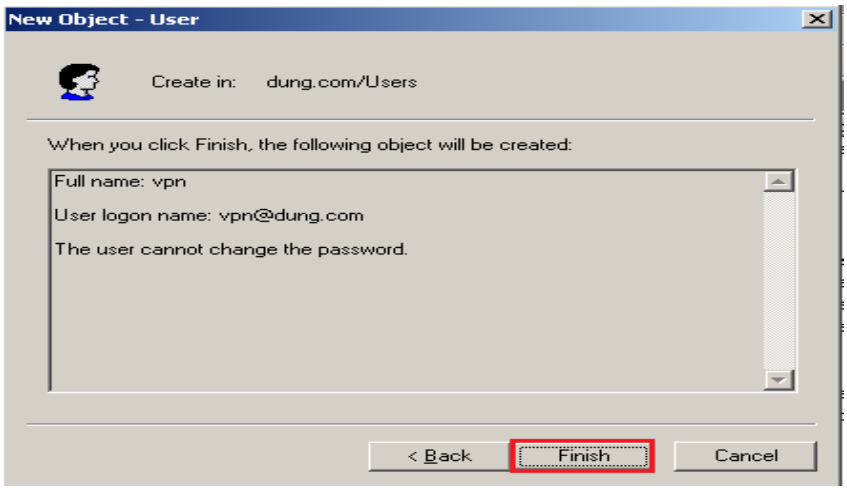
R_Click Users\New\User



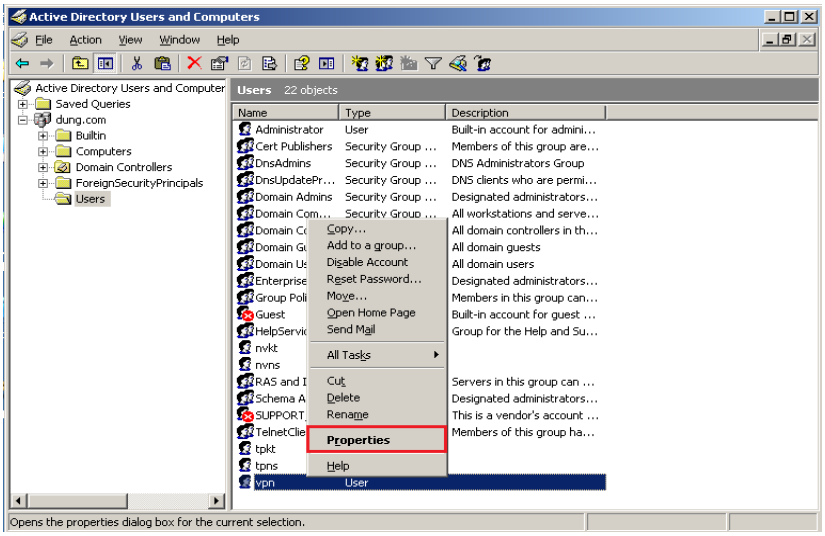
Điền thong tin User, sau đó Click Next



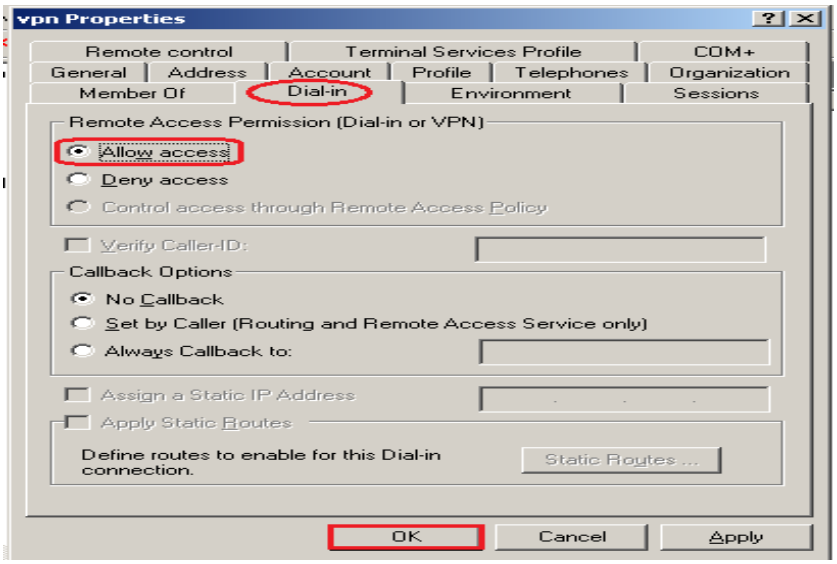
Điền Password và Check vào User cannot change password, sau đó Click Next



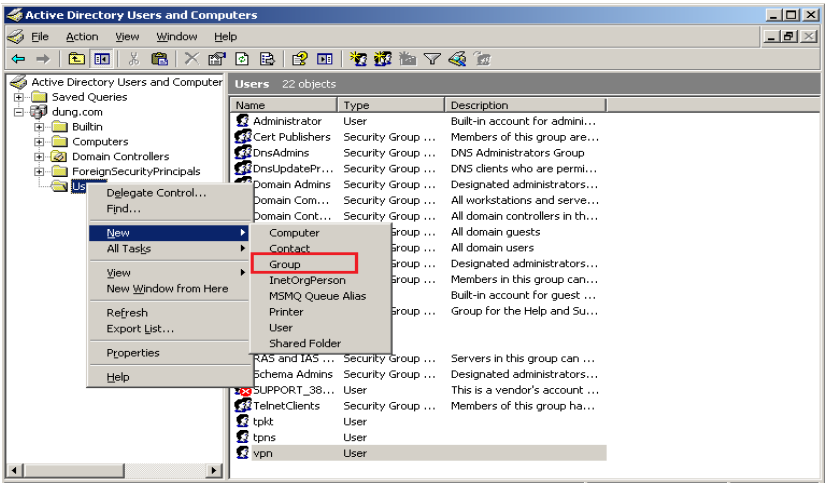
Click Finish



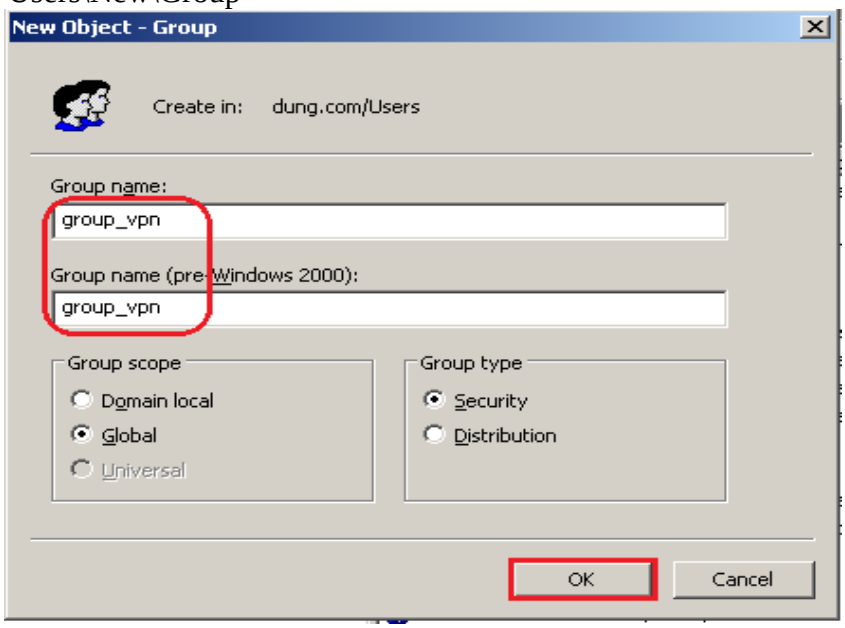
R_Click User vpn\Properties



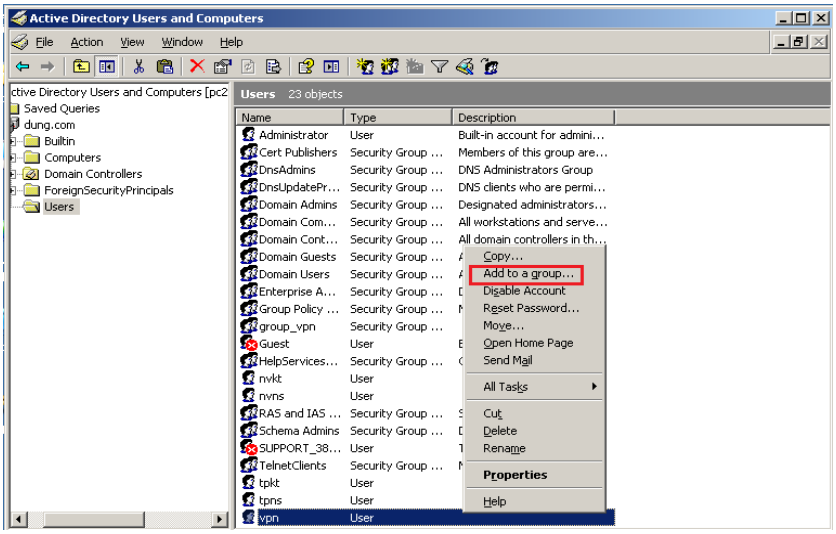
Vào tab Dial-in chọn option Allow access, sau đó Click OK



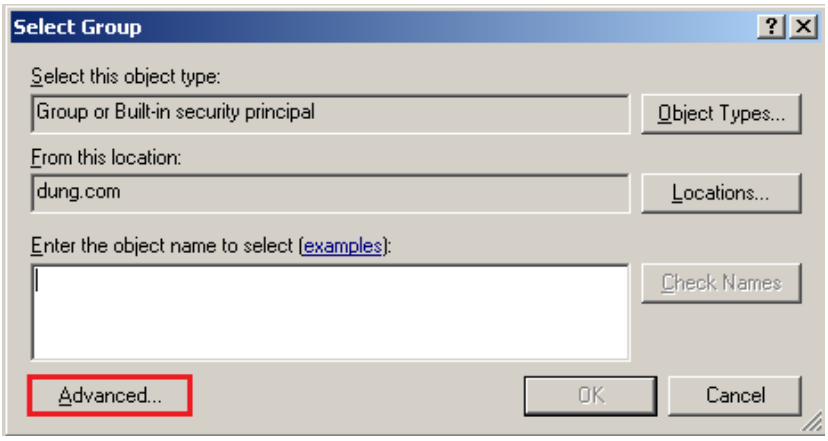
R_Click Users\New\Group



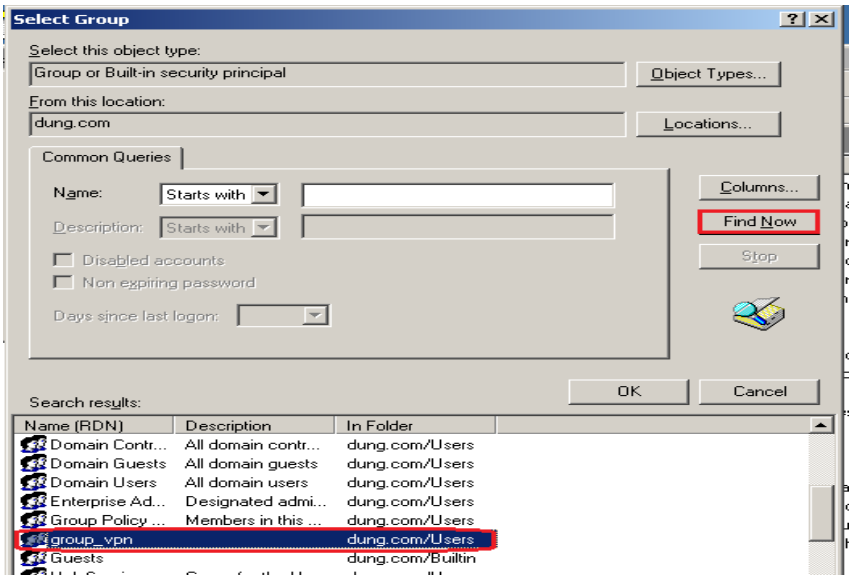
Điền Group name, sau đó Click OK



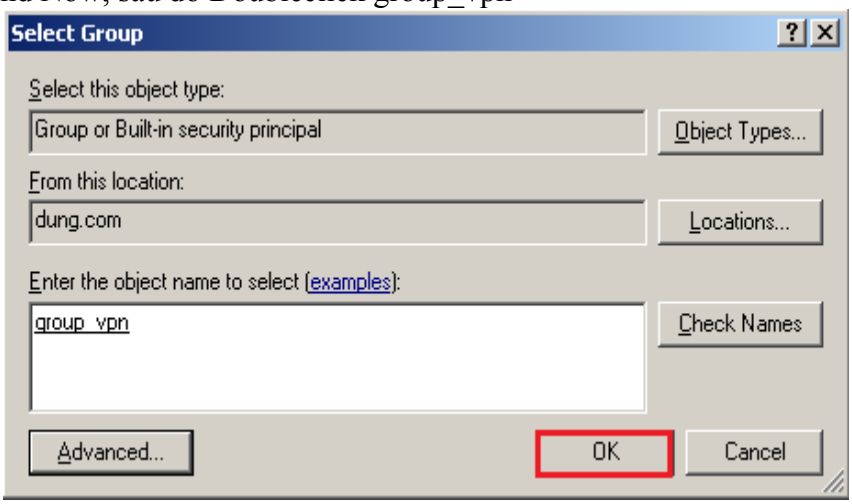
R_Click User vpn\ Add to a group…



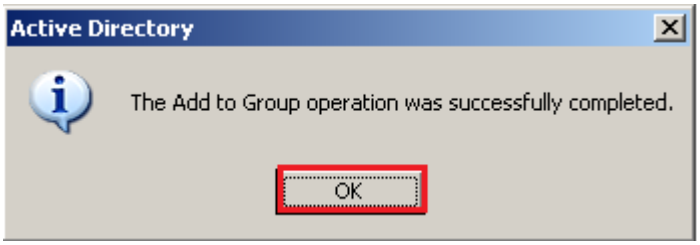
Click Advanced…



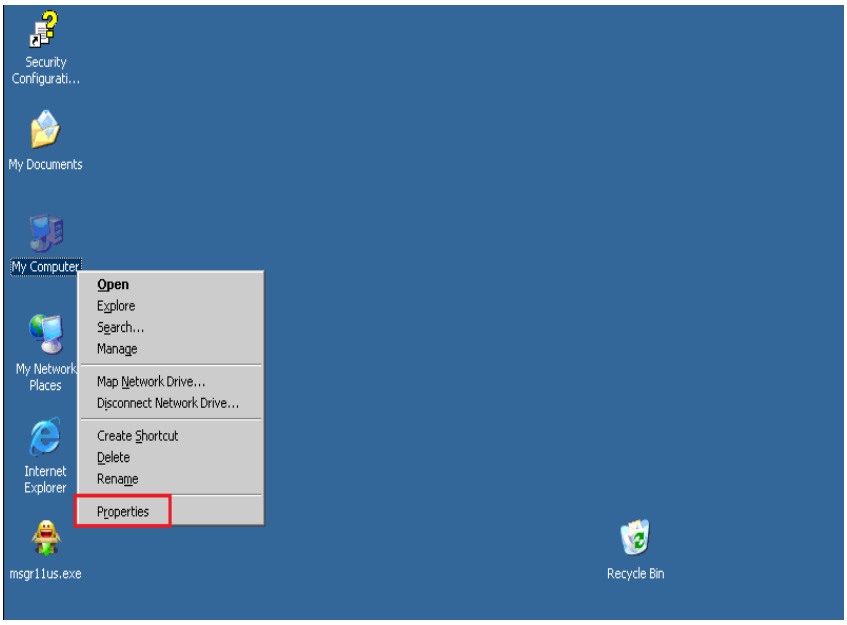
Click Find Now, sau đó Doubleclick group_vpn



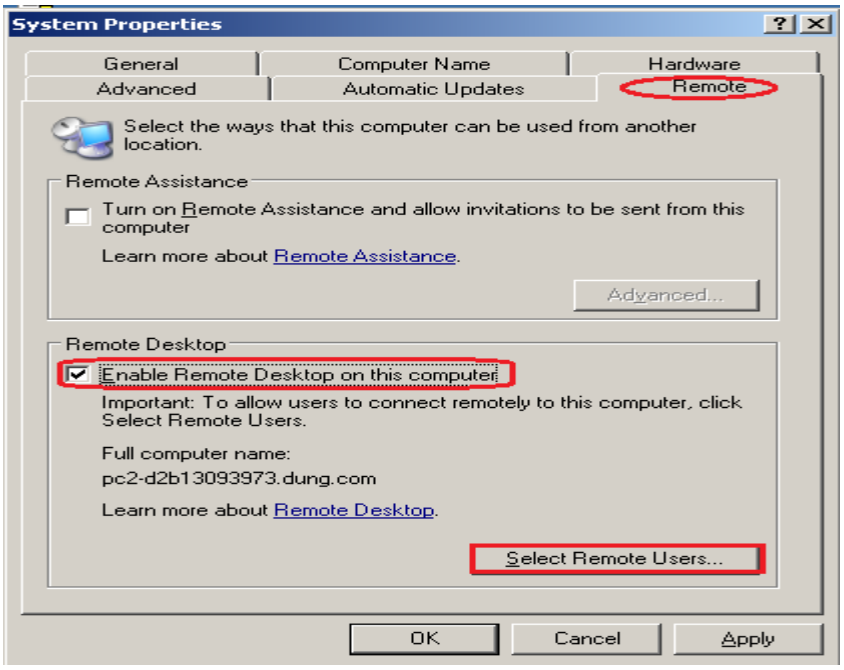
Click OK



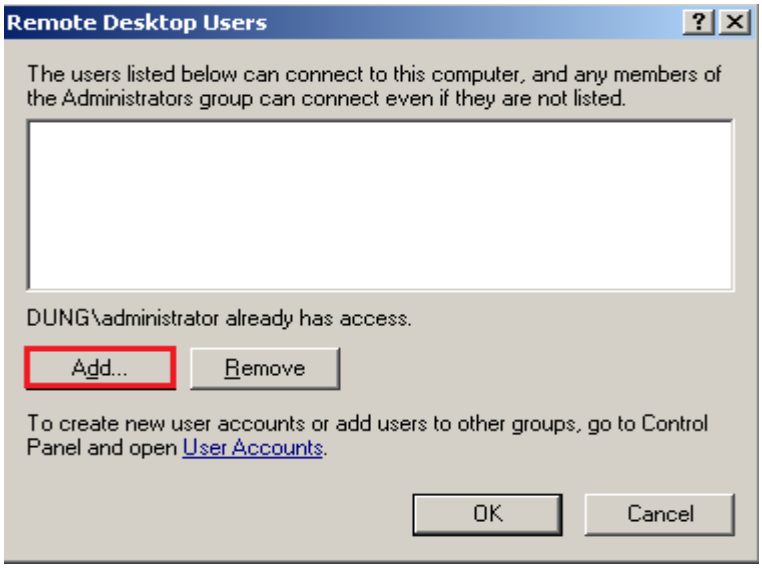
Click OK



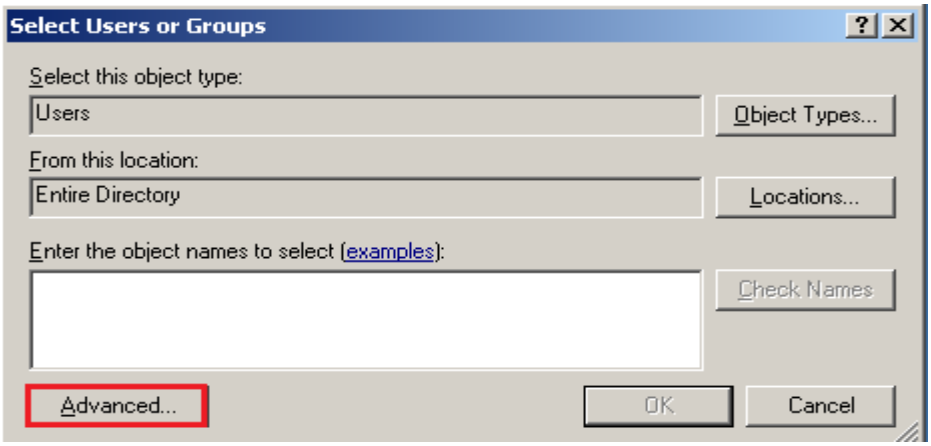
R_Click My Computer\Properties



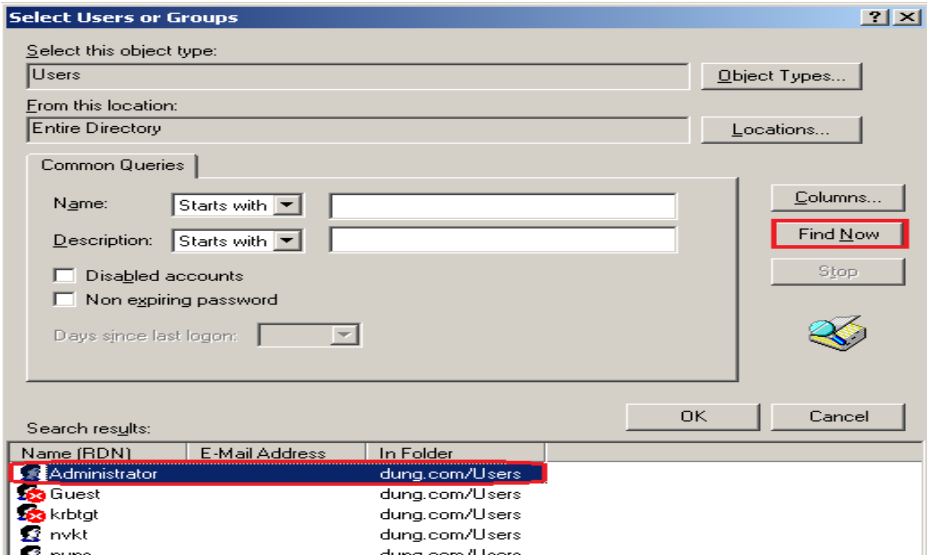
Vào tab Remote và Check Enable Remote Desktop on this computer, sau đó Click Select Remote Users.



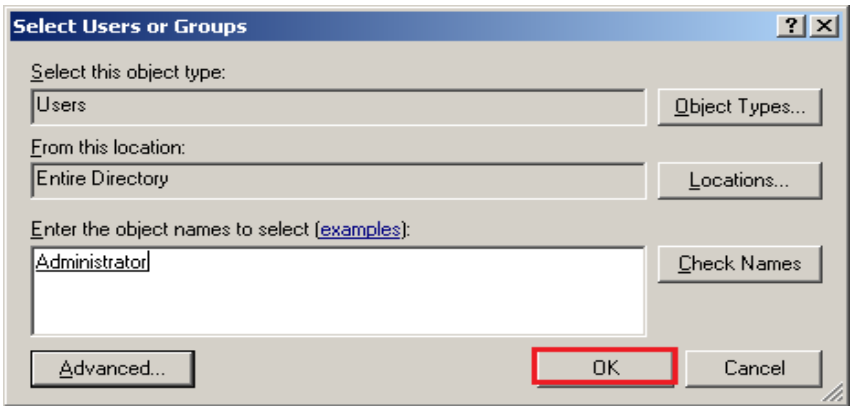
Click Add…



Click Advanced…

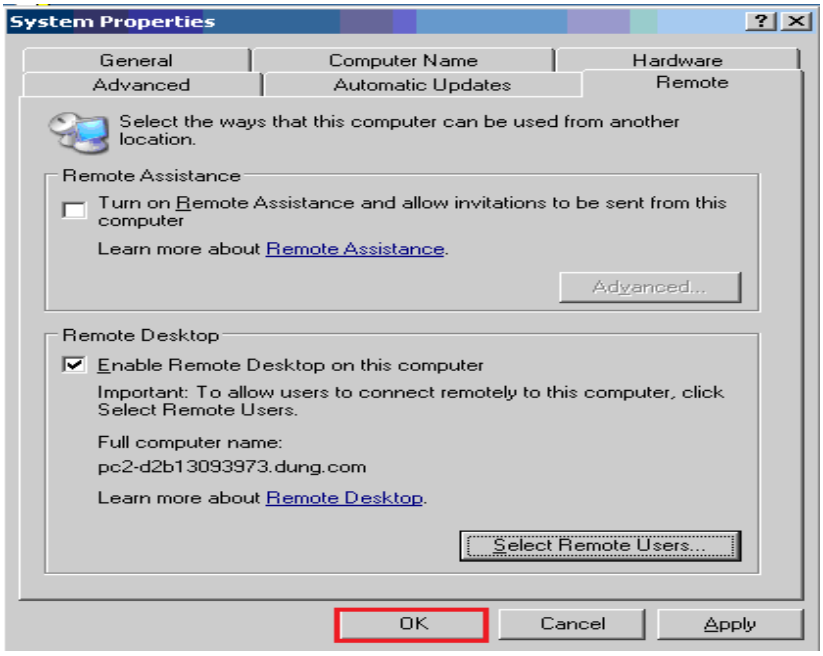


Click Find Now, sau đó Doubleclick Administrator



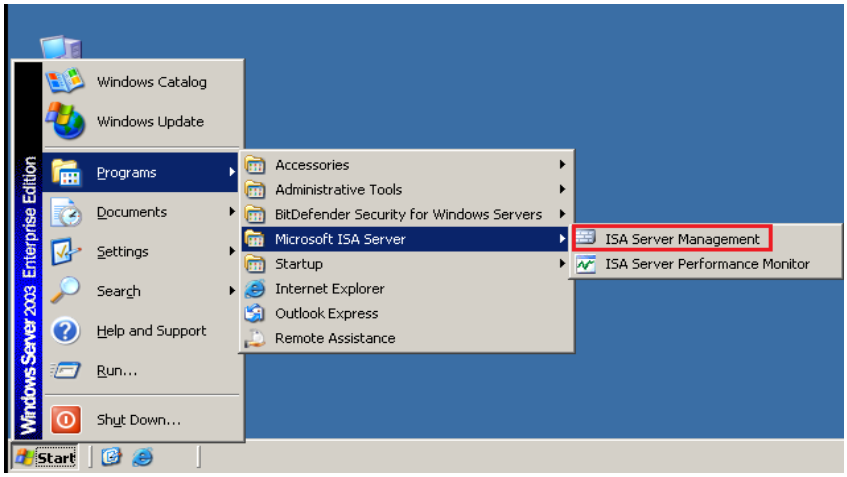
Click Ok

Click OK

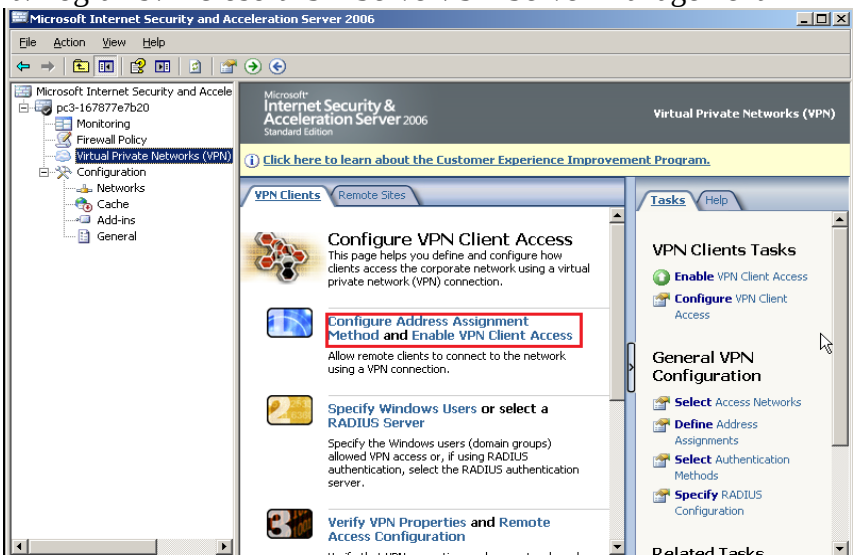


Click Apply\OK

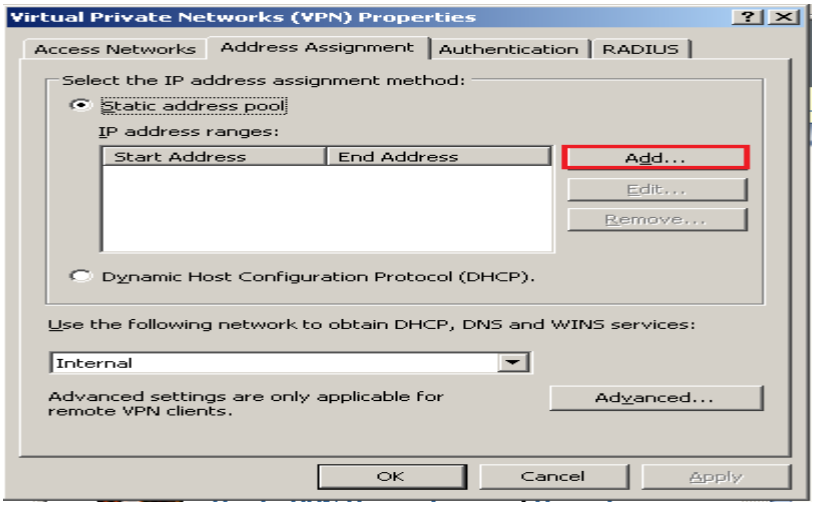
Bước 2: Cấu hình ISA



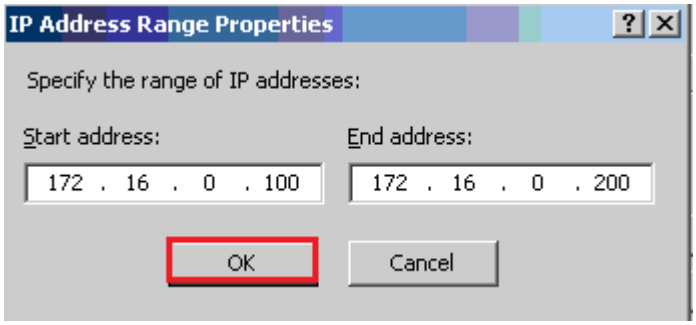
Vào Start\Programs\Microsoft ISA Server\ISA Server Management



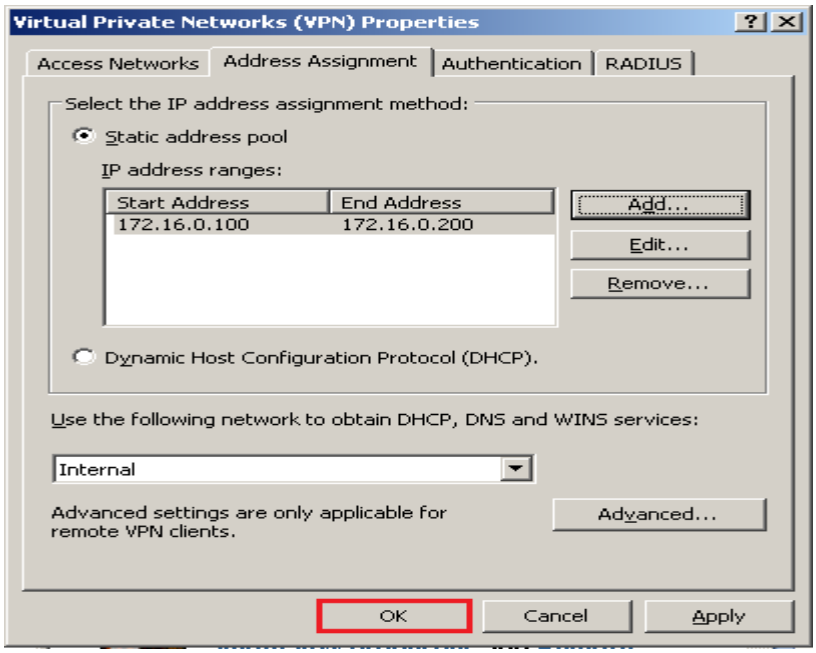
Click Virtual Private Networks(VPN)\ Click Configure address Assignment Method



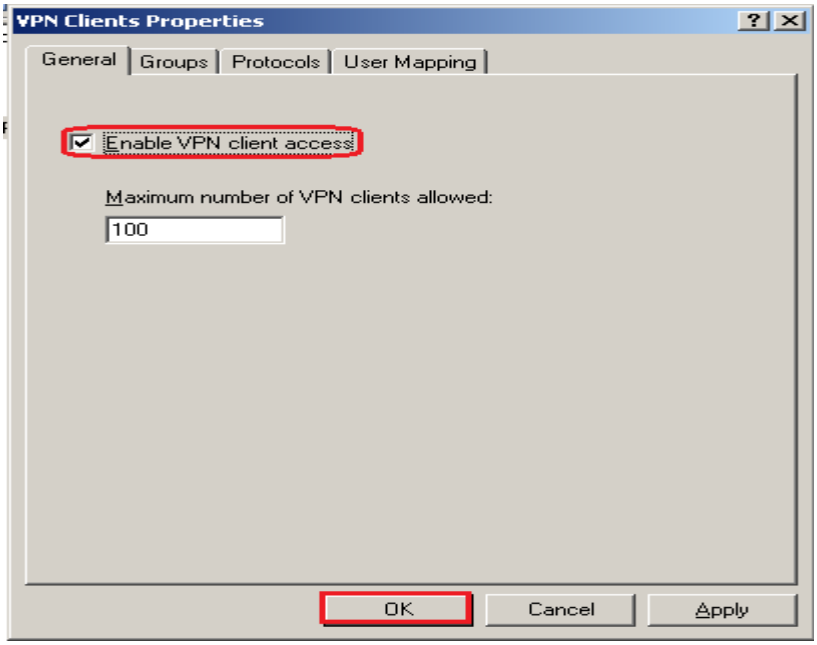
Click Add



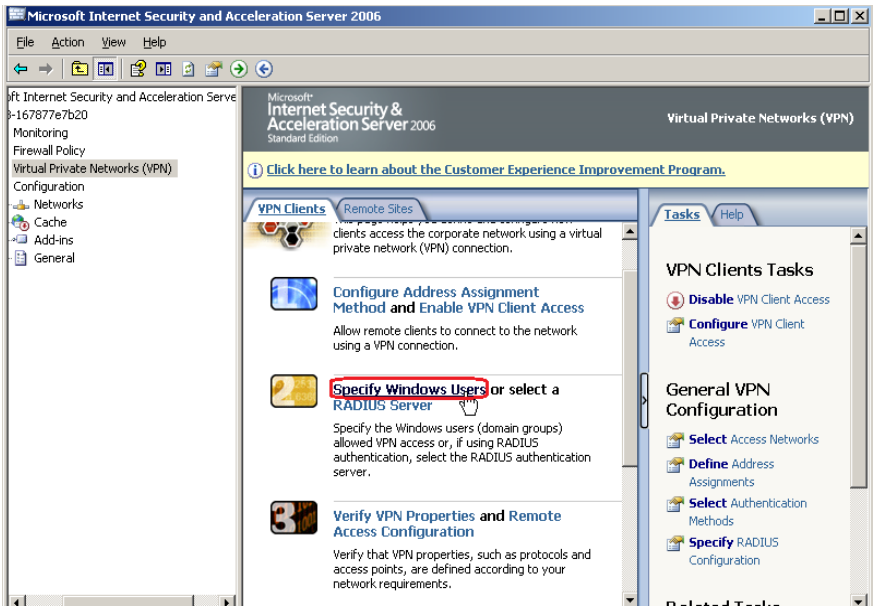
Điền dãy IP



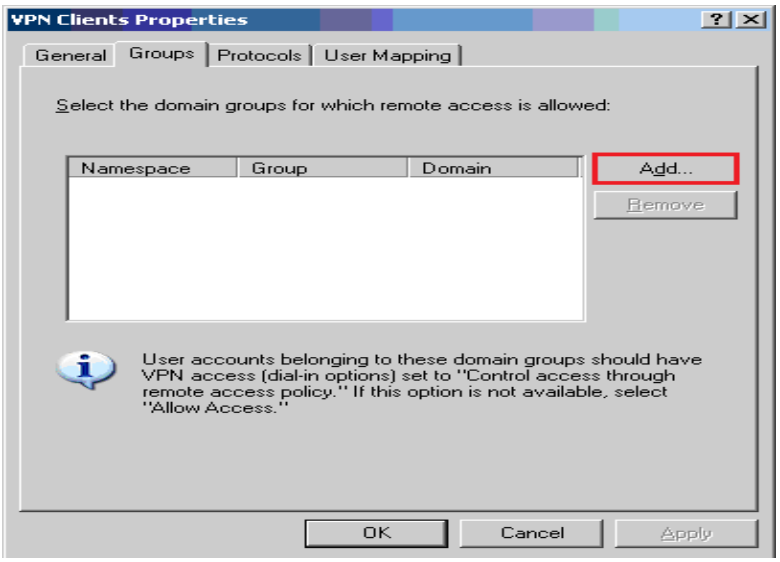
Click OK



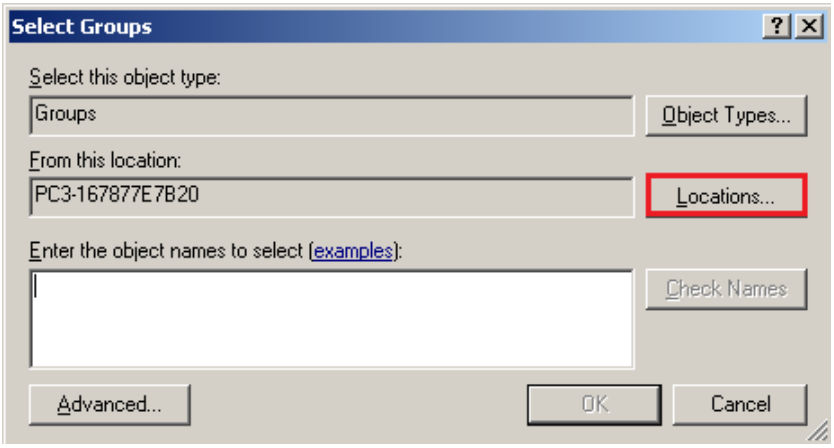
Click Enable VPN Client Access, vào tab General Check Enable VPN client access, sau đó Click OK



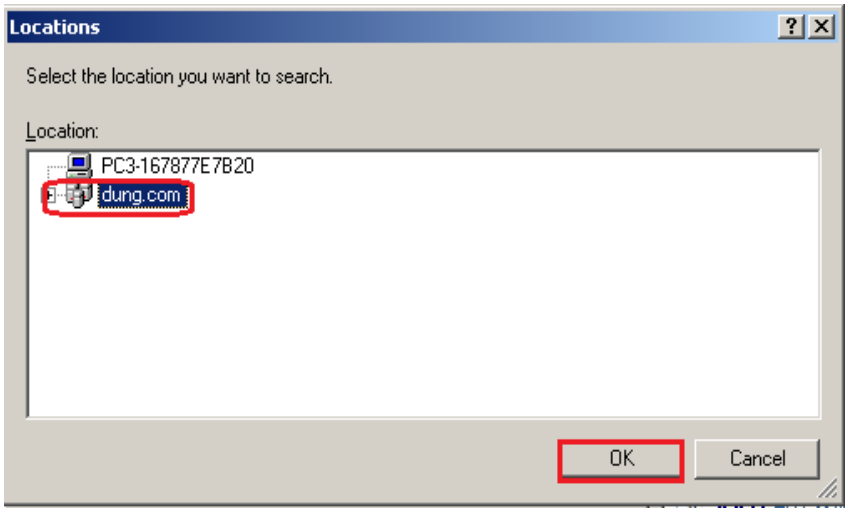
Click specify Windows Users



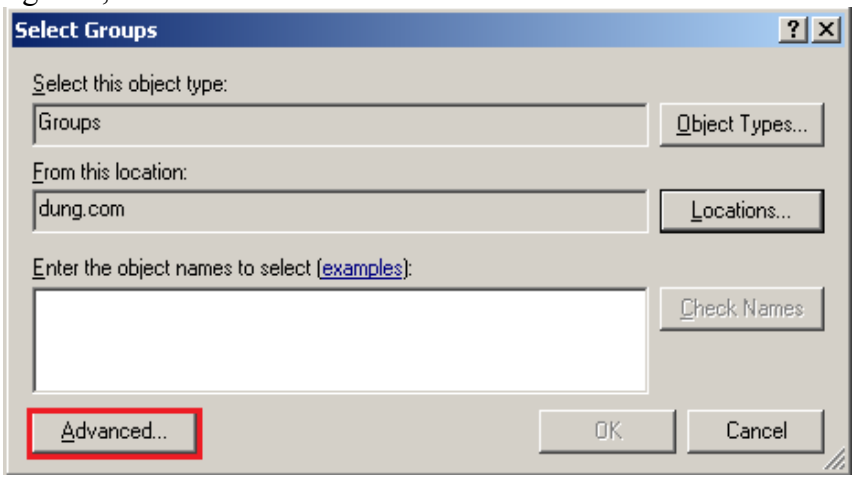
Click Add



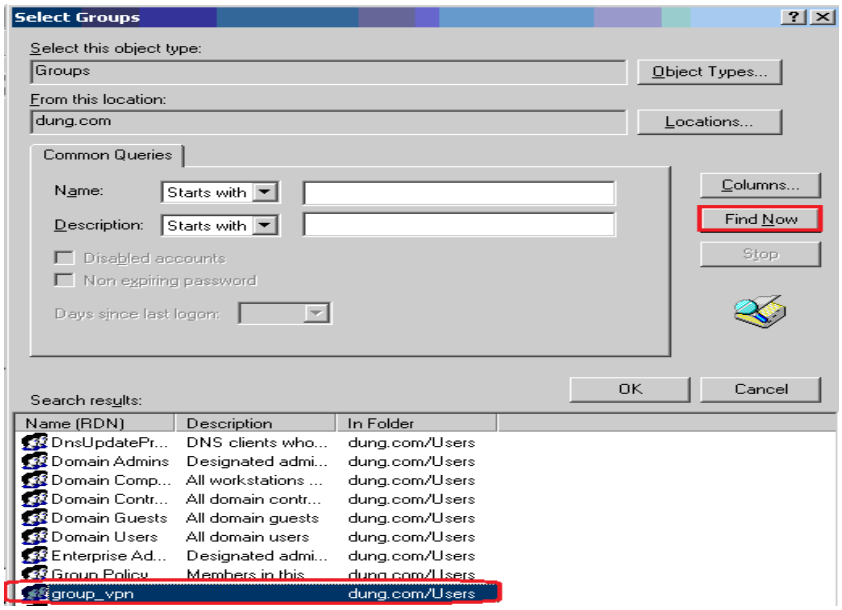
Click locations…



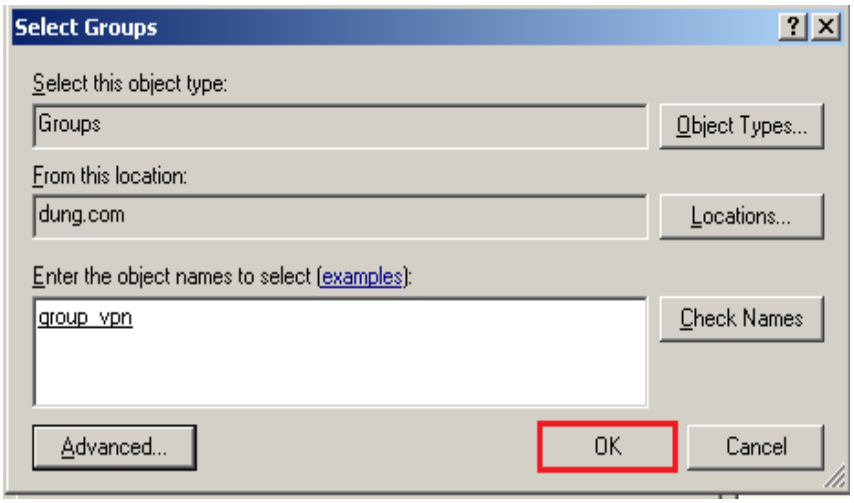
Chọn dung.com, sau đó Click OK



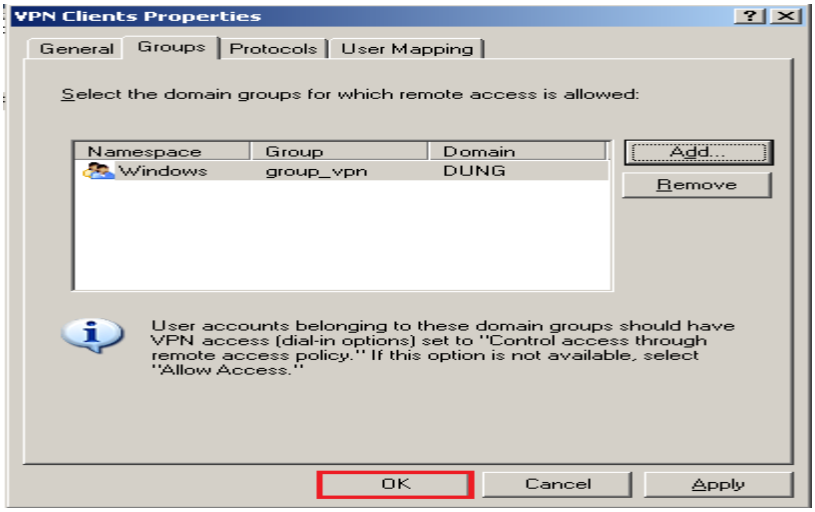
Click Advanced…



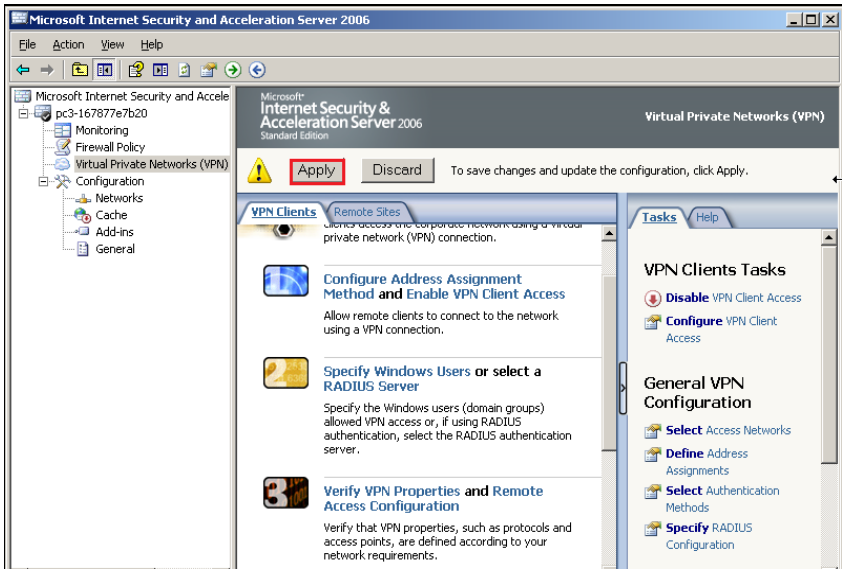
Click Find Now, sau đó Doubleclick group_vpn



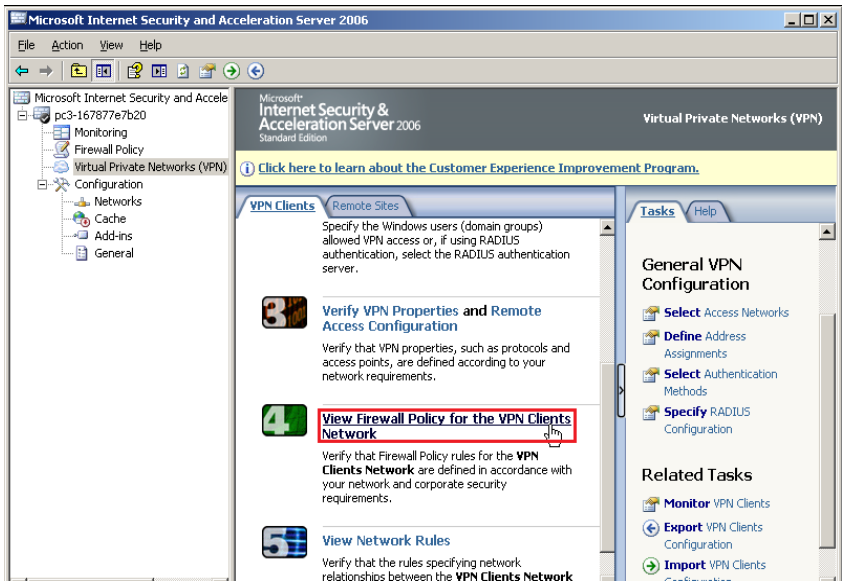
Click OK



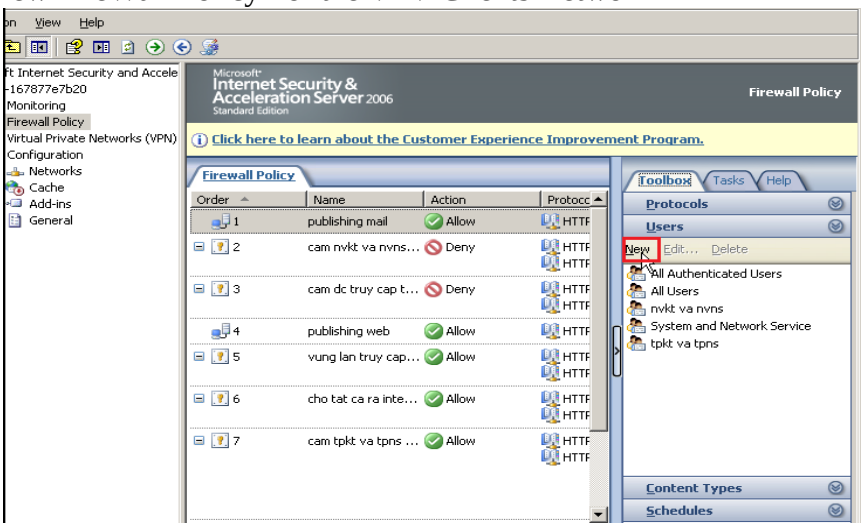
Click OK



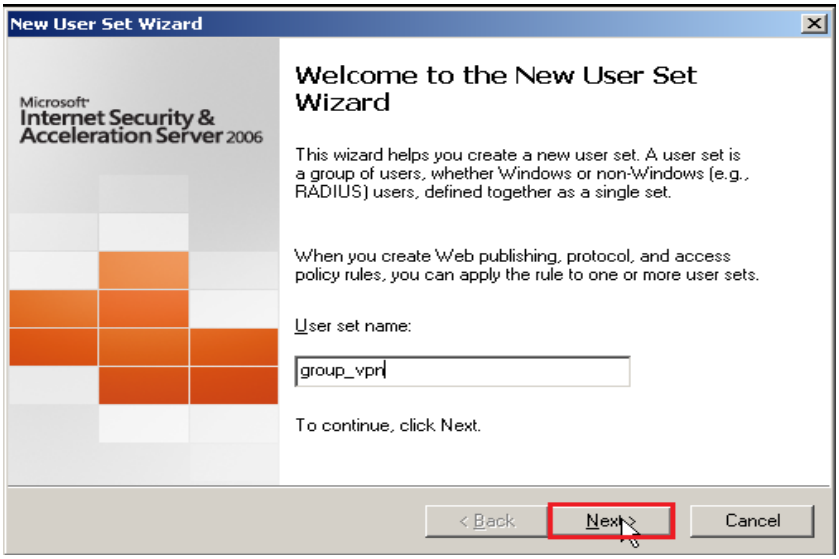
Click Apply



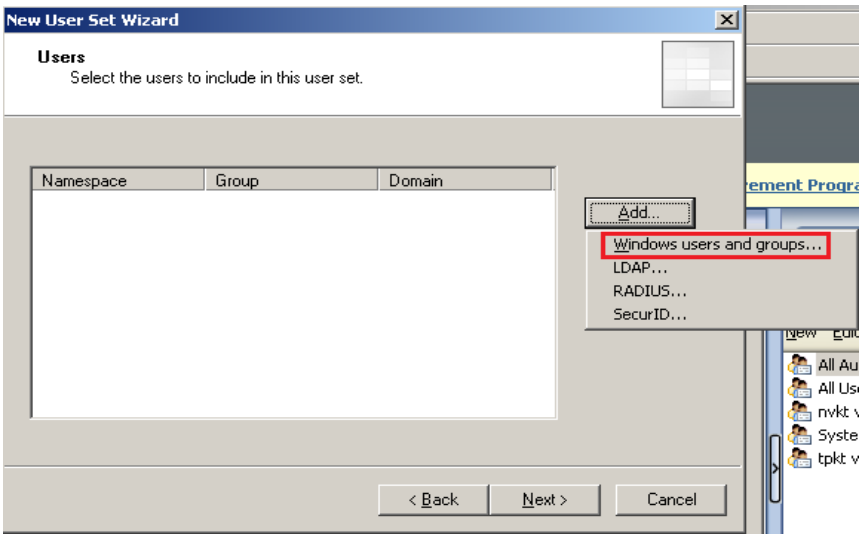
Click View FireWall Policy For the VPV Clients Network



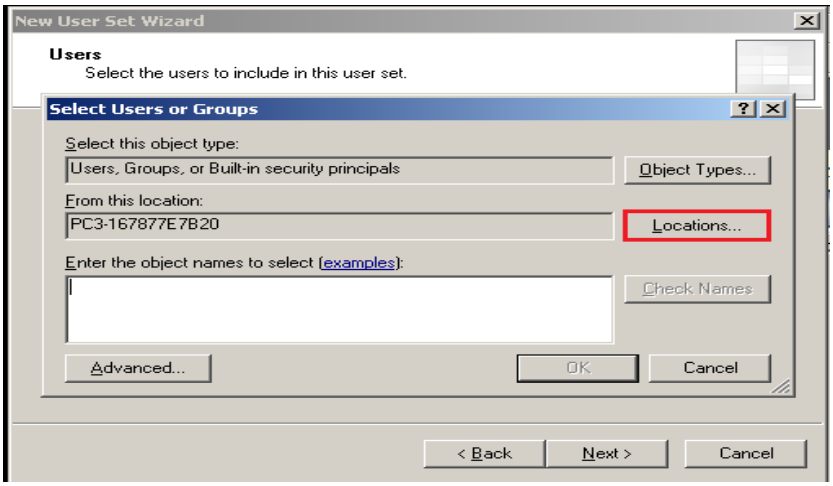
Click New



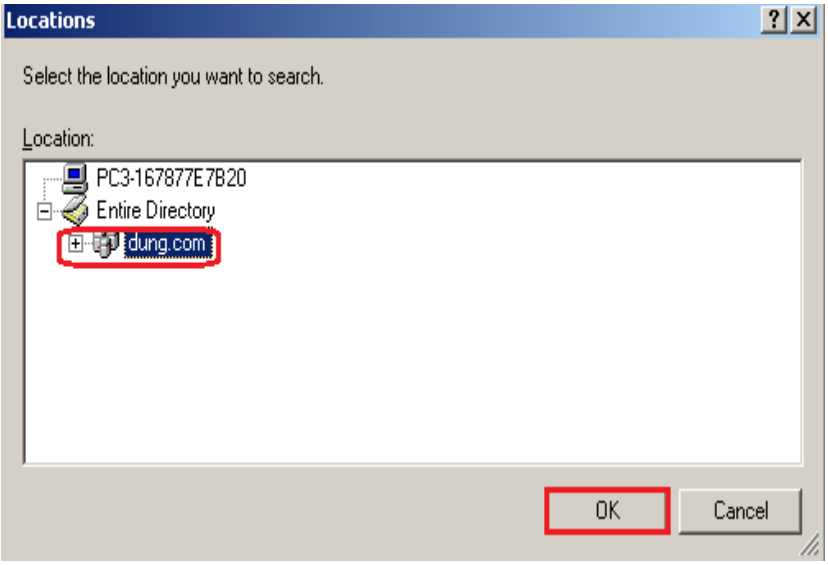
Điền User set name, sau đó Click Next



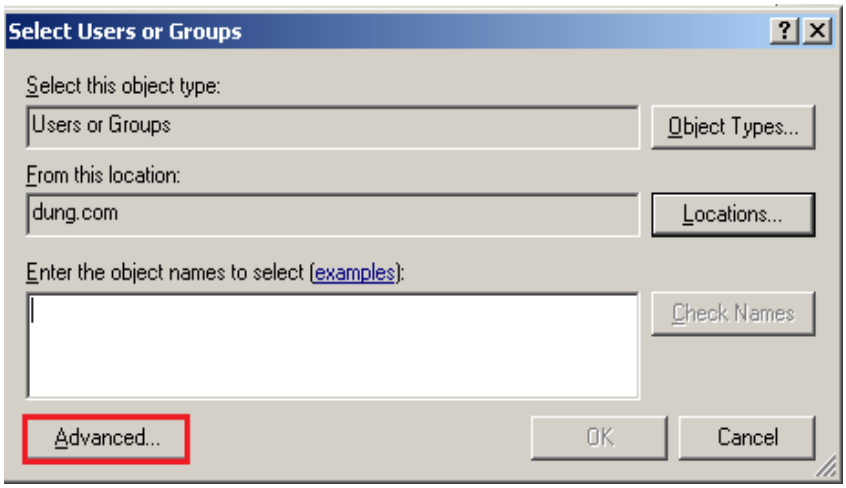
Click Add\Windows users and groups…



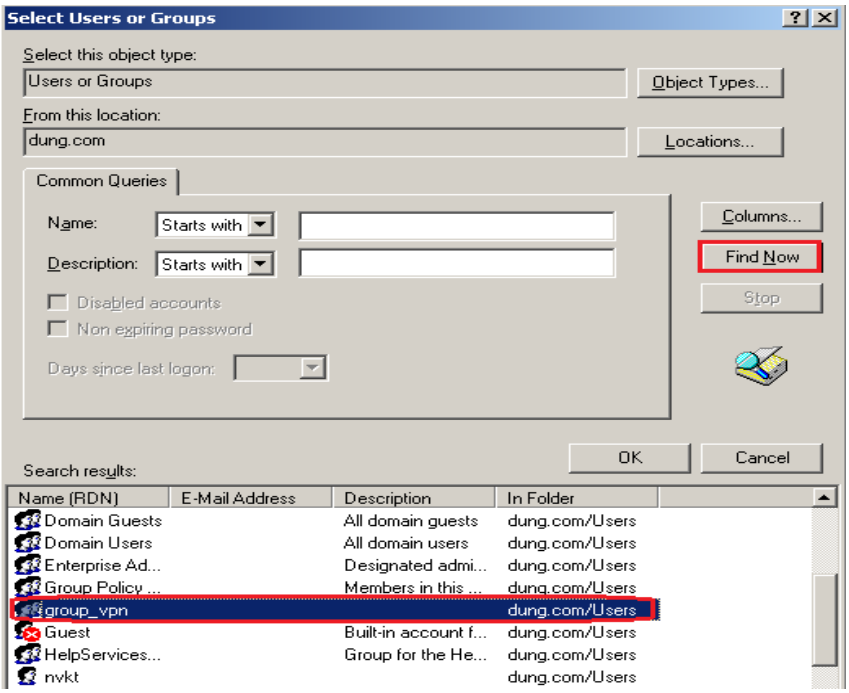
Click Locations



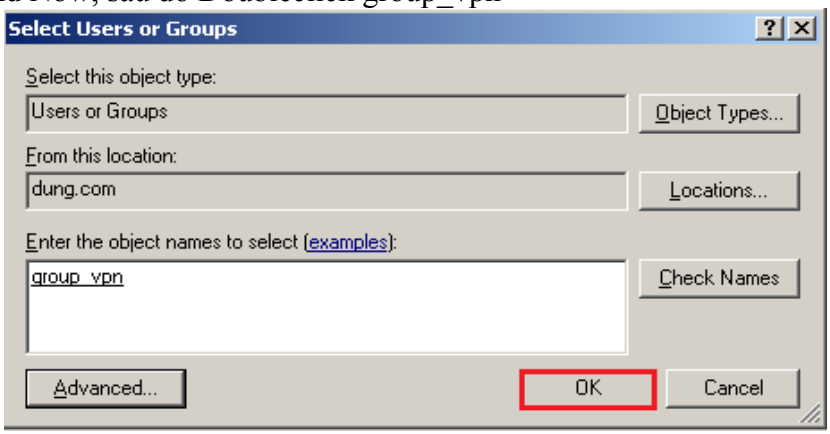
Chọn dung.com, sau đó Click OK



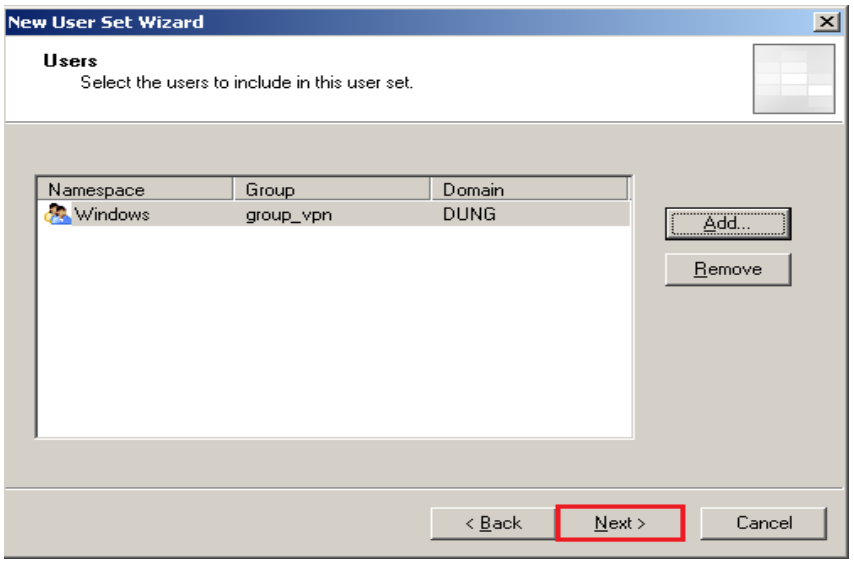
Click Advanced…



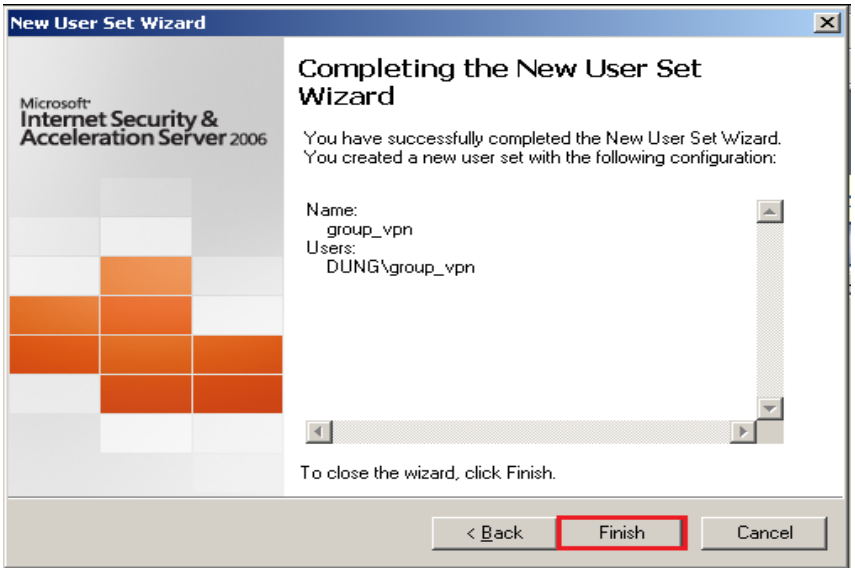
Click Find Now, sau đó Doubleclick group_vpn



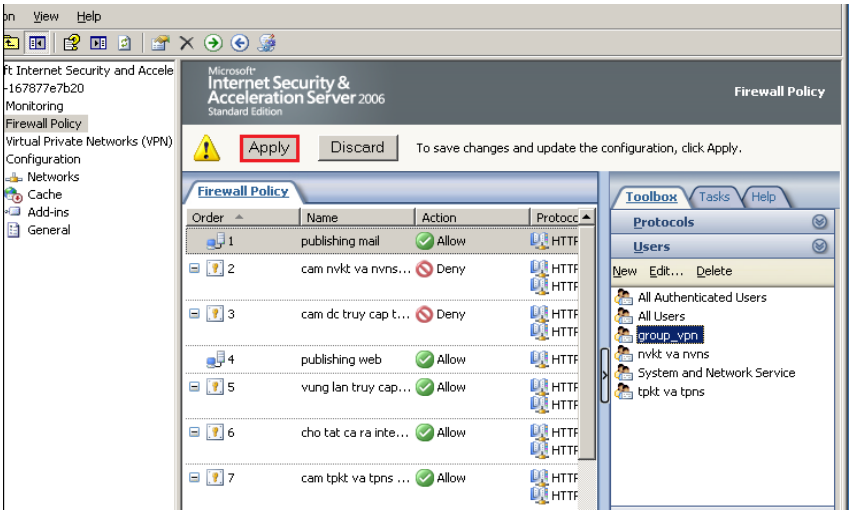
Click OK



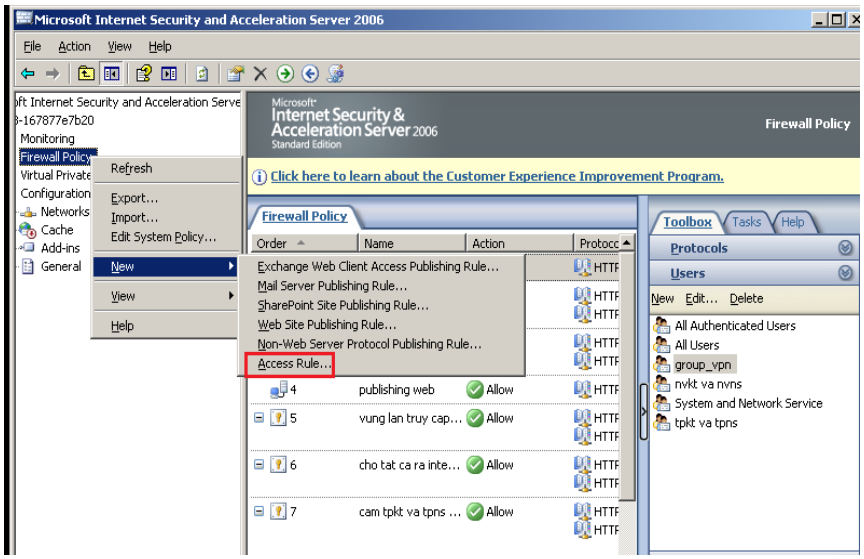
Click Next



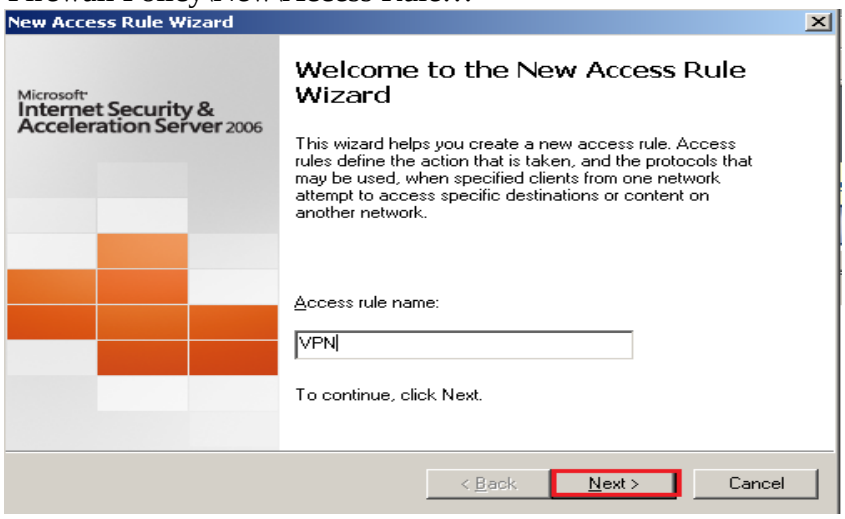
Click Finish



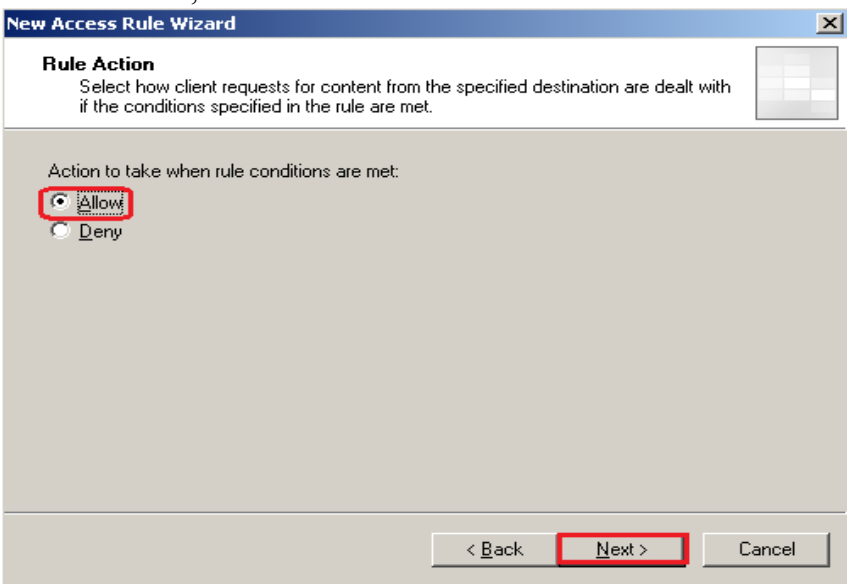
Click Apply



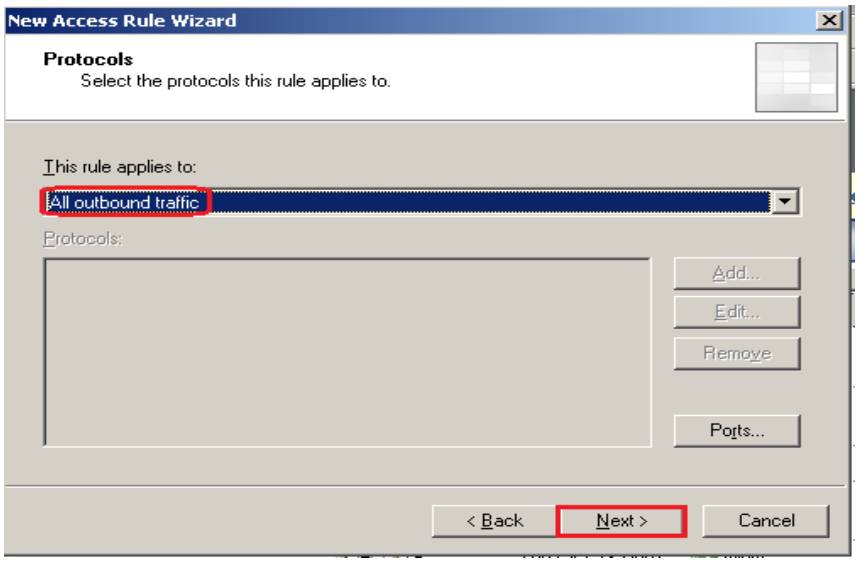
R_Click Firewall Policy\New\Access Rule…



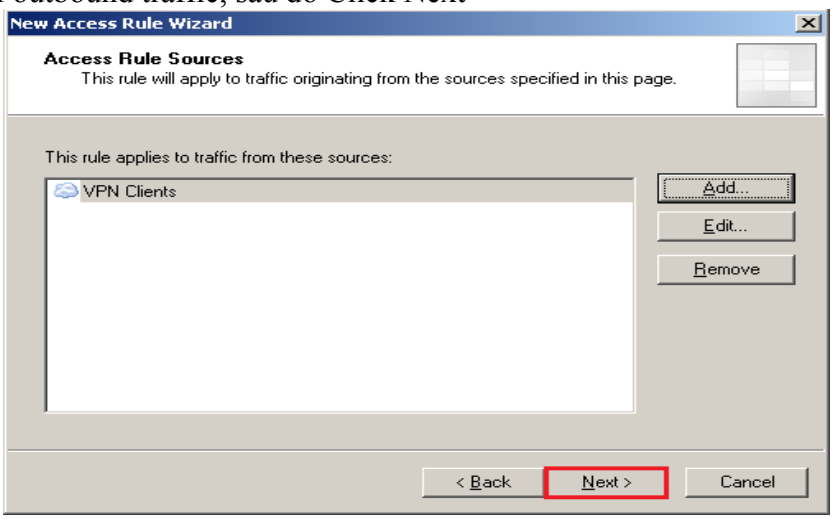
Điền Access rule name, sau đo Click Next



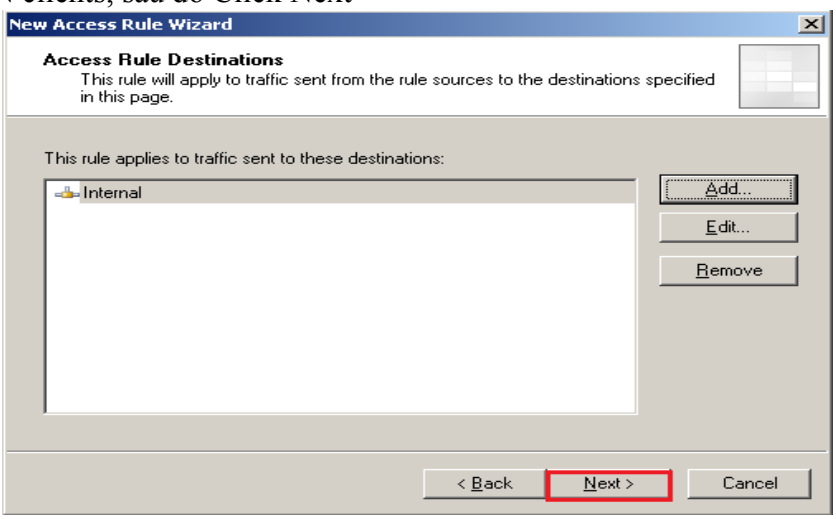
Chọn Allow, sau đó Click Next



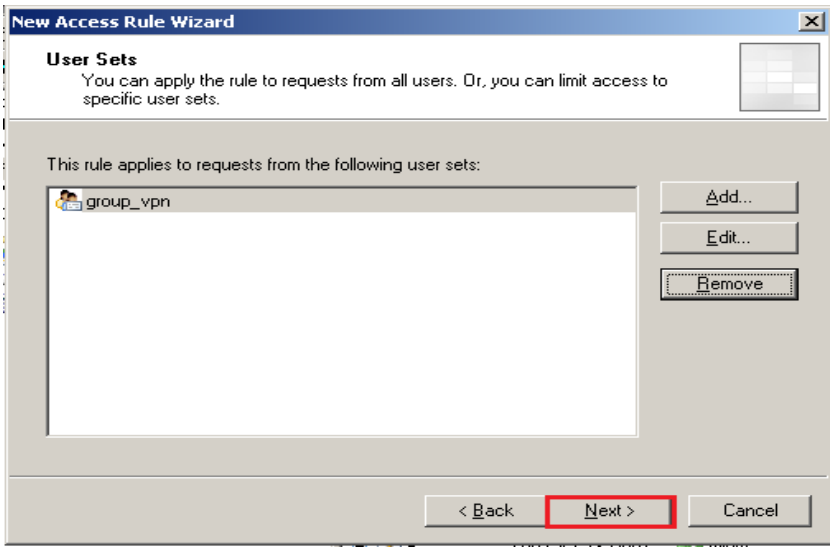
Chọn All outbound traffic, sau đó Click Next



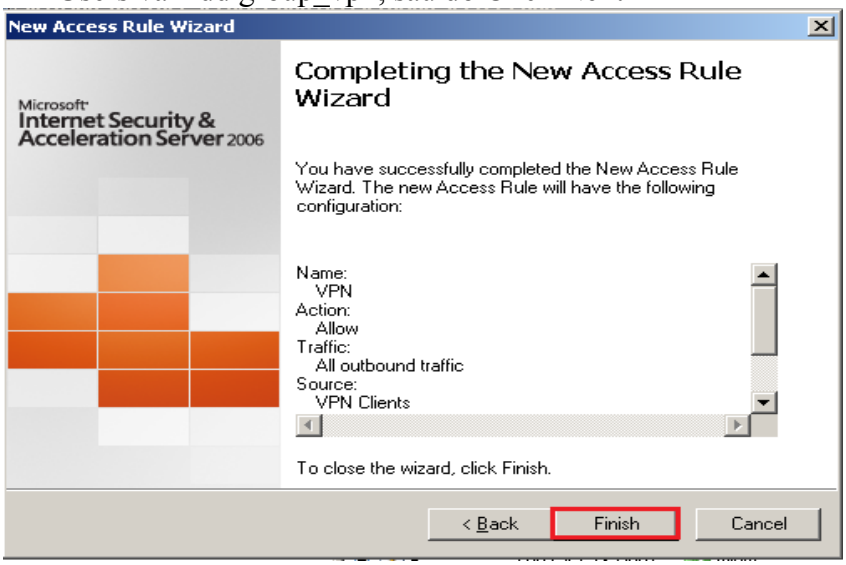
Add VPN clients, sau đó Click Next



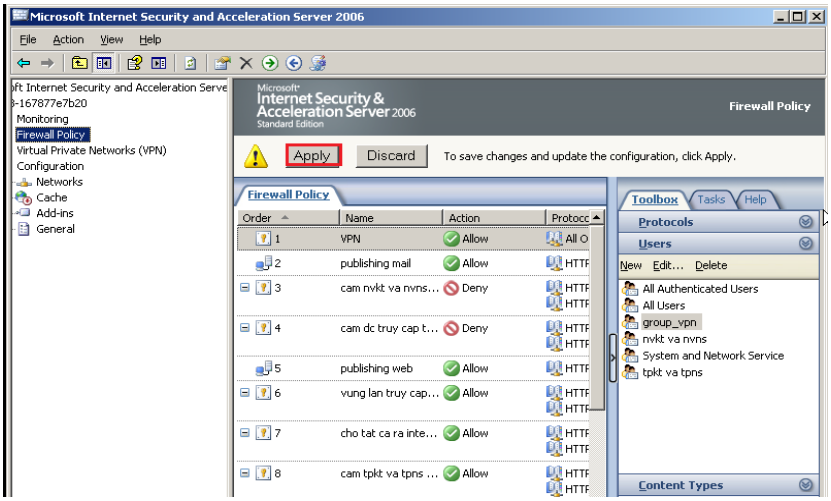
Add Internal, sau đó Click Next



Remove All Users và Add group_vpn, sau đó Click Next

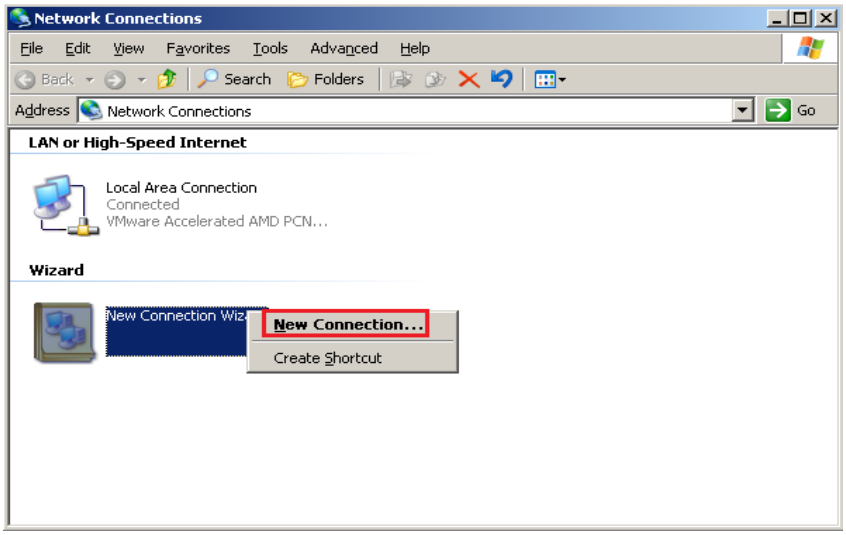


Click Finish



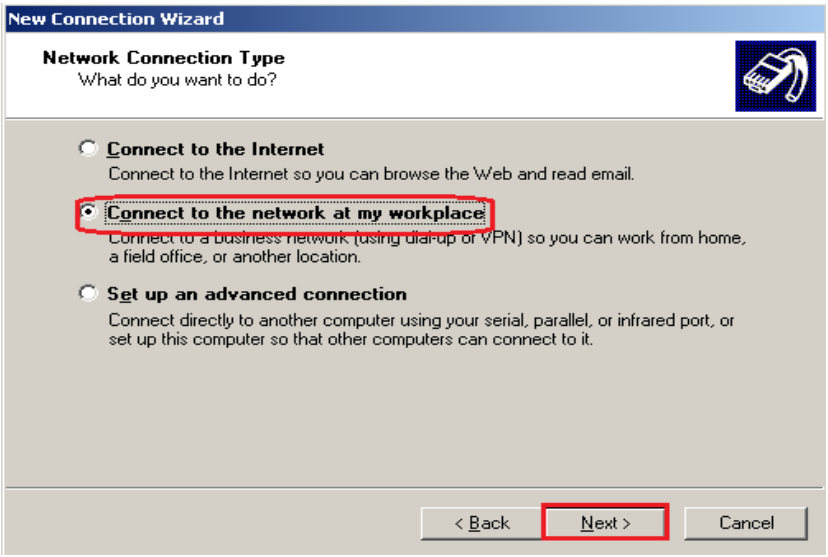
Click Apply

Bước 3: Cấu hình tạo một connection cho người dung internet sử dụng dịch vụ truy cập từ xa.

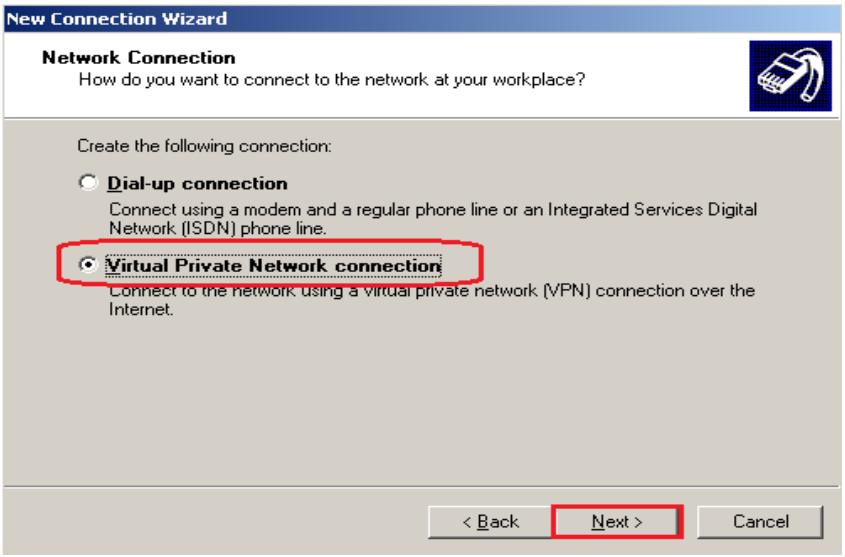


R_Click My Network Places\Properties. R_Click New Connection Wizard\New Connection…

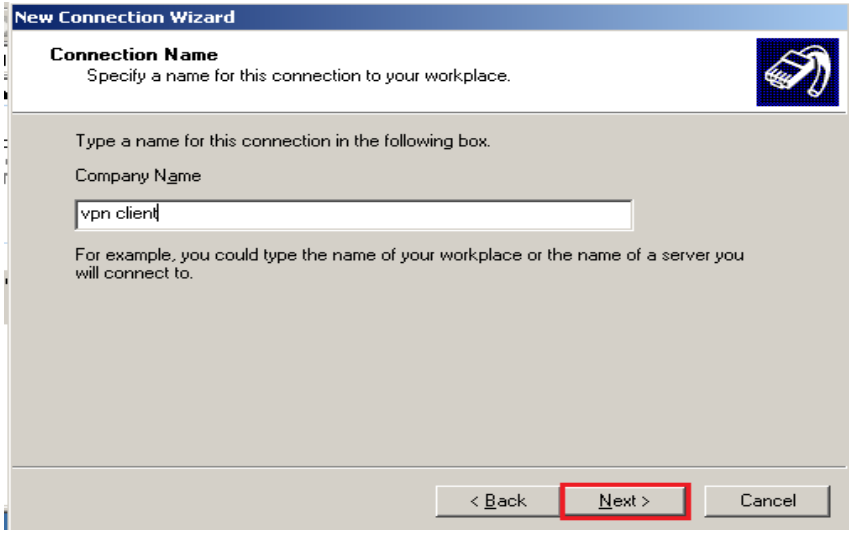
Click Next



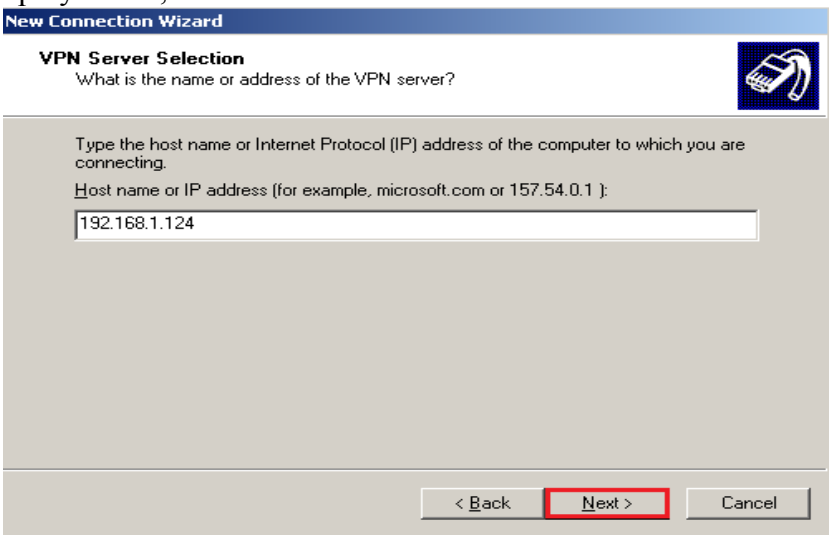
Chọn option Connect to the network at my workplace, sau đó Click Next



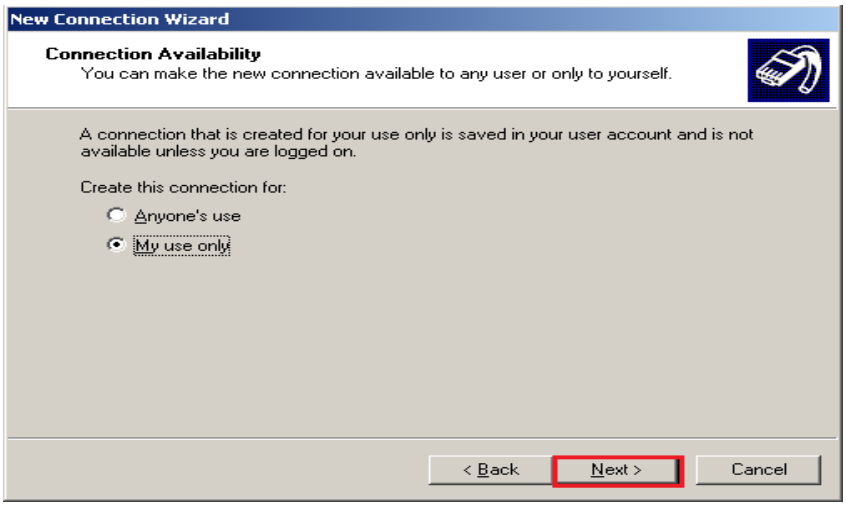
Chọn option Virtual Private Network connection



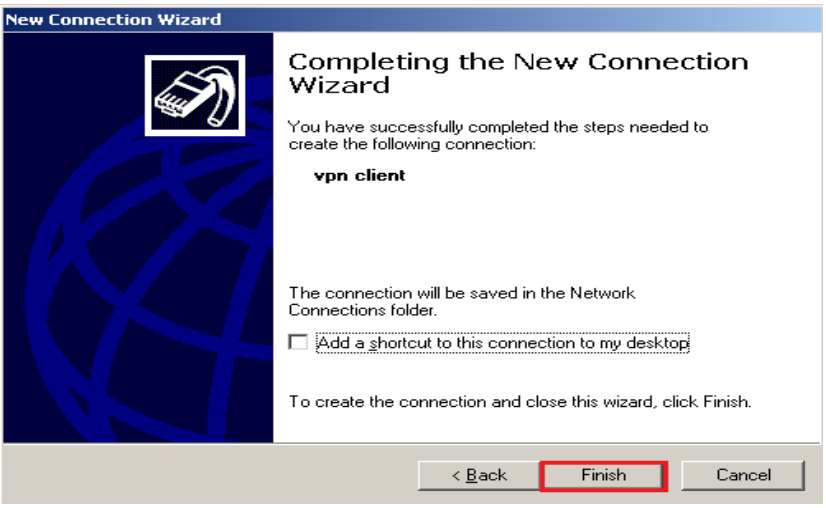
Điền Compary Name, sau đó Click Next



Điền Host name or IP address, sau đó Click Next

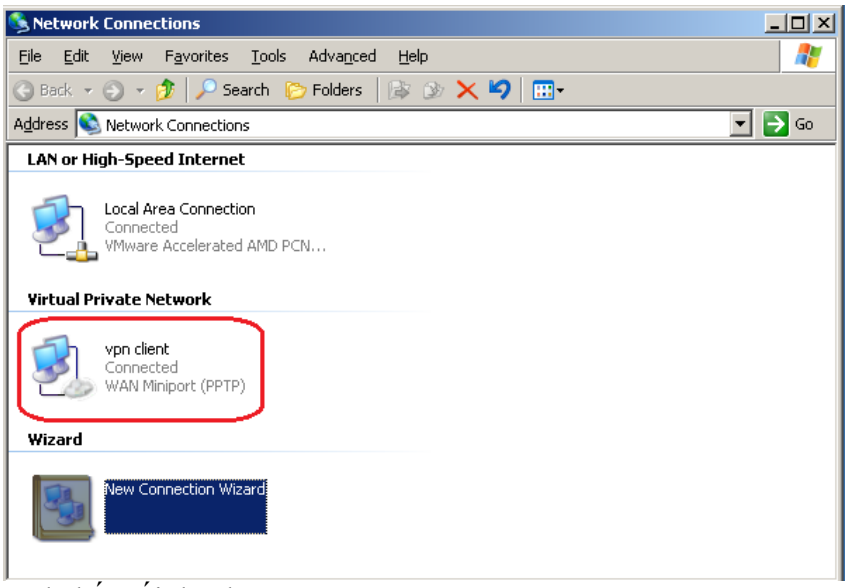


Click Next

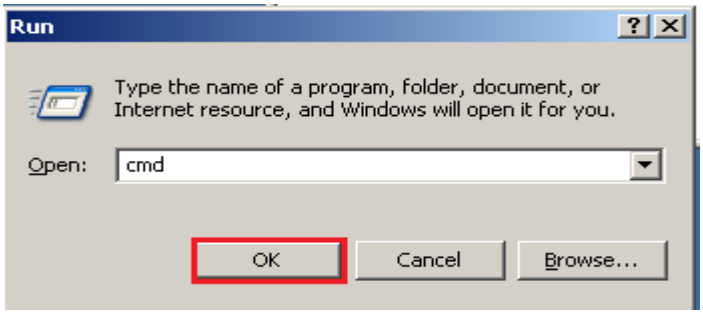


Click Finish

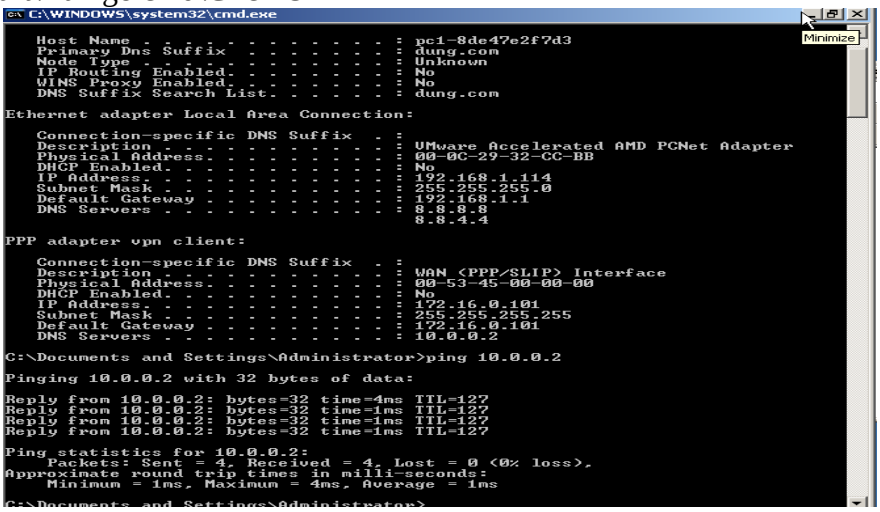
Điền User name và Password, sau đó Click Connect

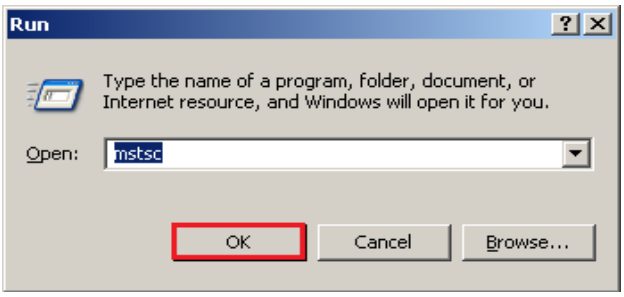


Vpn client đã kết nối thành công

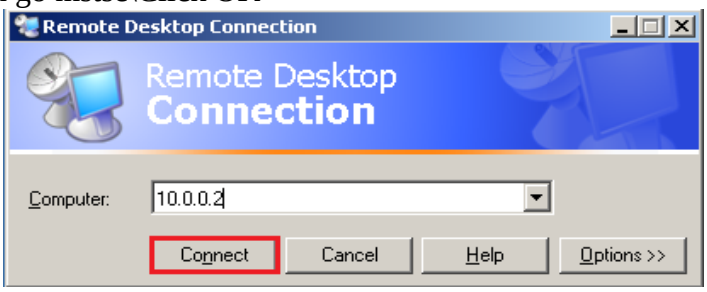


Vào Start\Run gõ cmd\Click OK

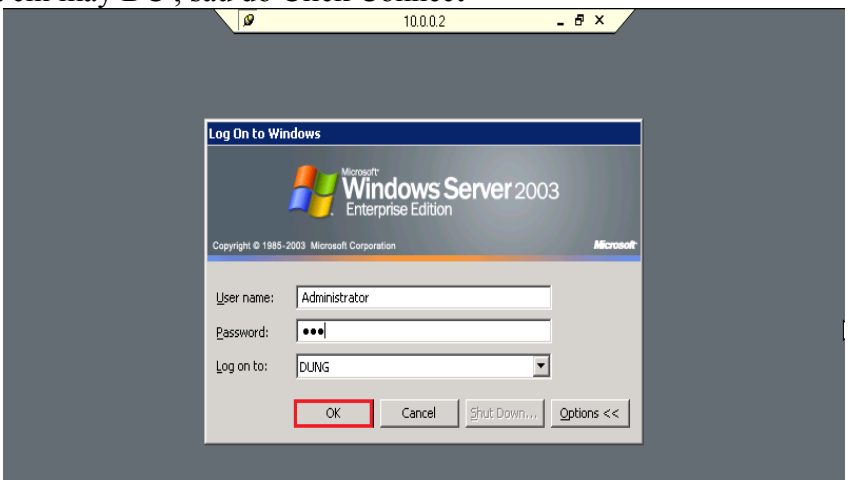




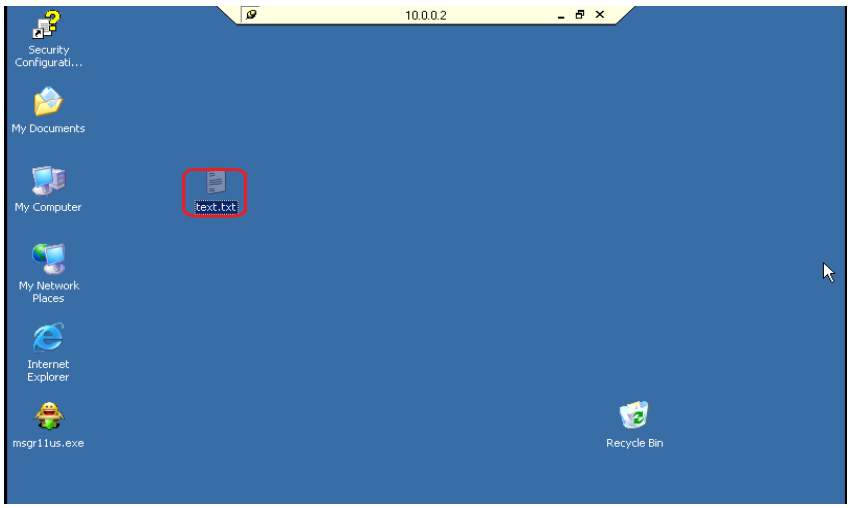
Vào Start\Run gõ mstsc\Click OK



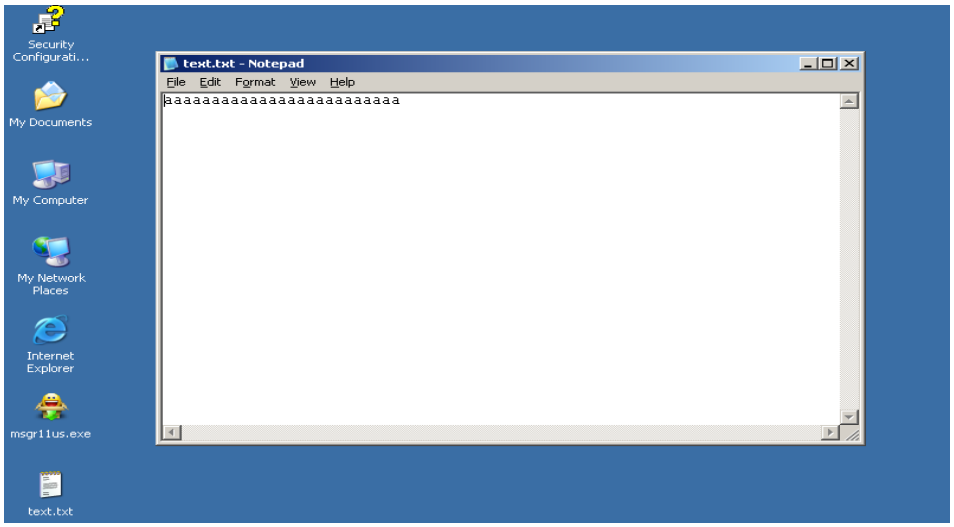
Điền địa chỉ máy DC , sau đó Click Connect



Điền User name và Password , Sau đó Click OK



Trên giao diện máy DC tạo File Text.text



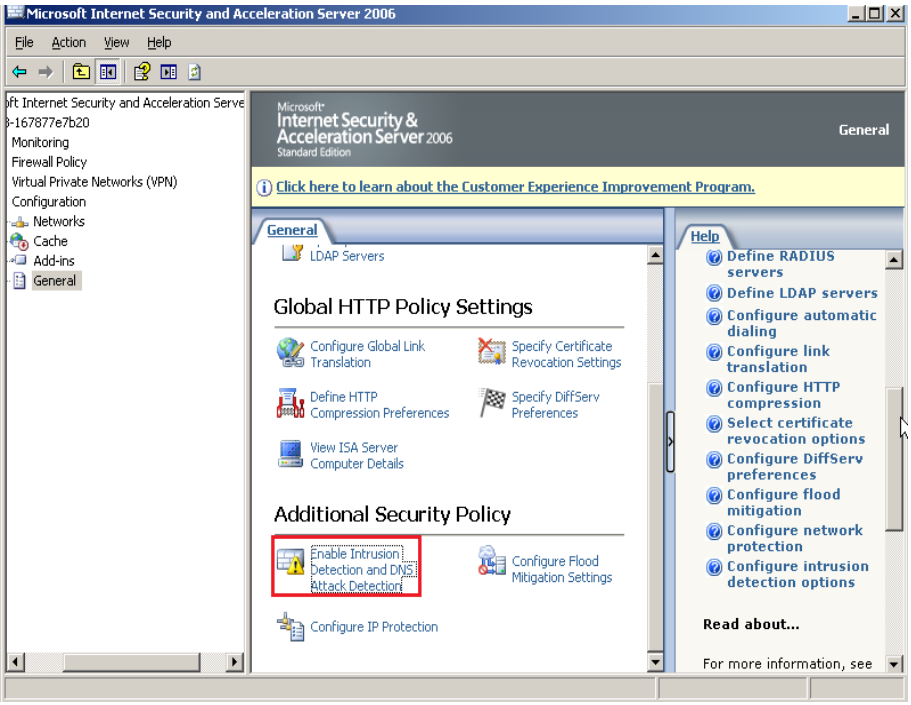
Sang máy DC mở file text.text với nội dung như trên

9. Intrusion Detection

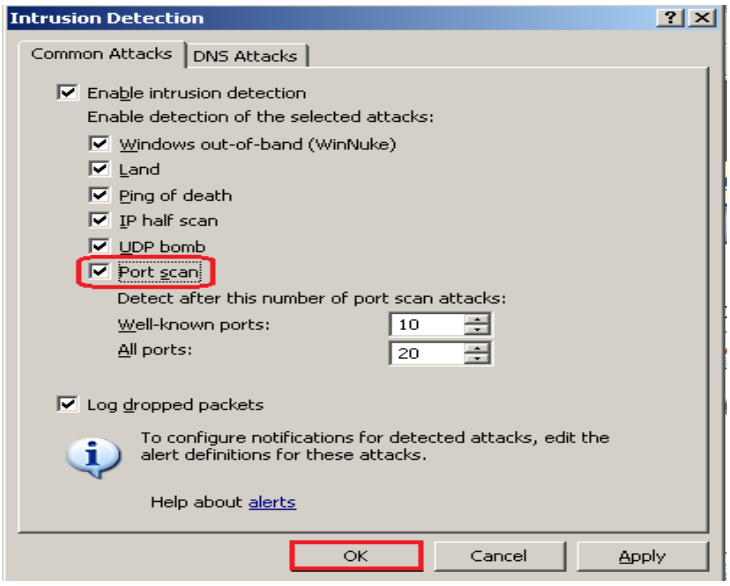
Giả sử mạng đã dựng thành công ISA Server khi đó một Hacker nào đó từ bên ngoài mạng Internet tìm mọi cách tấn công mạng nội bộ bằng cách dò tìm các Port được mở trong mạng và khai thác các lỗ hổng trên các Port này.

Như vậy nếu hệ thống không có ISA Server sẽ không hề hay biết sự nguy hiểm đang rình rập này. Trong phần này sẽ tìm hiểu về một tính năng rất hay của ISA Server là Intrusion Detection dùng để phát hiện các tấn công từ bên ngoài vào hệ thống mạng nội bộ.

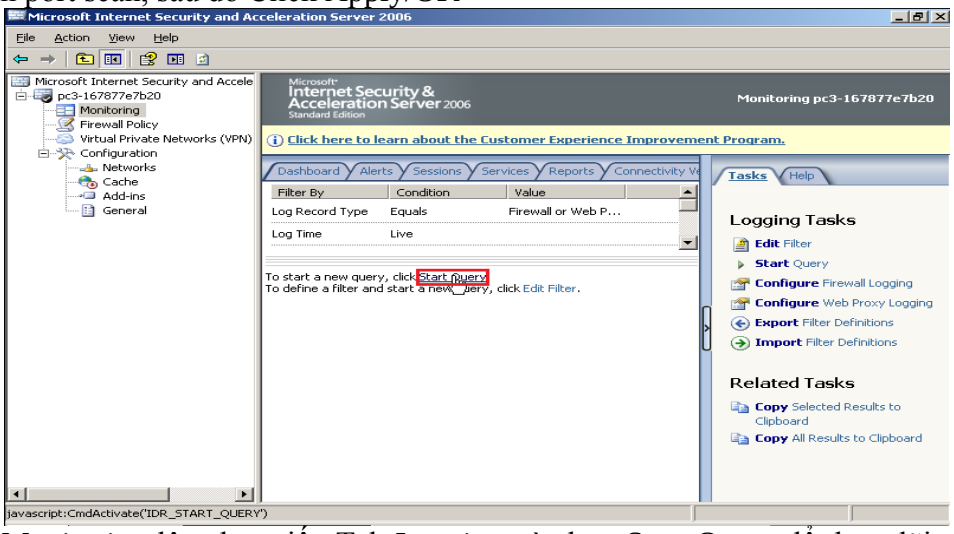
Bật chương trình ISA Server lên chọn Configuration chọn tiếp mục General



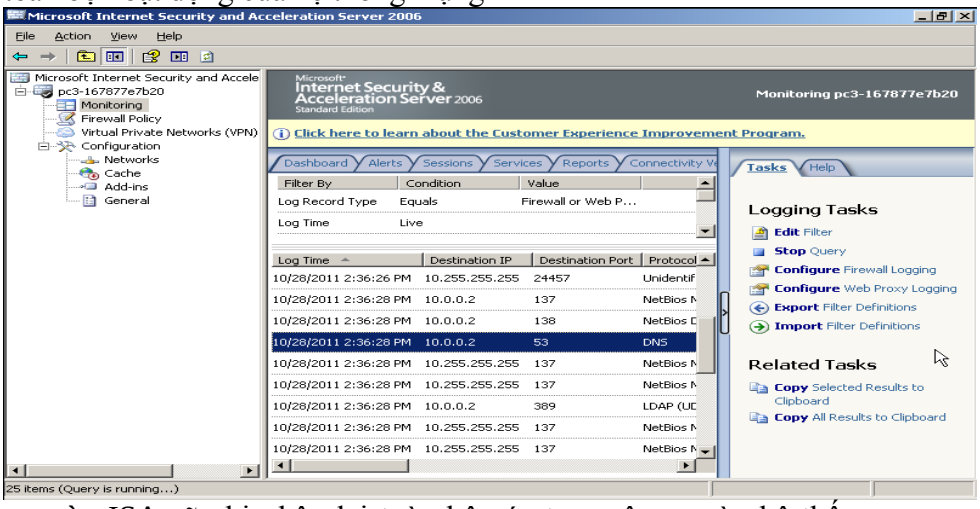
Click Enable Intrusion Detection and DNS Attack Detection



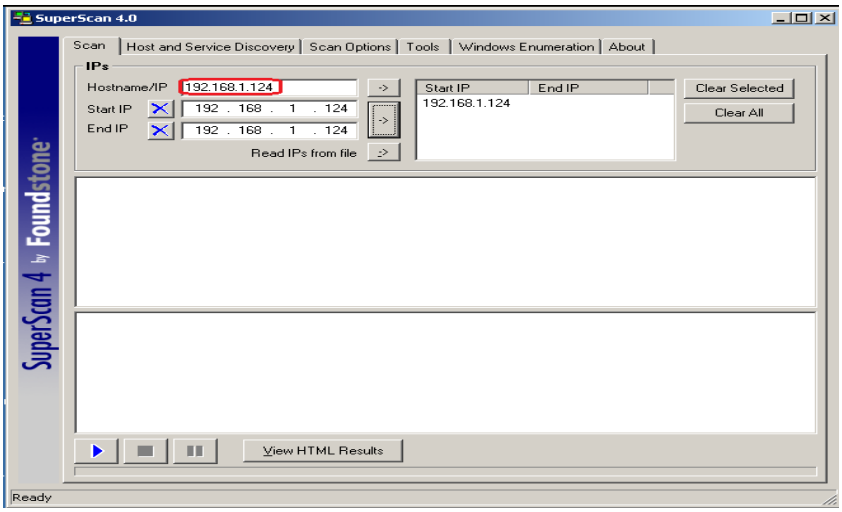
Chọn port scan, sau đó Click Apply/OK



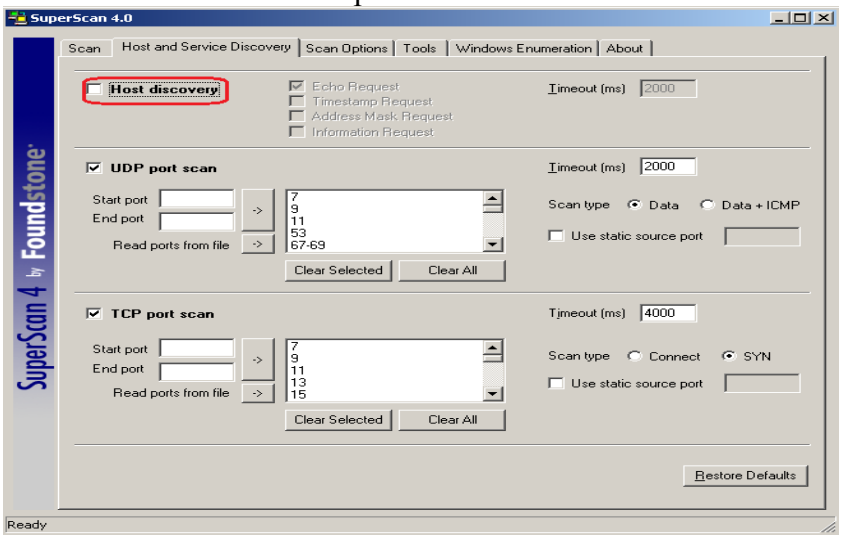
Bật Monitoring lên chọn tiếp Tab Logging và chọn Start Query để theo dõi giám sát toàn bộ hoạt động của hệ thống mạng



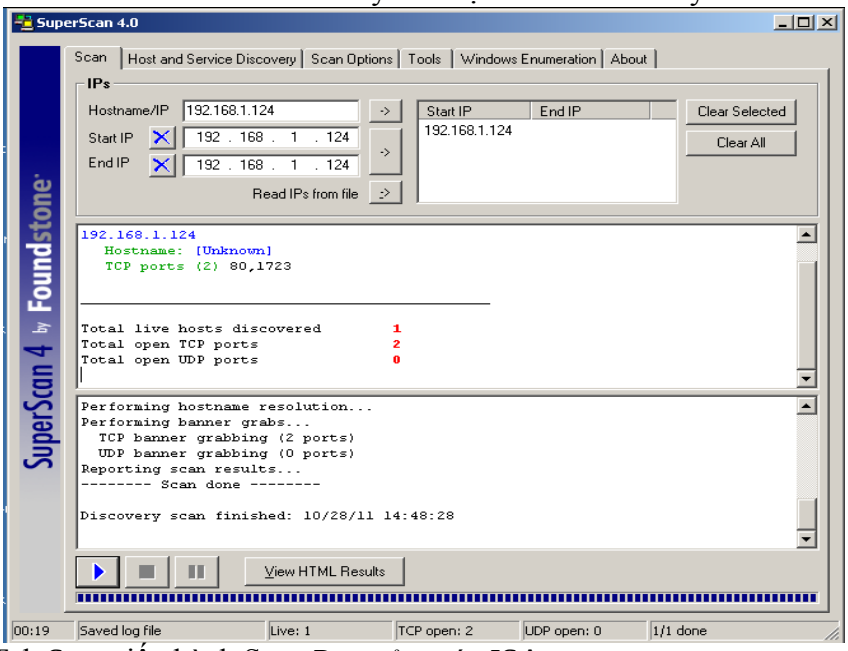
Trong này ISA sẽ ghi nhận lại toàn bộ các truy cập ra vào hệ thống mạng một cách chi tiết



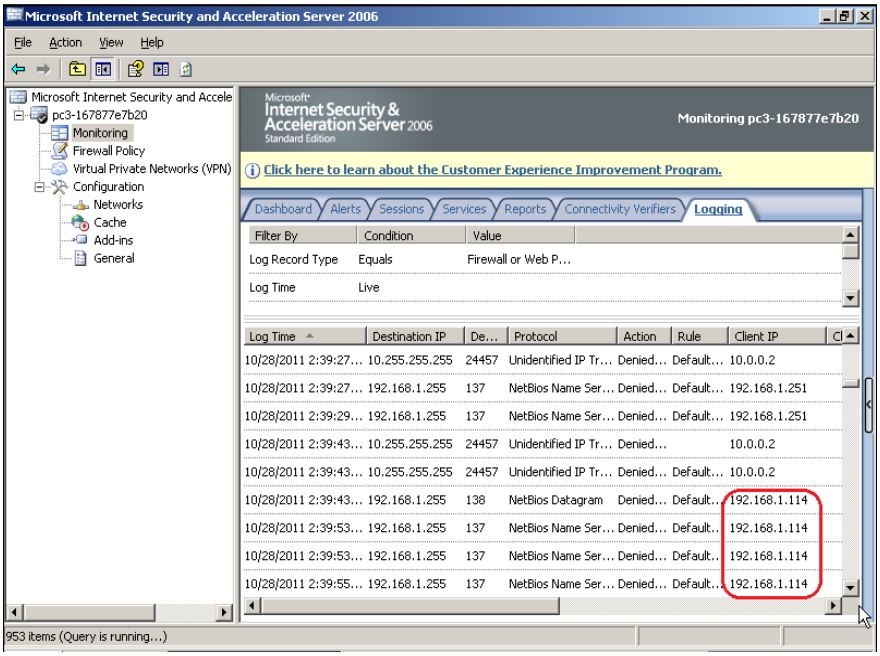
Bây giờ tại máy Client internet cài đặt một chương trình có tính năng Scan các Port đã mở trên ISA Server đó là SuperScan 4.0



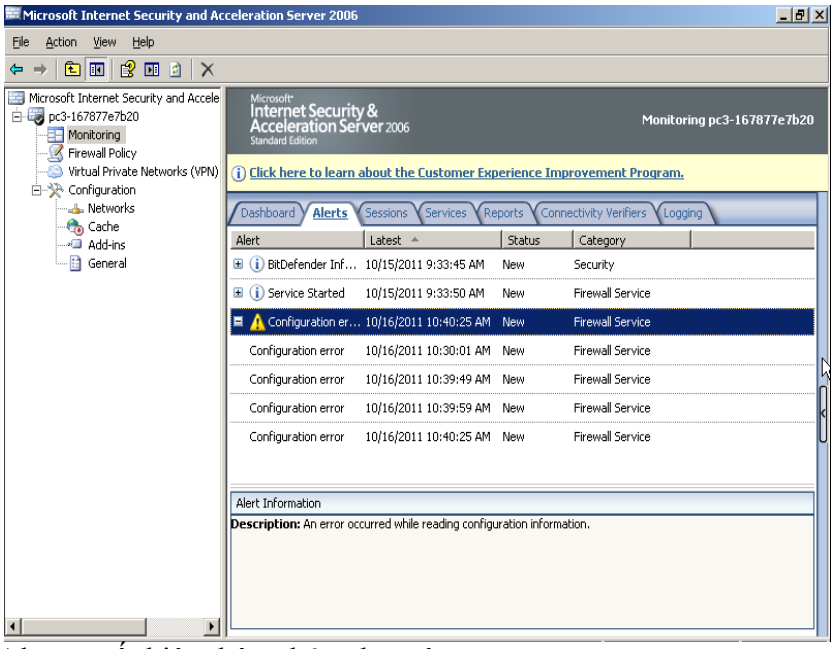
Chọn Tab Host and Service Discovery bỏ chọn Host Discovery



Trở lại Tab Scan tiến hành Scan Port của máy ISA



Trở lại máy ISA Server bật lại Logging sẽ thấy các truy cập từ máy Client vào mạng



Vào tab Alerts xuất hiện thông báo như trên

10. Caching

Một trong những đặc trưng khiến Proxy server được ưu chuộng là khả năng caching, tức là khả năng lưu trữ các trang web mà proxy server từng truy cập.

Isa server sẽ có khả năng thực hiện Forward Caching và Reverse caching.

- **Cơ chế reverse caching:**

Khi có một internet client truy cập vào một internal web server được publish thông qua ISA server, proxy server trên ISA sẽ truy cập web cho client và lưu trữ nội dung website.

Khi các internet client khác truy cập vào internal web server, nếu nội dung có sẵn trong cache thì proxy server sã lấy ra mà không cần phải truy cập web server nữa.

- **Cơ chế Forward Caching**

Khi một internal client truy cập vào trang web nào đó thì ISA sẽ tự đọng lưu nội dung trang web đó trông cache của mình.

Nếu một internal khác truy cập vào trang web mà ISA đã cache lại thi ISA sẽ lấy nội dung lưu trong cache truyền cho client đó.

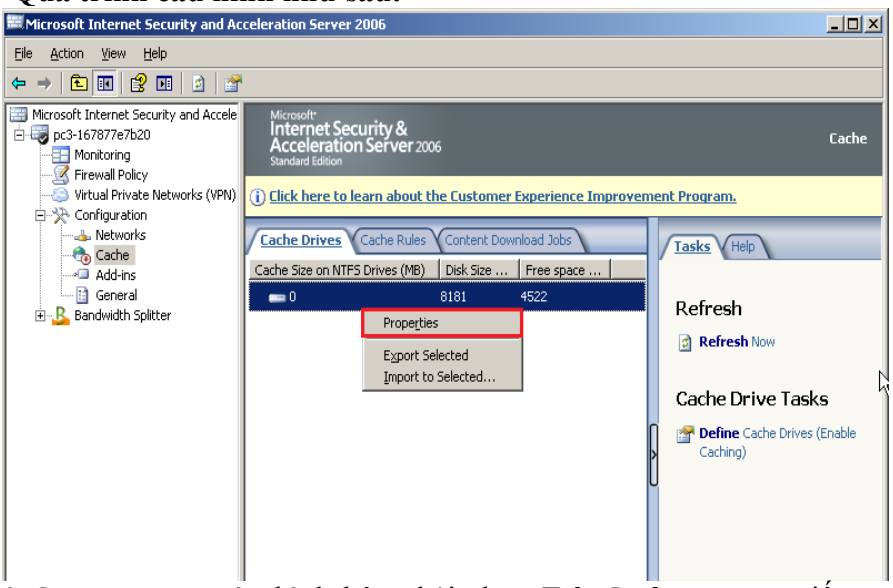
- **Một số vấn đề liên quan đến ổ đĩa lưu cache**

Đĩa cache phải là ổ đĩa cục bộ (local drive).

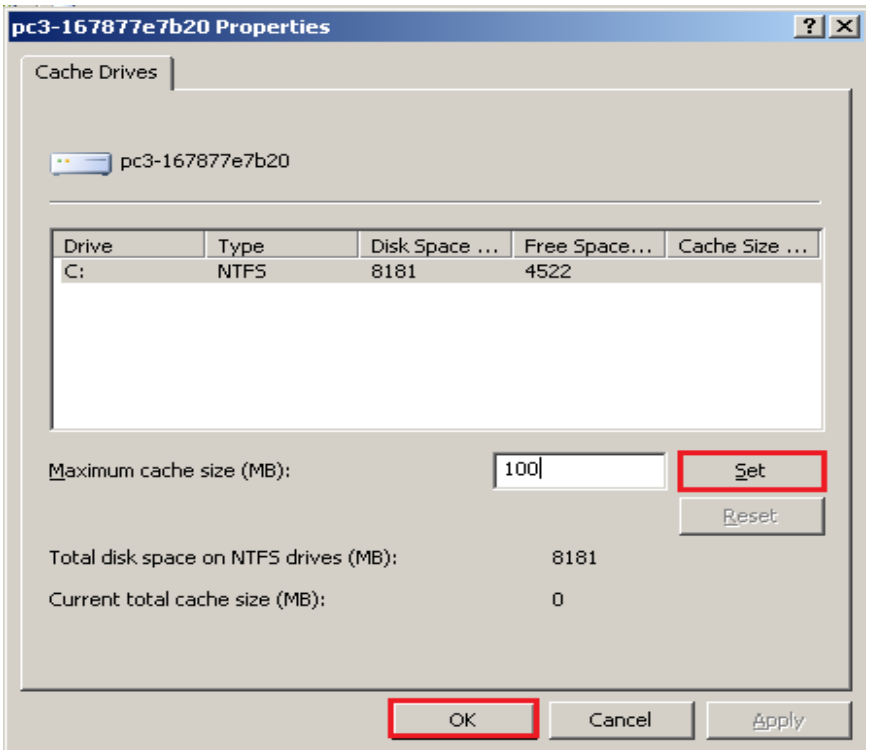
Đĩa cache phải được định dạng NTFS.

Để tối ưu hóa hiệu năng, nên lưu cache trên một đĩa vật lí khác với đĩa hệ thống và đĩa cài đặt chương trình ISA.

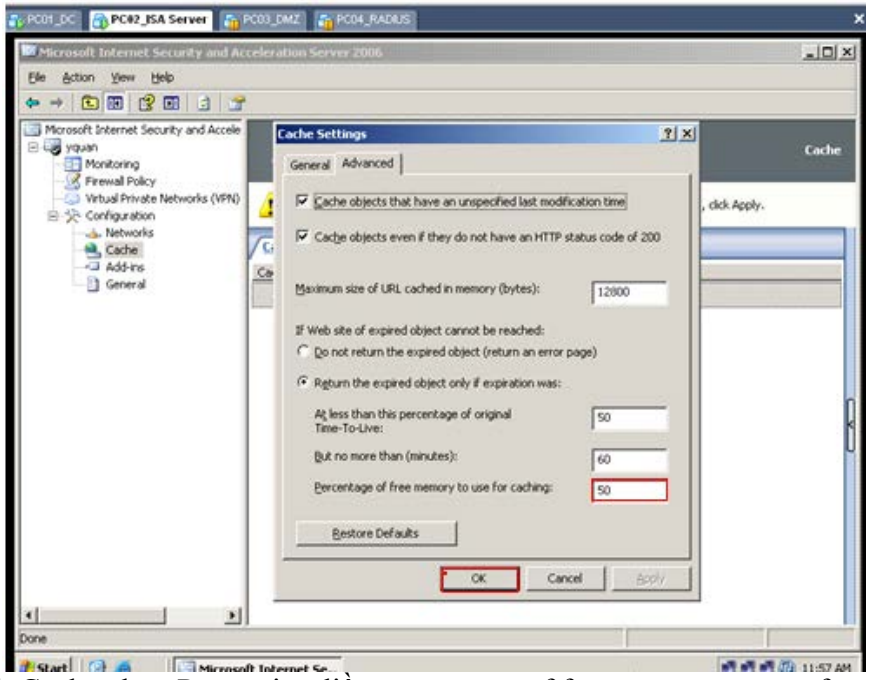
- **Quá trình cấu hình như sau:**



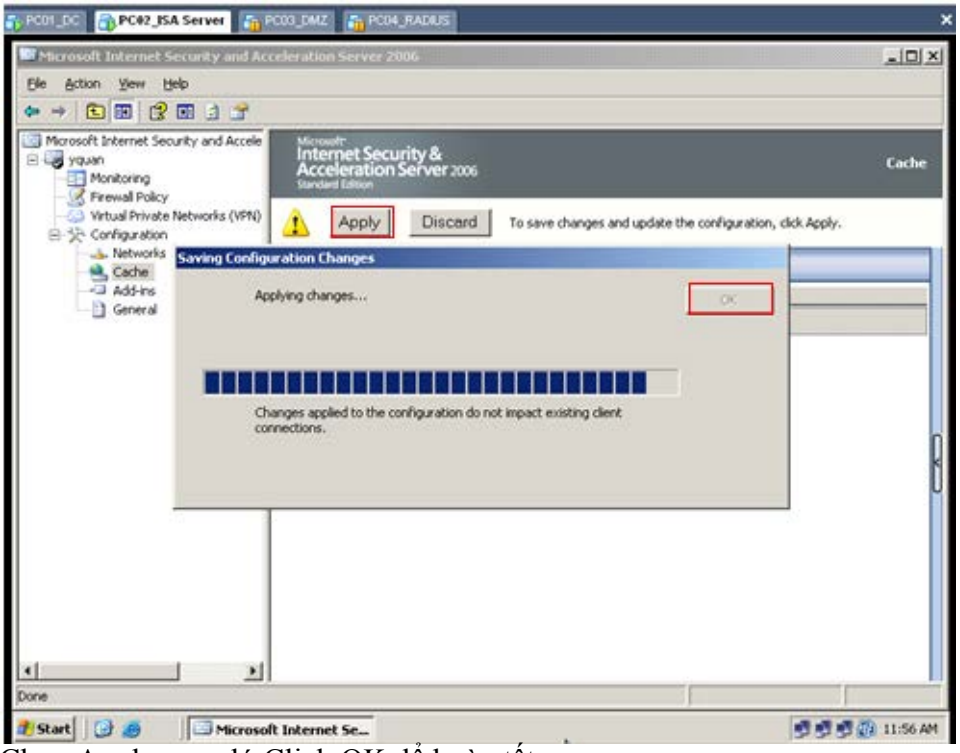
Tại ISA Server trong màn hình bên phải chọn Tab Cache Drivers tiếp tục nhấp phải vào Cache Driver chọn Properties



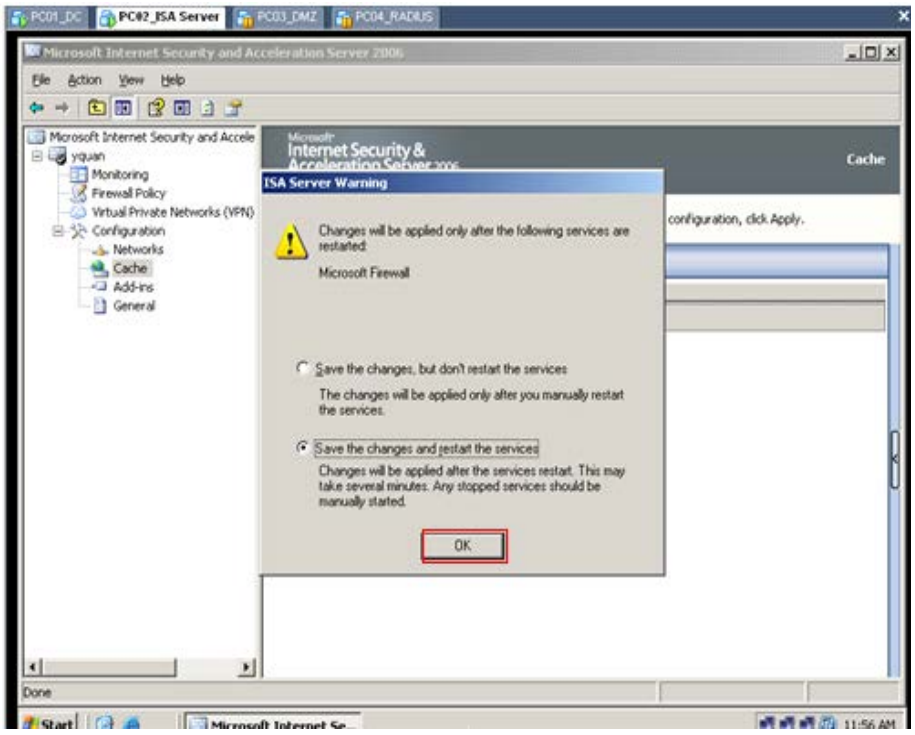
Set giá trị Cache cho ISA trong bài là 100MB, sau đó Click OK



R_Click Cache chọn Properties điền percentage of free memory to use for caching là 50, Sau đó Click OK

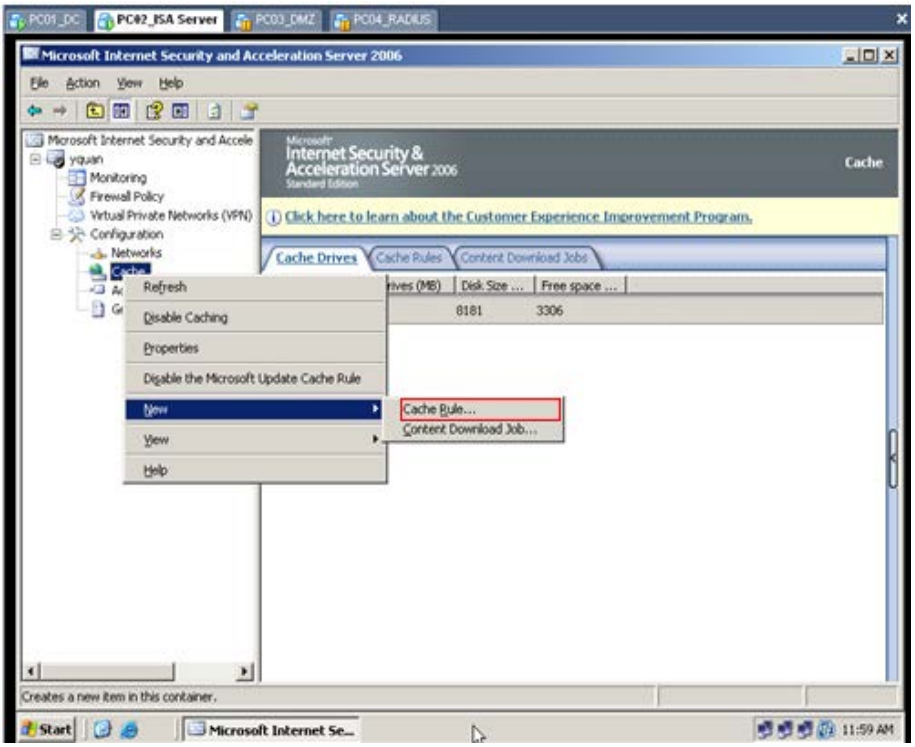


Chọn Apply, sau đó Click OK để hoàn tất

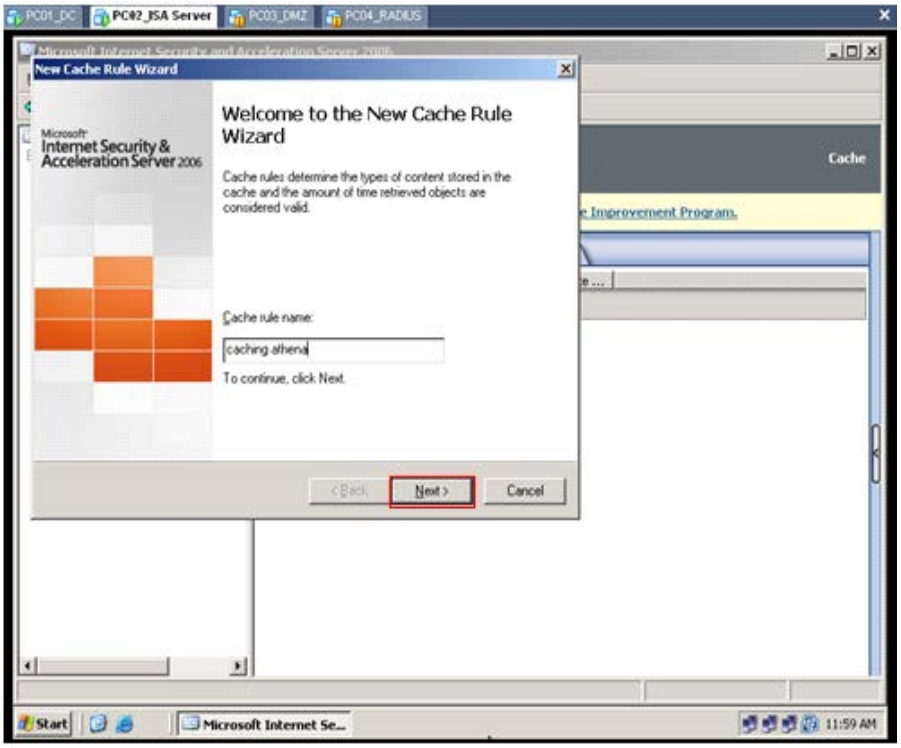


Chọn option save the change and restart the services, sau đó Click OK

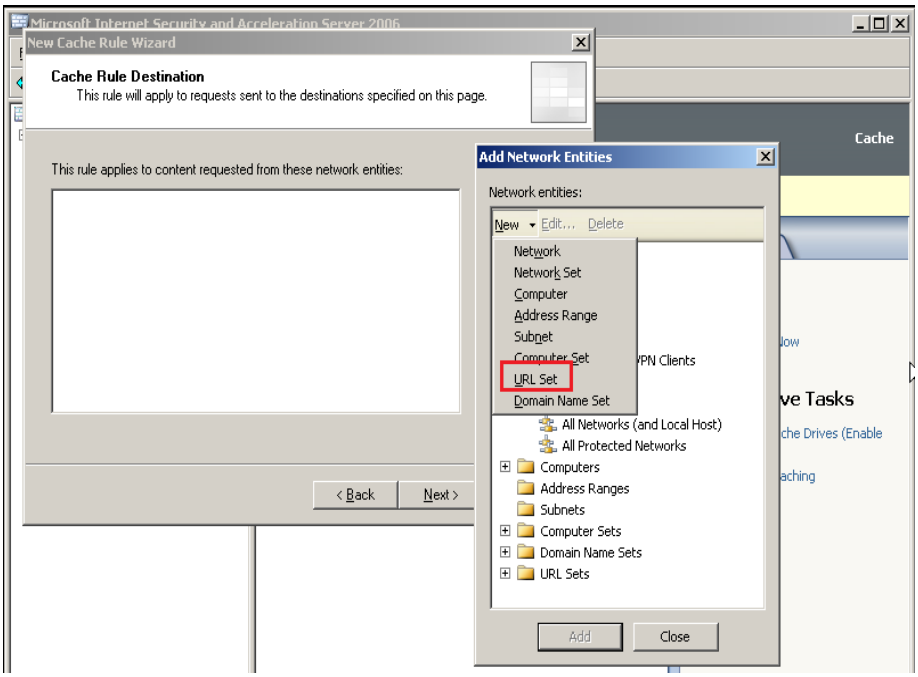
Tạo cache Rule



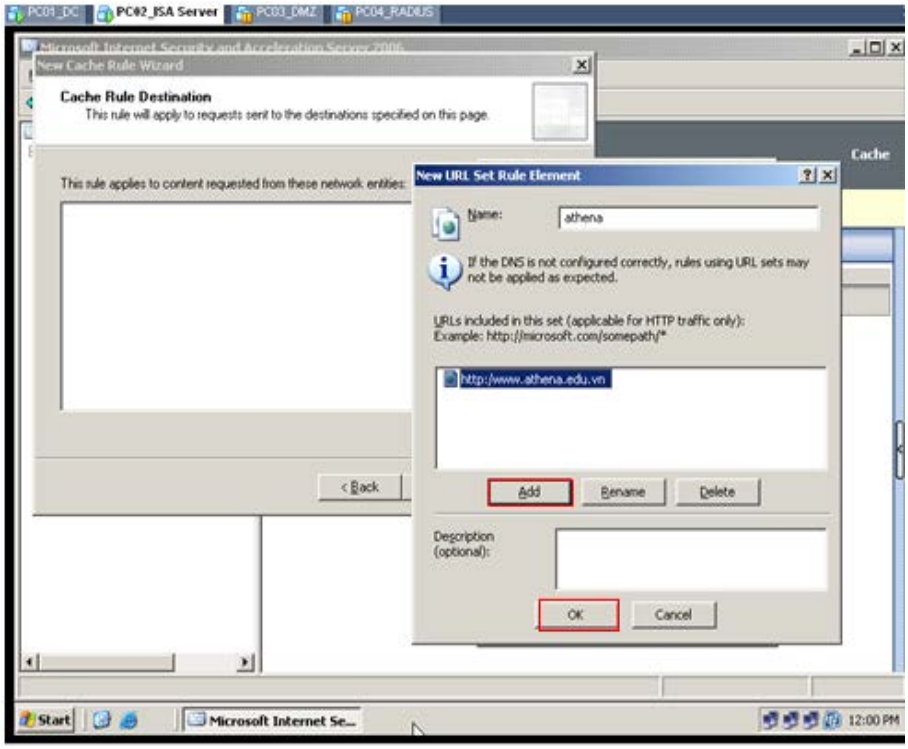
R_Click Cache\New\Cache Rule…



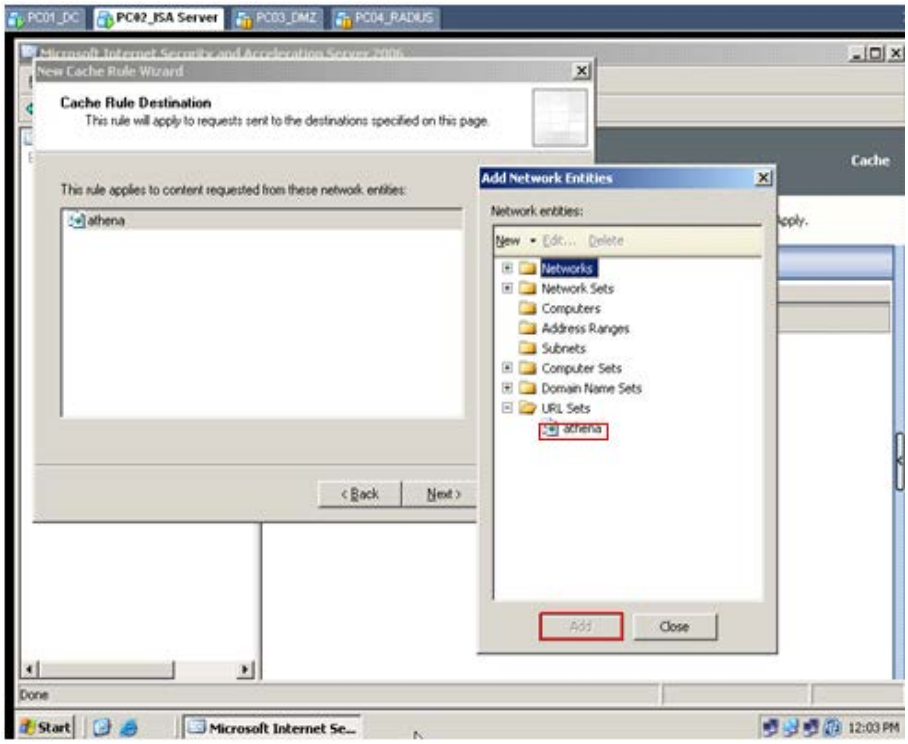
Điền Cache Rule name, sau đó Click Next



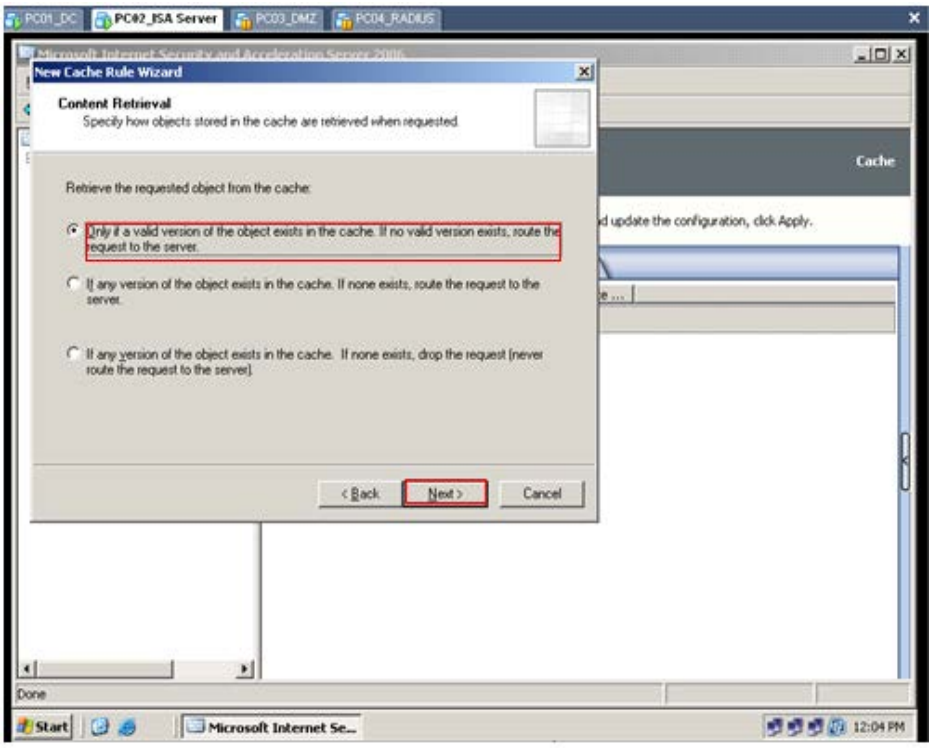
Click Add\New\URL Set



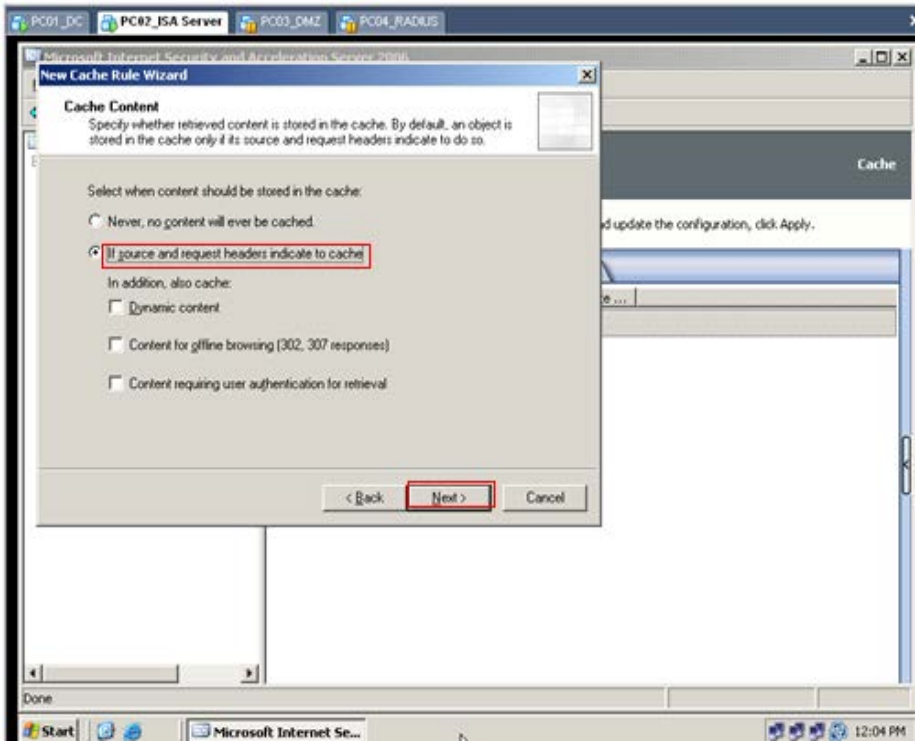
Click Add điền đường dẫn Web Site Athena, sau đó Click OK



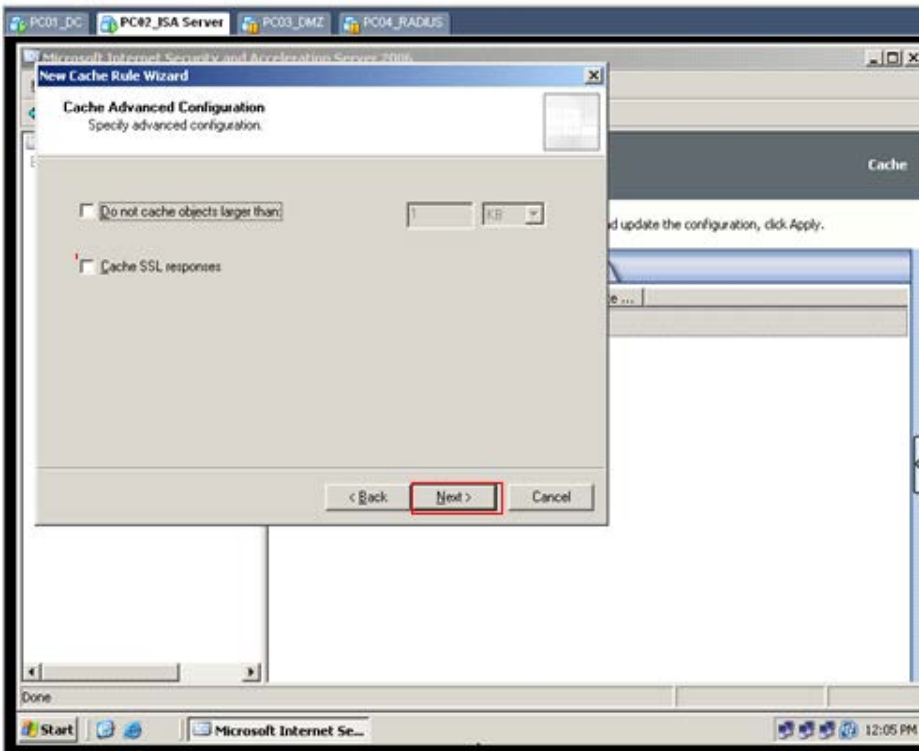
Chọn Web Site, sau đó Click Add



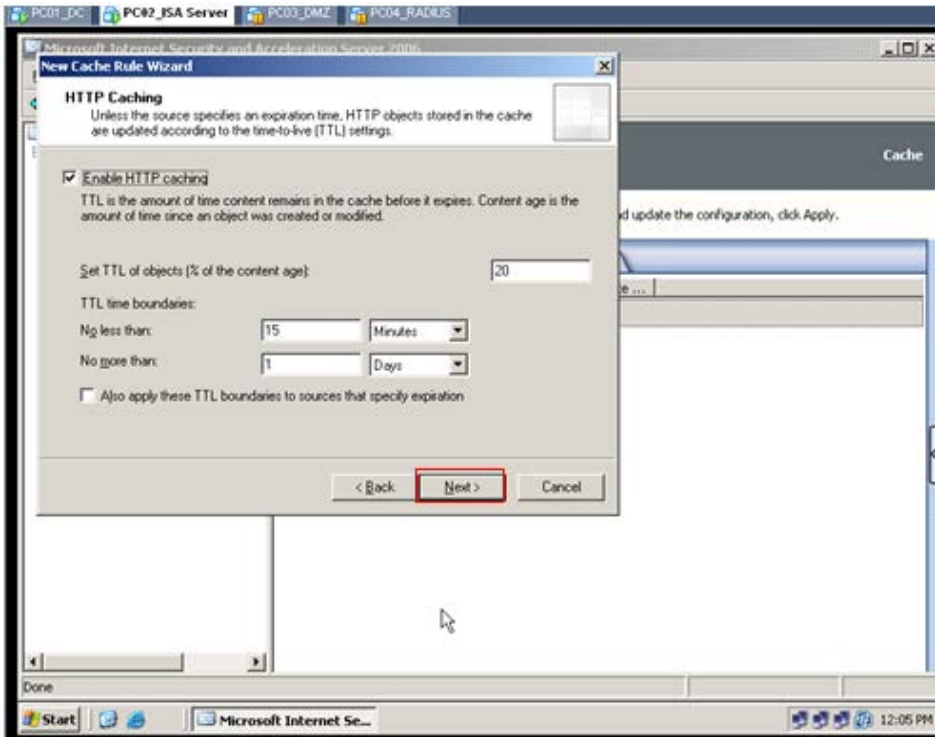
Giữ nguyên mặc định, sau đó Click Next



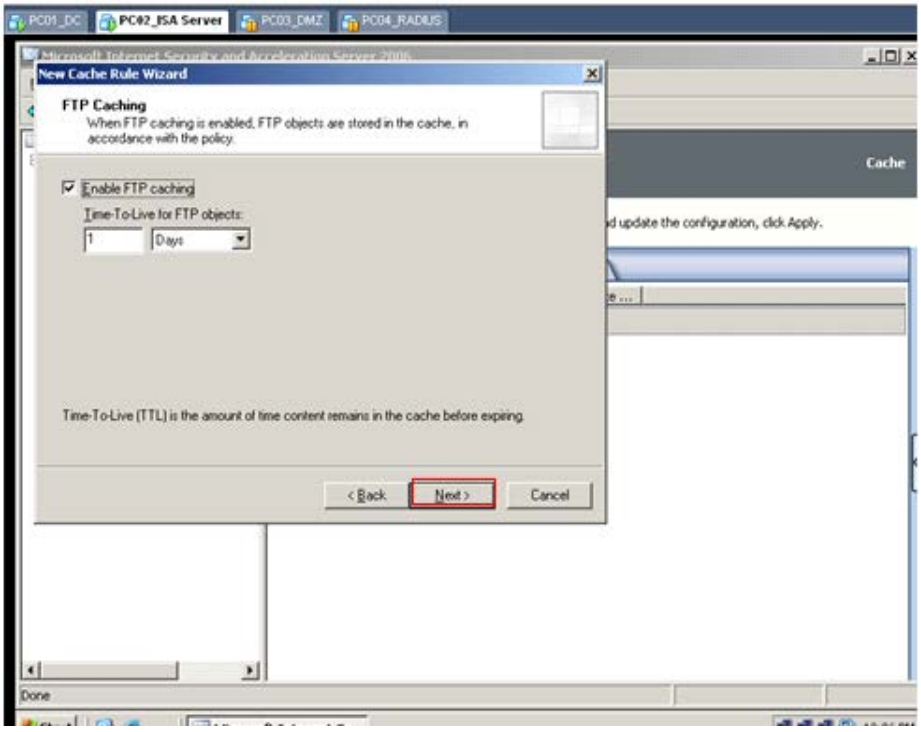
Giữ nguyên mặc định , sau đó Click Next



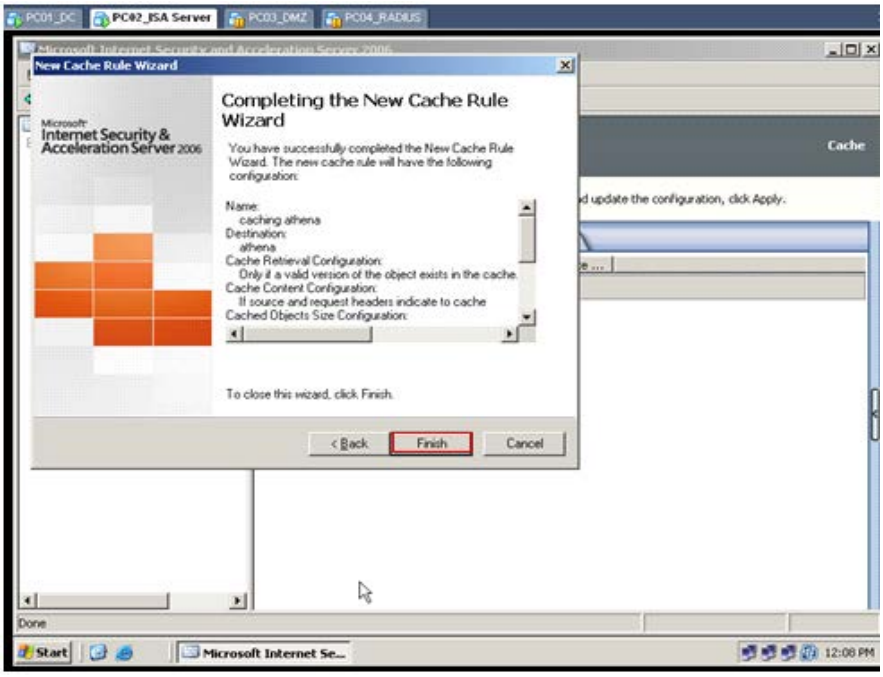
Giữ nguyên mặc định, sau đó Click Next



Để mặc định, sau đó Click OK

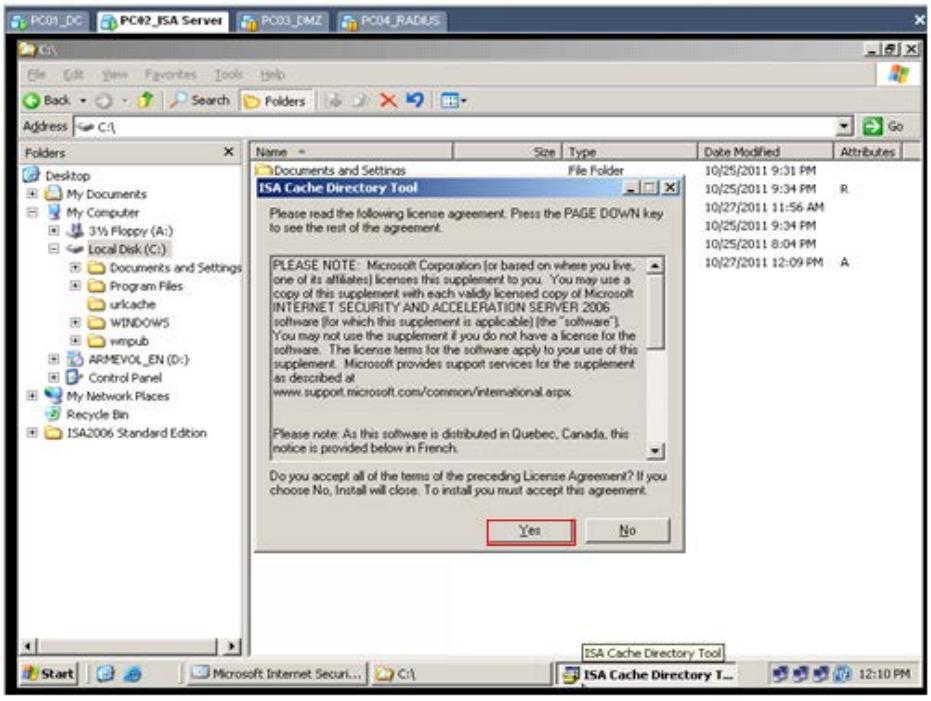


Giữ nguyên mặc định, sau đó Click Next

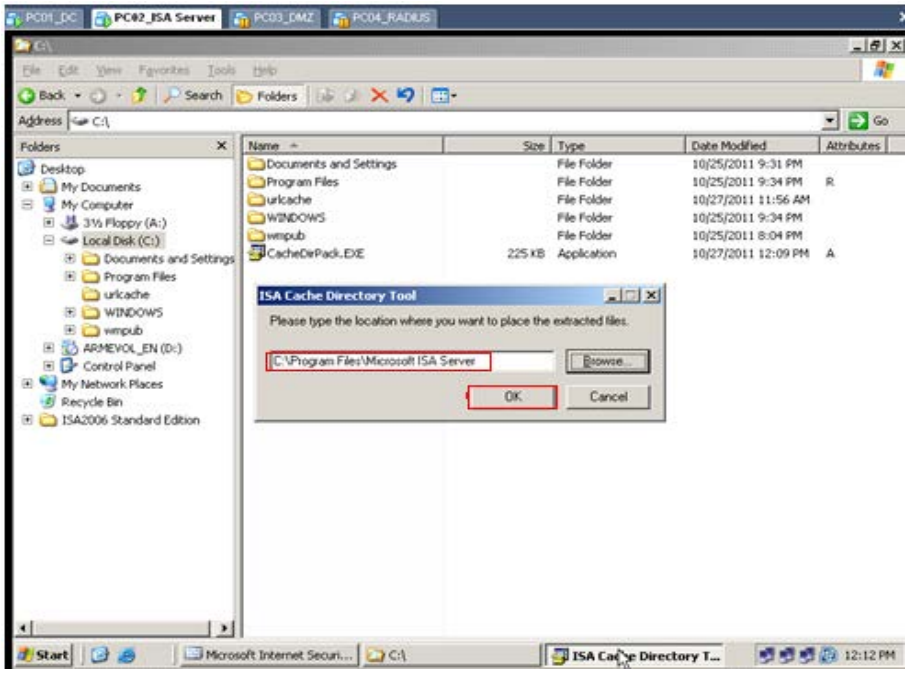


Click Finish để hoàn tất

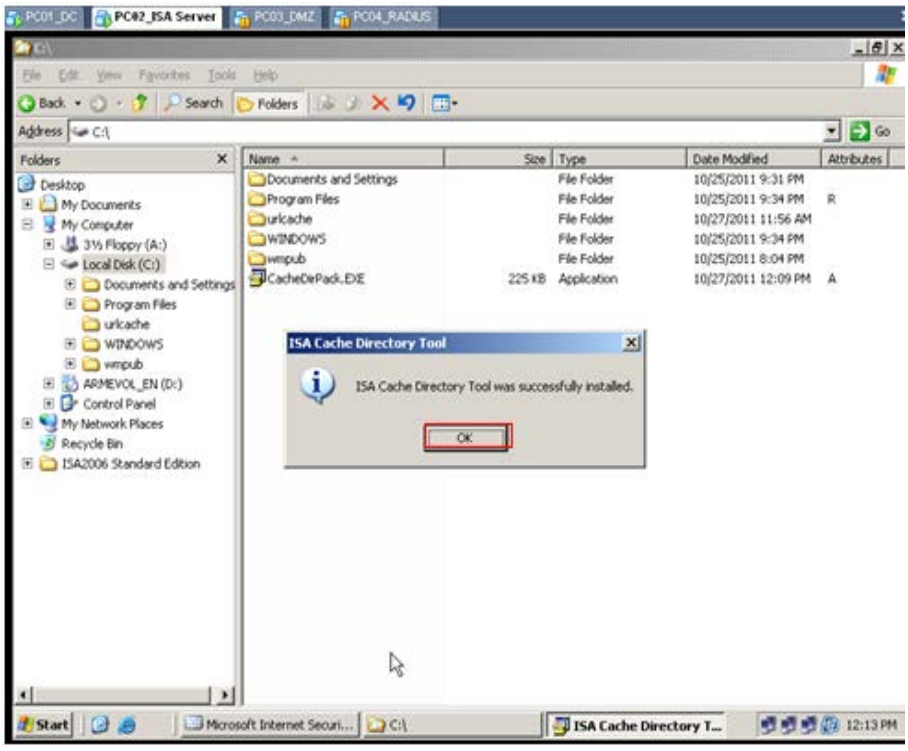
Cài đặt ISA Cache Directory Tool



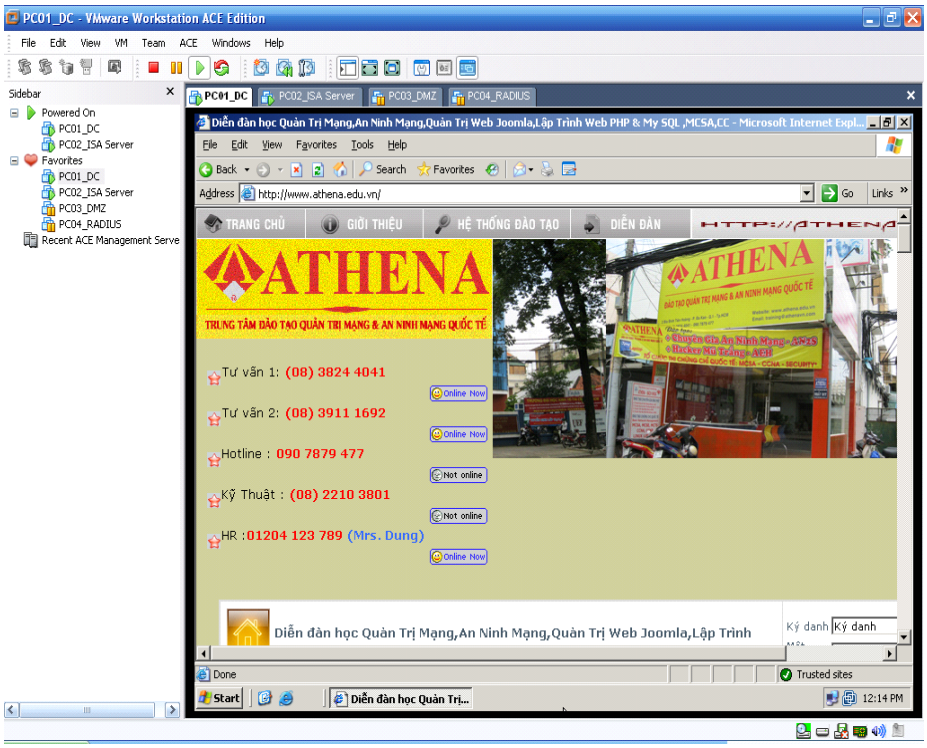
Click nên phần mềm, sau đó Click Yes



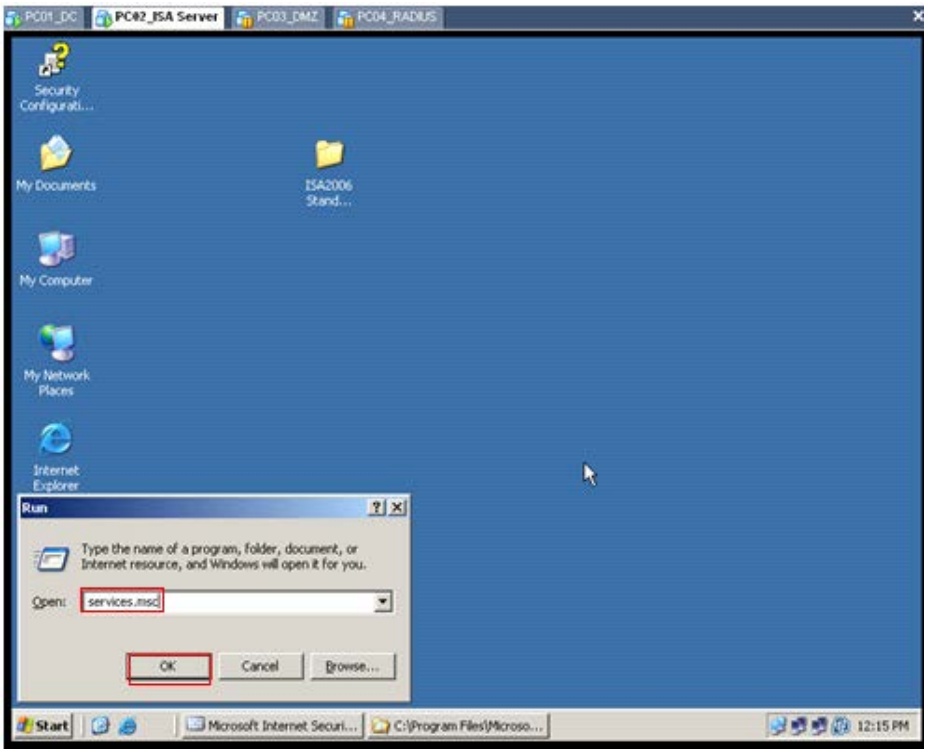
Chọn đường dẫn như trên, sau đó Click OK



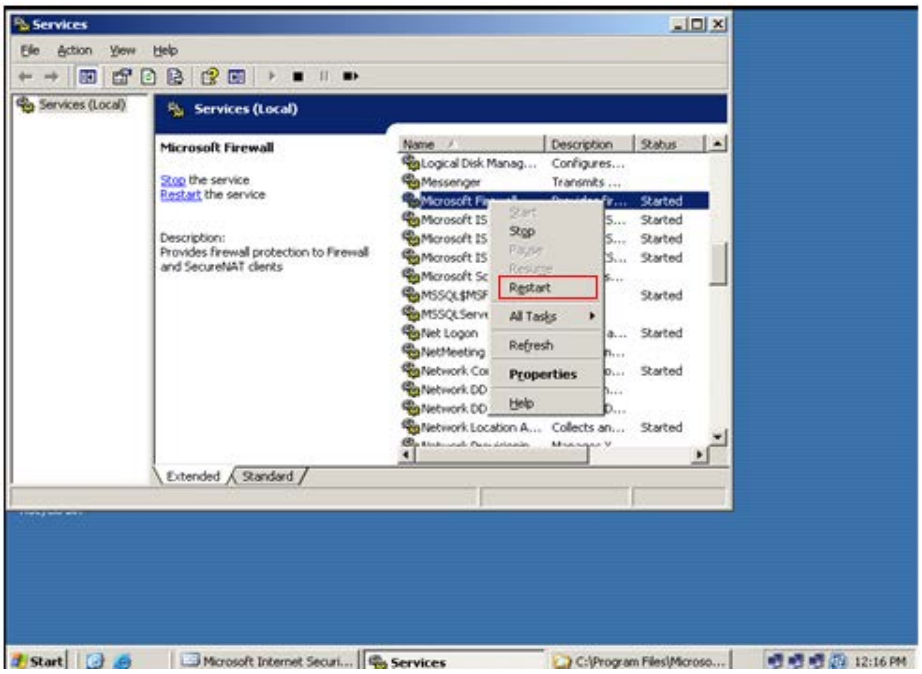
Click OK



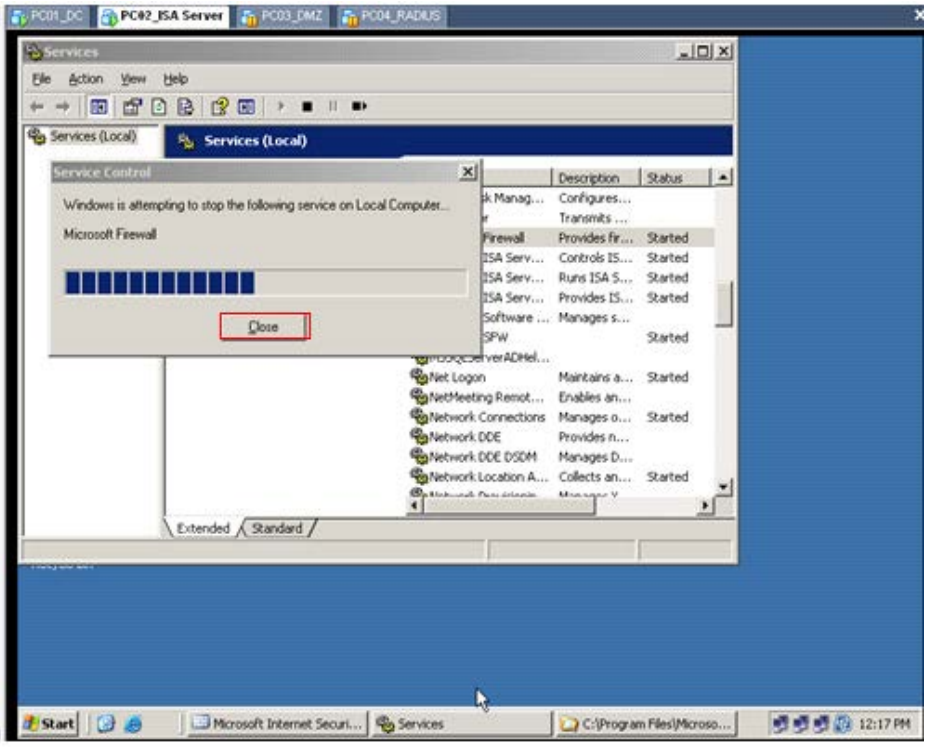
Vào máy DC gõ Trang Web http://www.athena.edu.vn



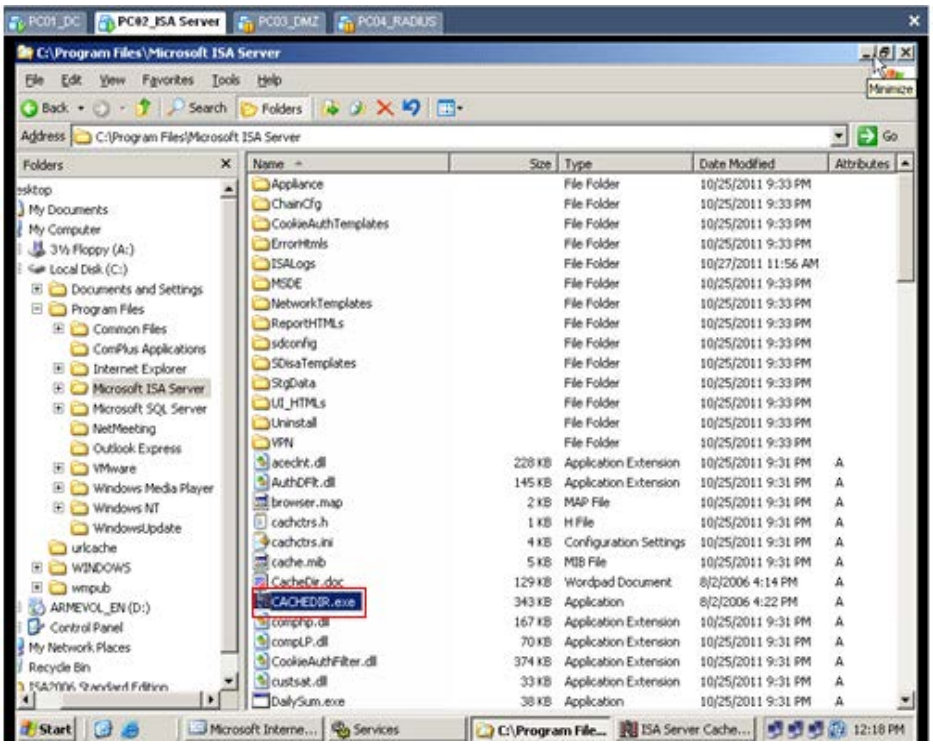
Trên máy ISA vào Start\run\services.msc



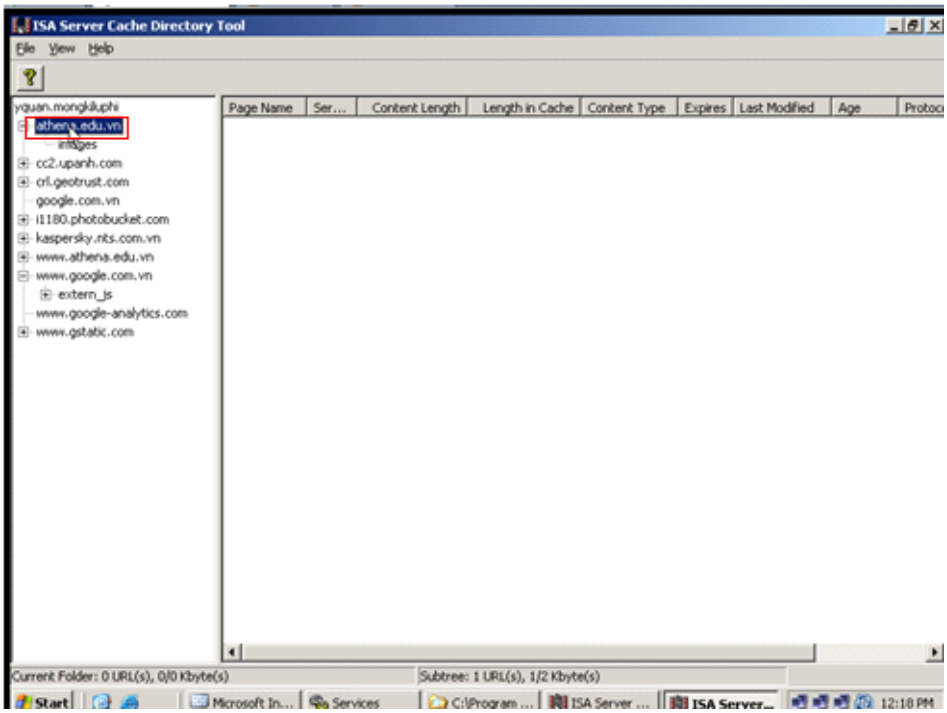
R_Click Microsoft Firewall Click restart



Quá trình restart bắt đầu

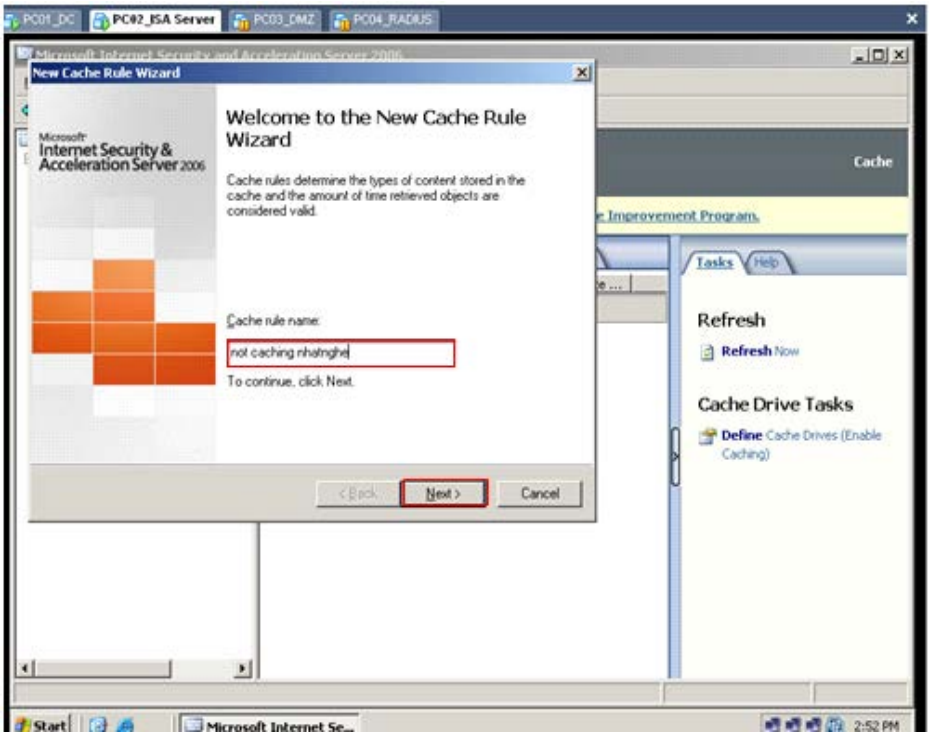


Vào C:\\Program Files\Microsoft ISA Server, sau đó Click CACHEDER.exe

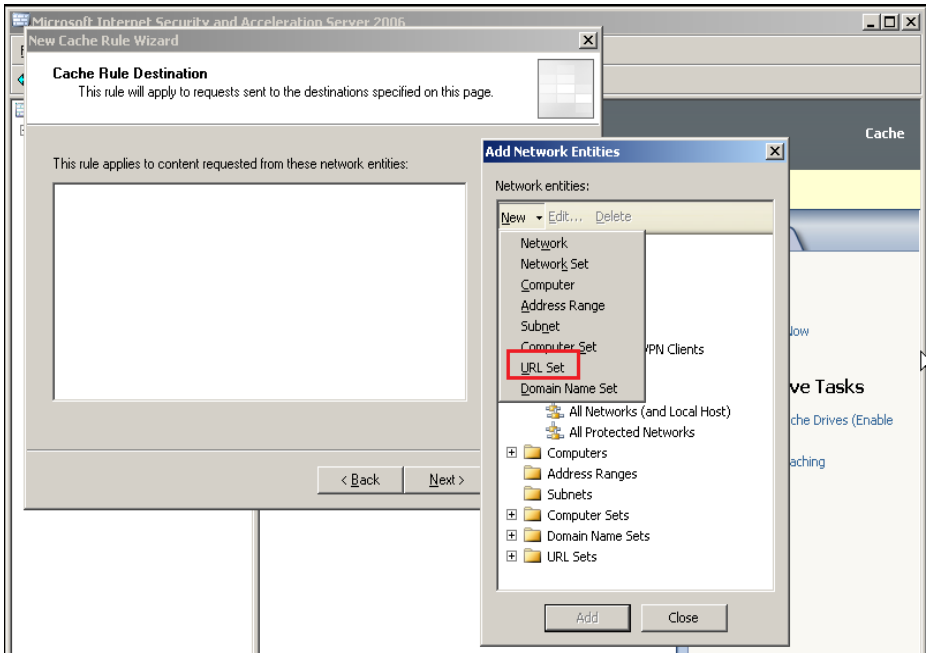


Ta đã Caching được trang Web Athena

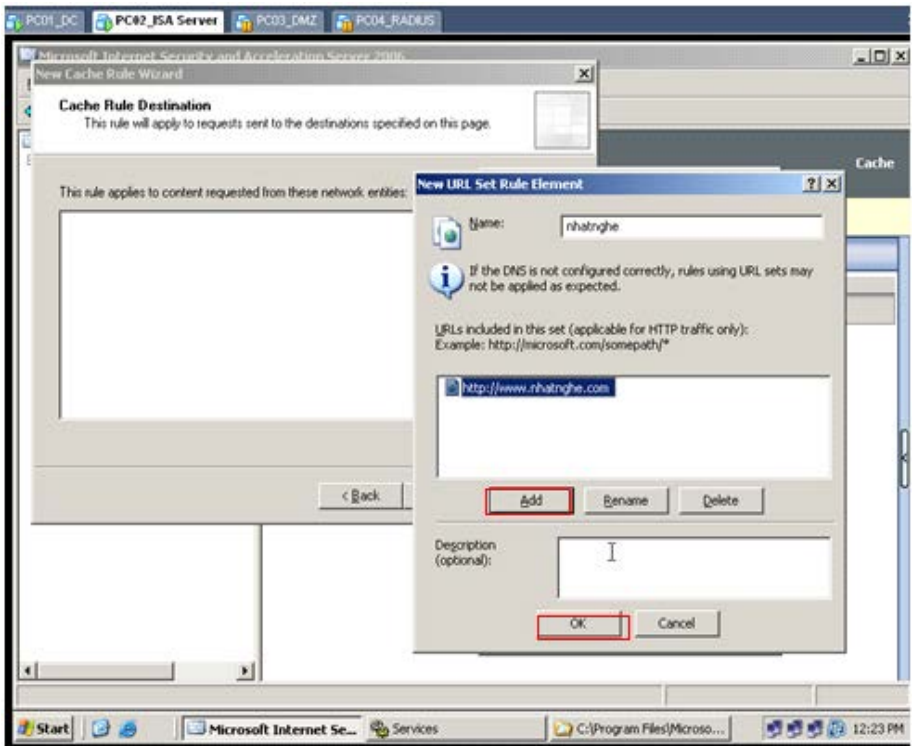
Cấm Cache trang Web nhatnghe



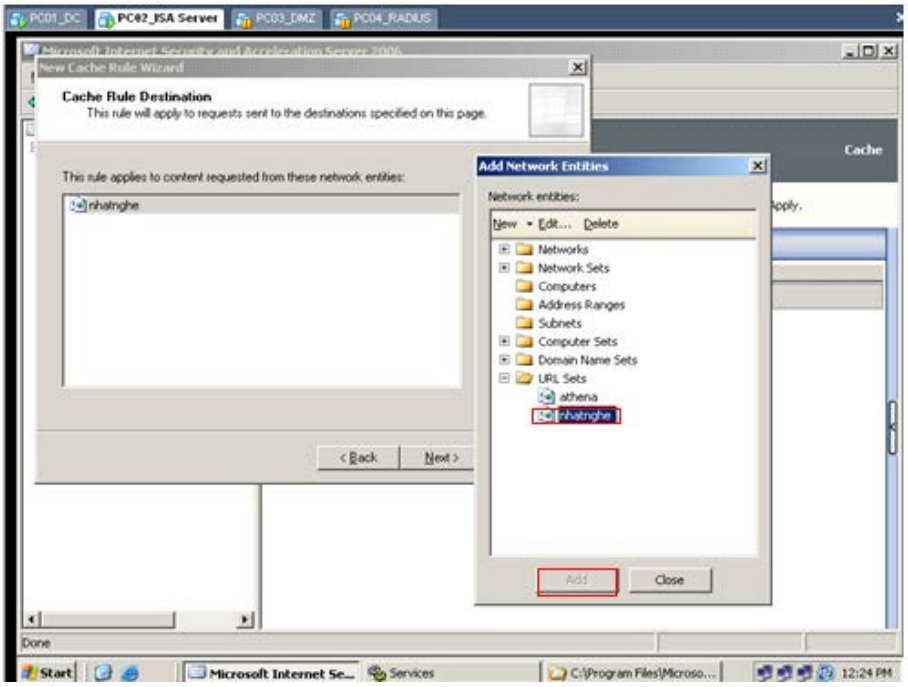
Điền Cache Rule name, sau đó Click Next



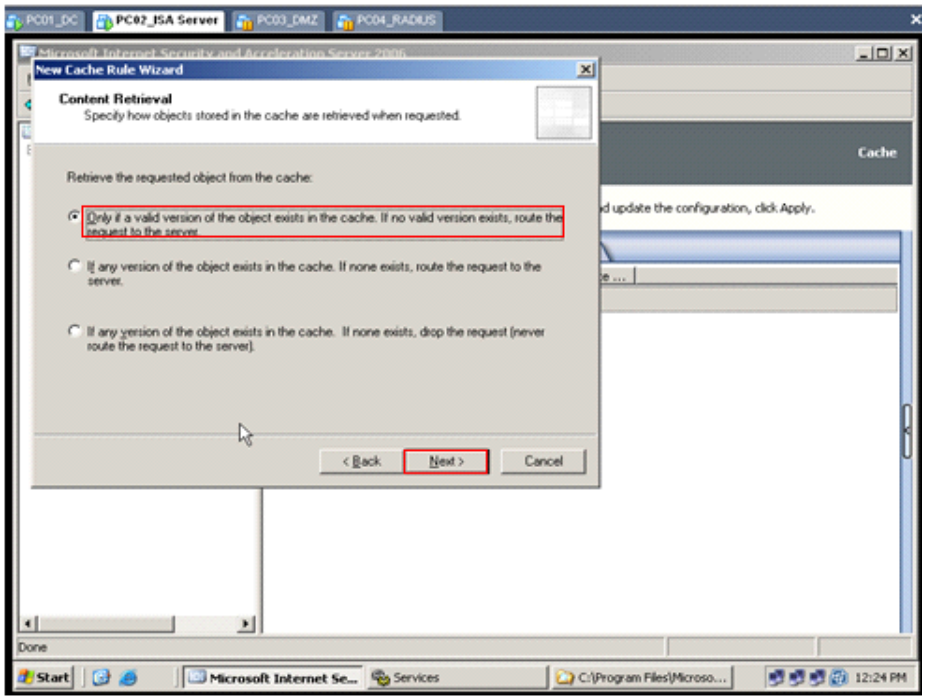
Click Add\New\URL Set



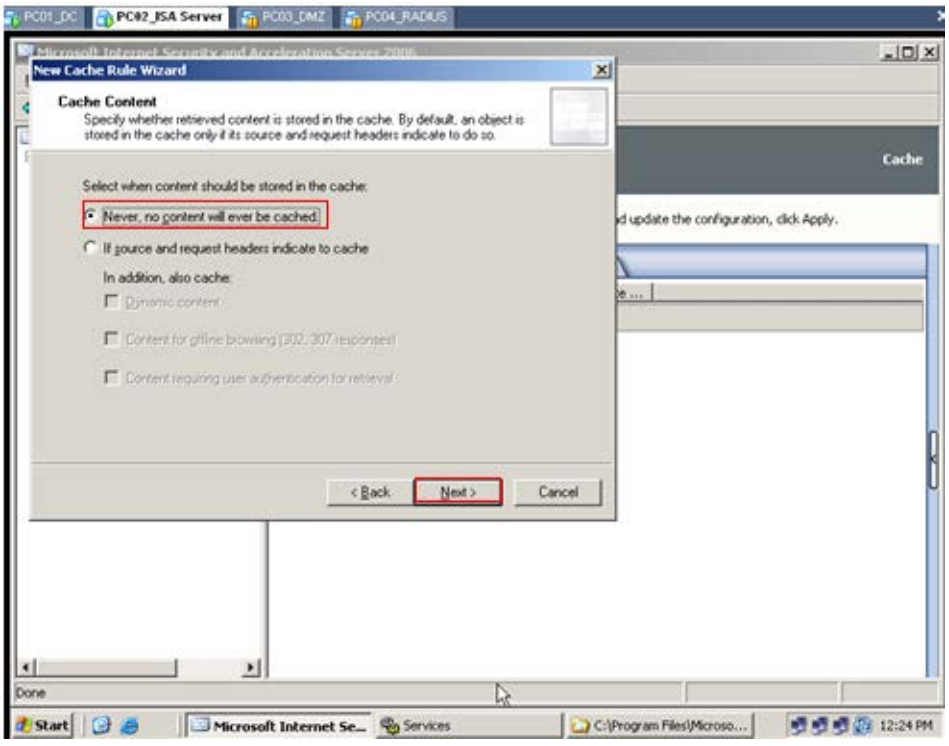
Click Add điền địa chỉ trang Web http://www.nhatnghe.com, sau đó Click OK



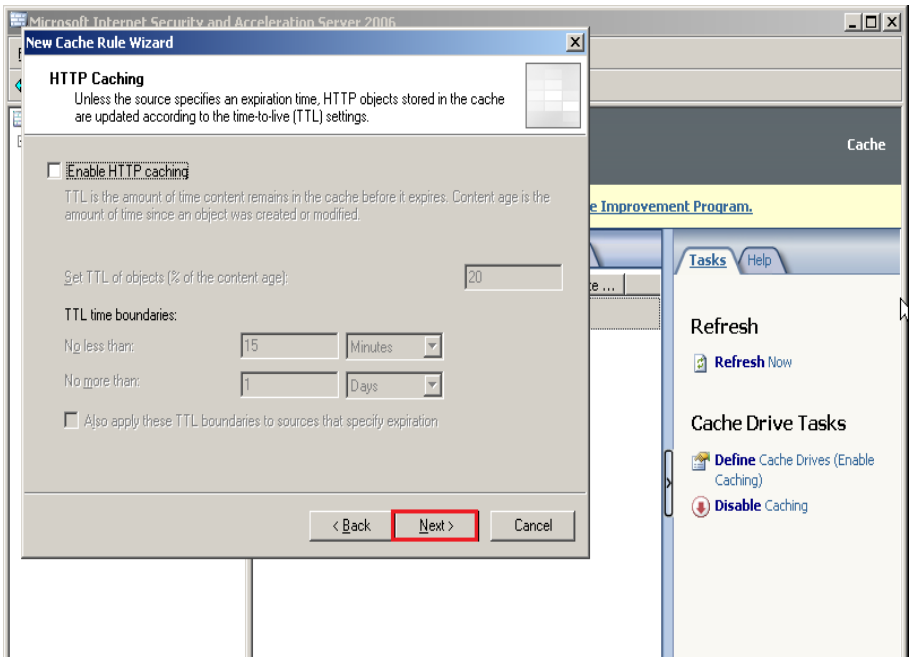
Click nhatnghe, sau đó Click Add



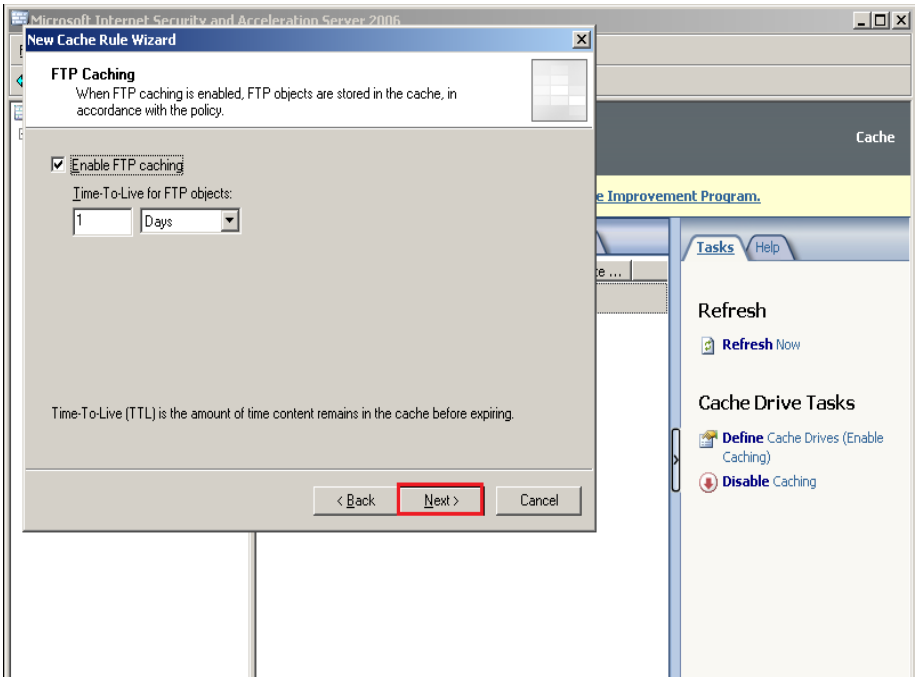
Giữ nguyên mặc định, sau đó Click Next



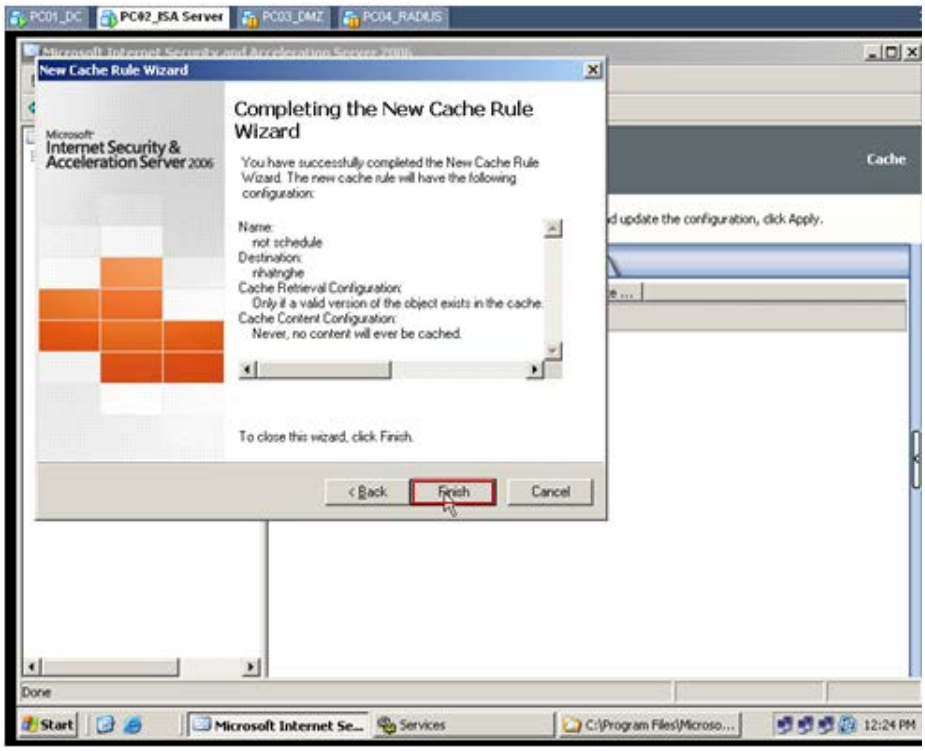
Giữ nguyên mặc định, sau đó Click Next



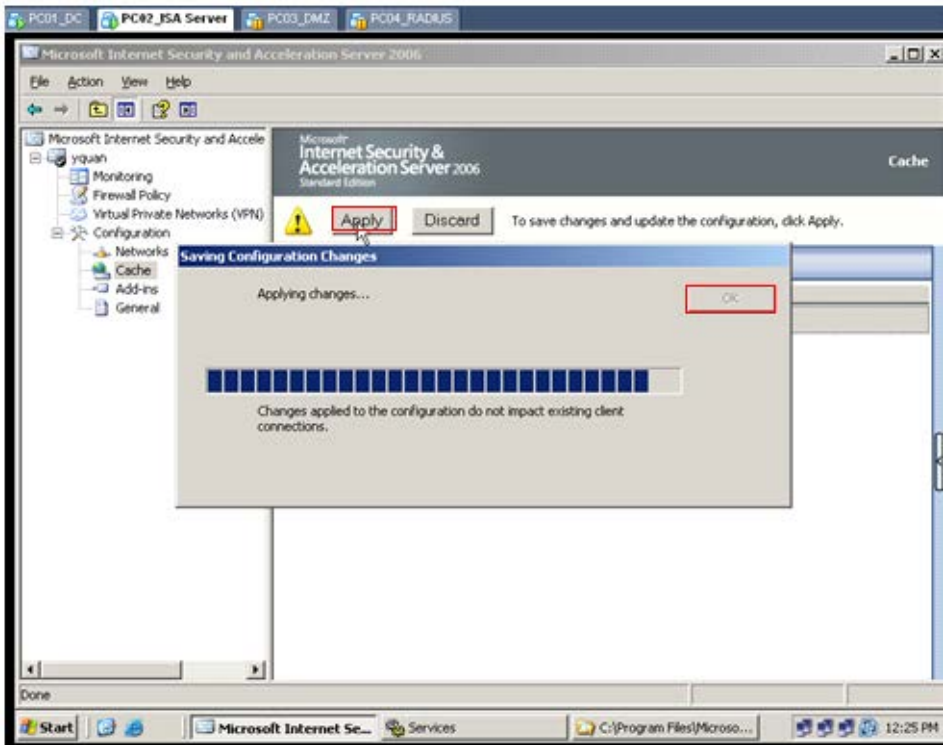
Gỡ bỏ Enable HTTP caching



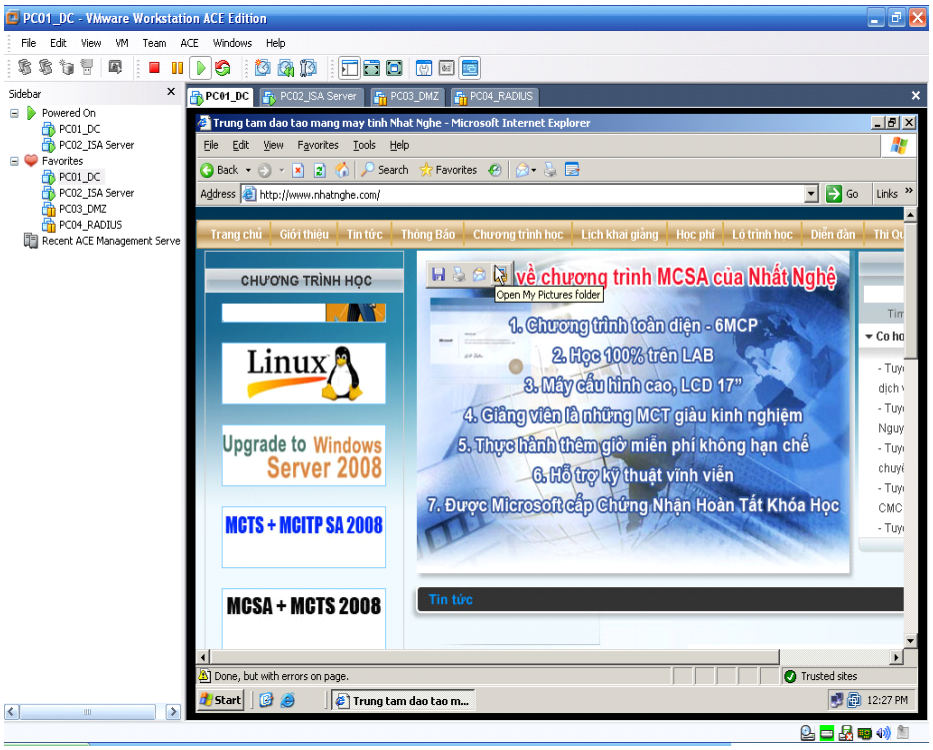
Giữ nguyên mặc định, sau đó Click Next



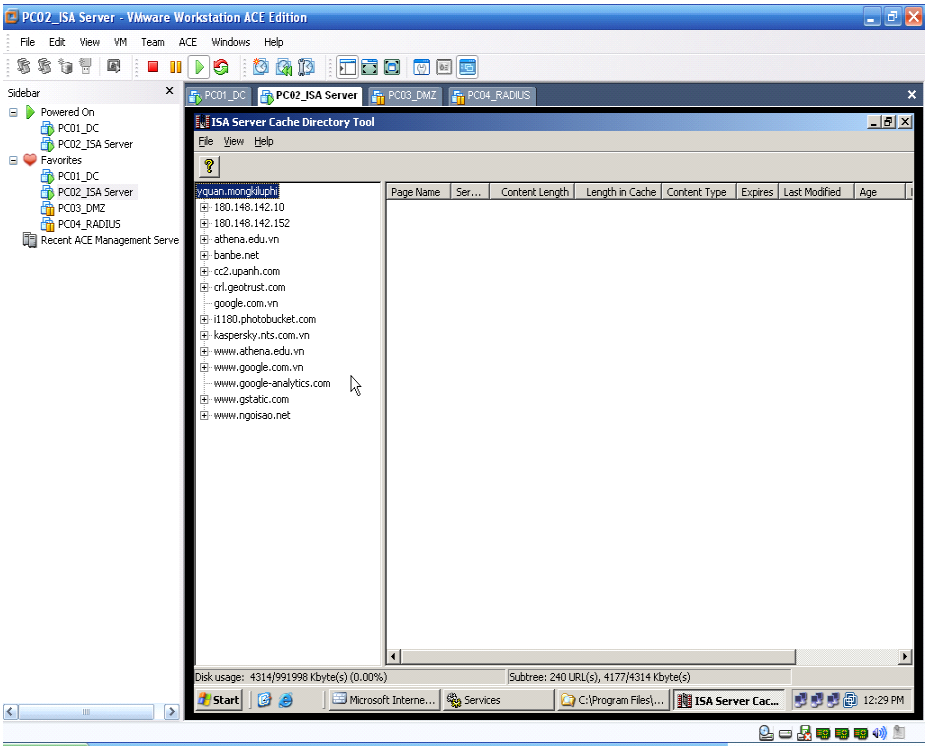
Click Finish để hoàn tất



Click Apply, sau đó Click OK

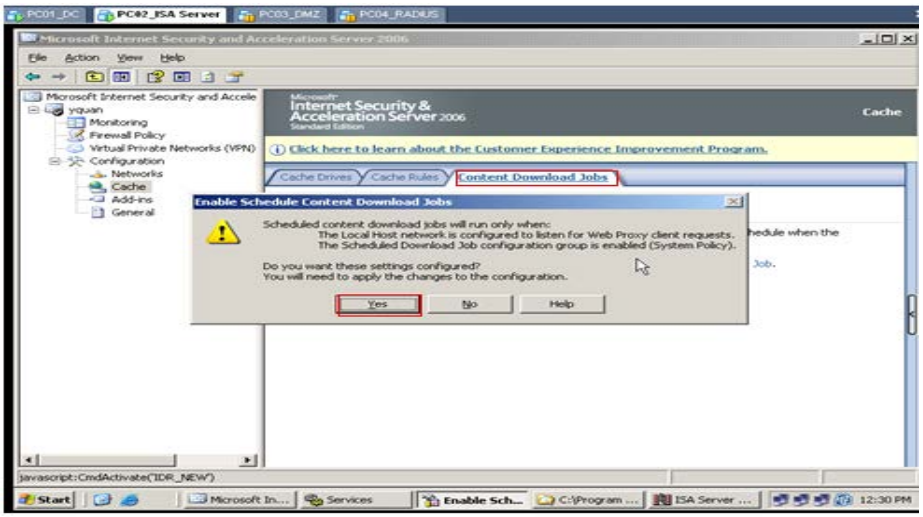


Vào máy DC gõ địa chỉ tràn Web http://www.nhatnghe.com

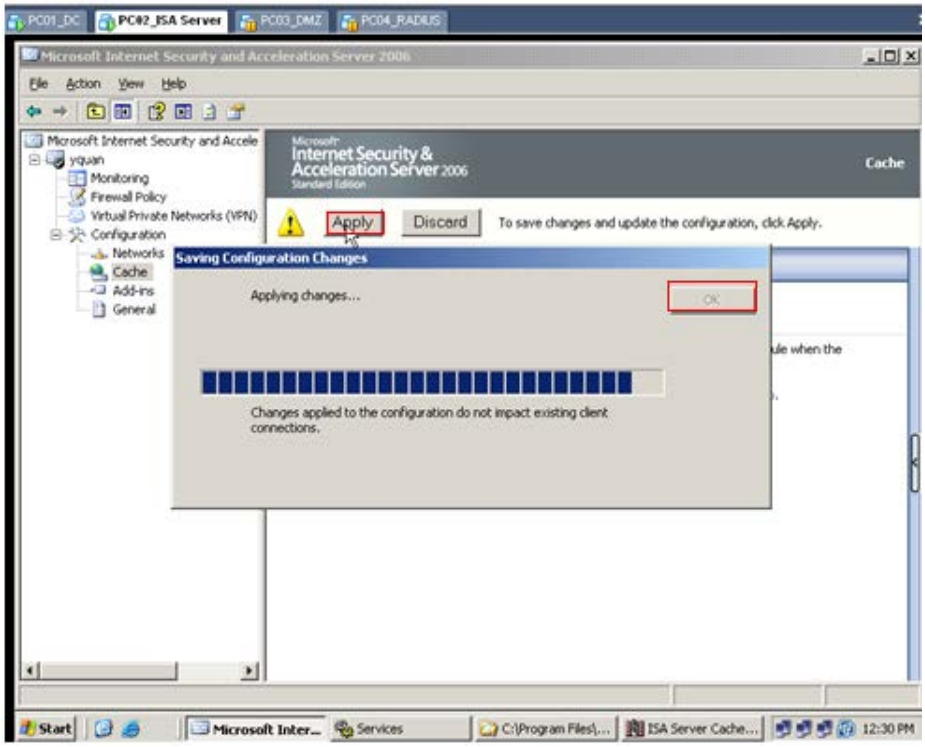


Ta sẽ không thấy trang Web http://www.nhatnghe.com hiện thị trong danh sách

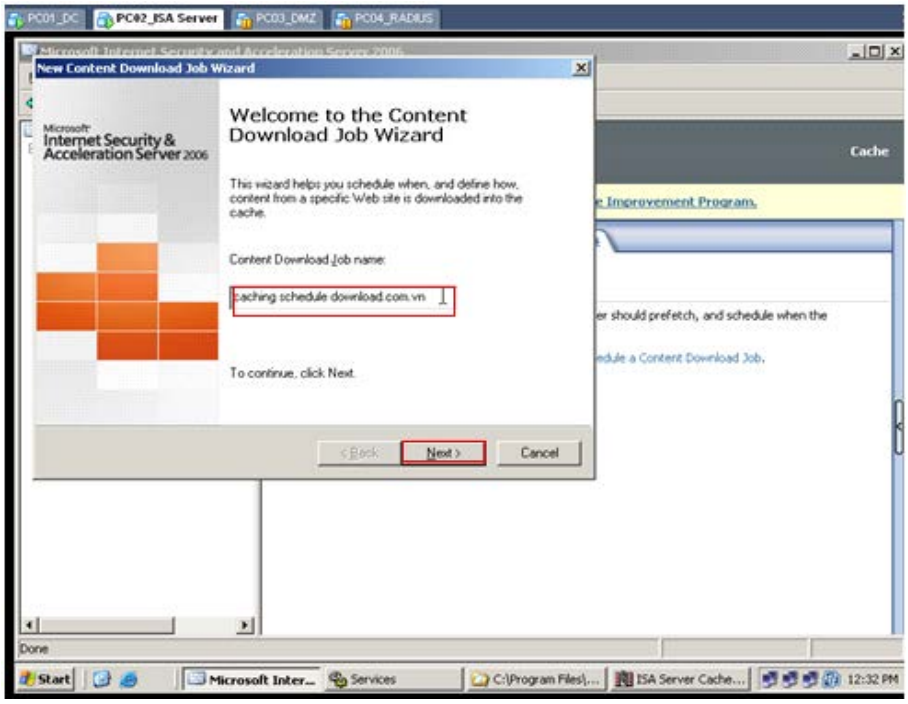
Đến đây ta đã cấu hình hoàn tất cho ISA Server Cache thụ động tất cả các trang Web, nghĩa là với những trang Web có nội dung không được lưu trữ trong Cache của ISA sẽ phải tốn công tải nguyên cả trang về.Như vậy với một số trang Web mà ta muốn ISA tự động Cache vào thời điểm nhất định nào đó thì ta phải tạo một Job cho ISA cập nhật chủ động trang này. Ta làm như sau:



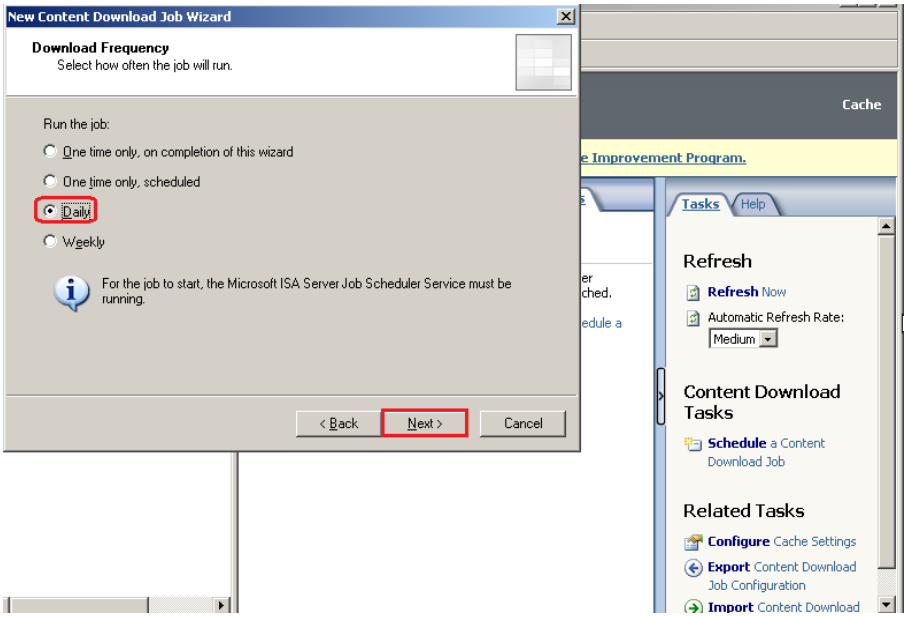
Vào máy ISA Server chọn Tab Content Download Jobs trong Cache tiếp tục nhấp chọn Schedule a Content Download Job để Enable tính năng chủ động Cache lên, sau đó Click Yes



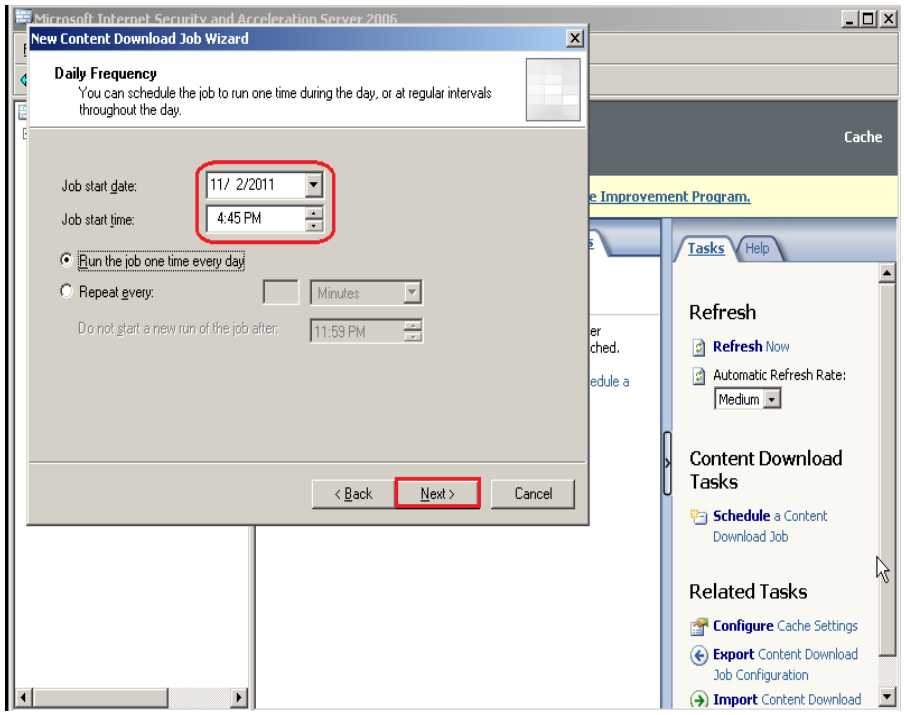
Click Apply



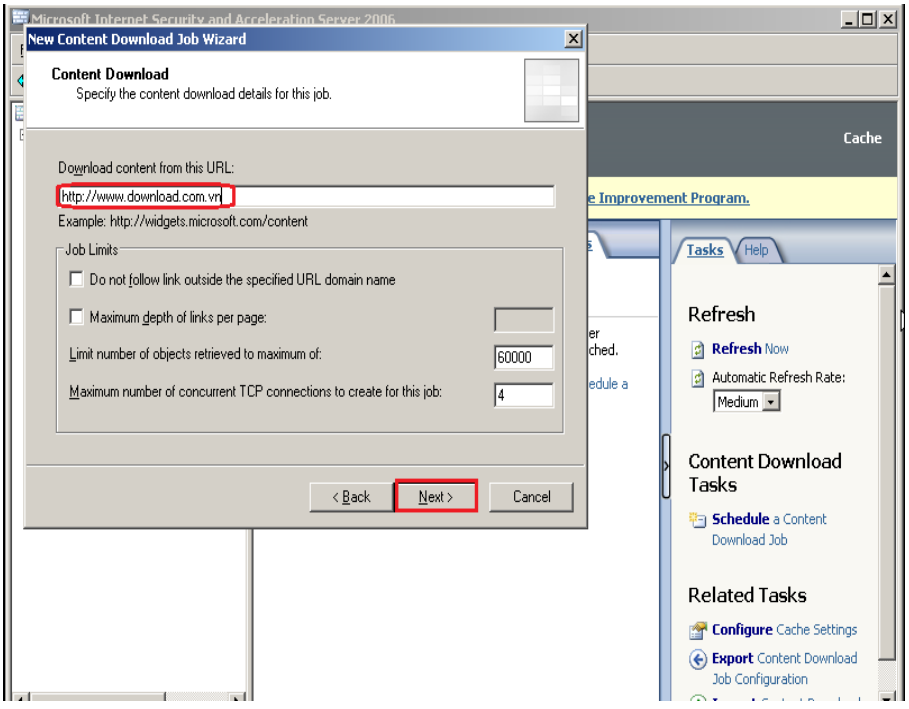
Điền Content Download Job name, sau đó Click Next



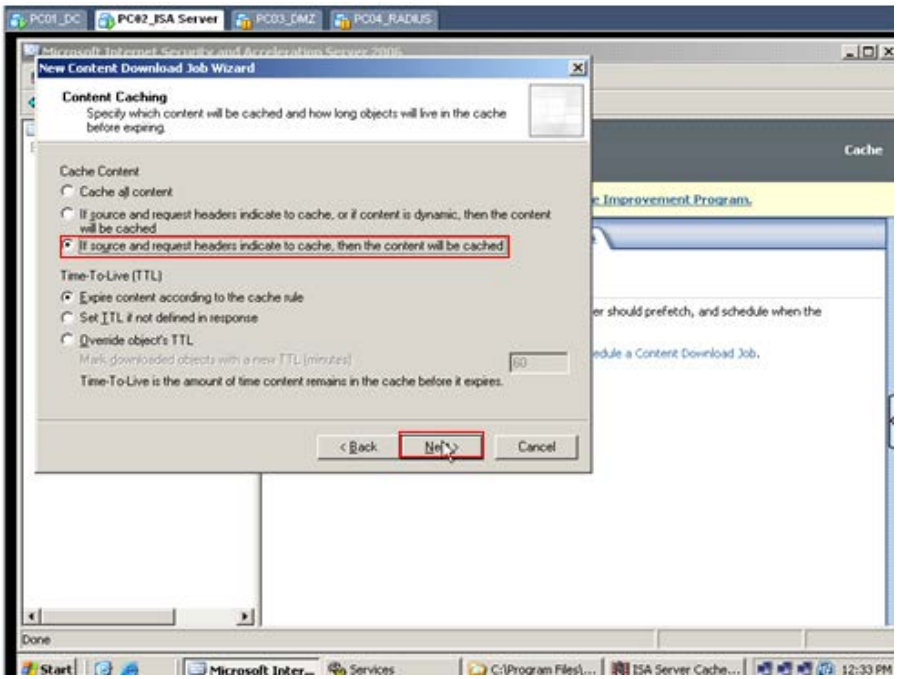
Chọn Daily để thực hiện Cache mỗi ngày, sau đó Click Next



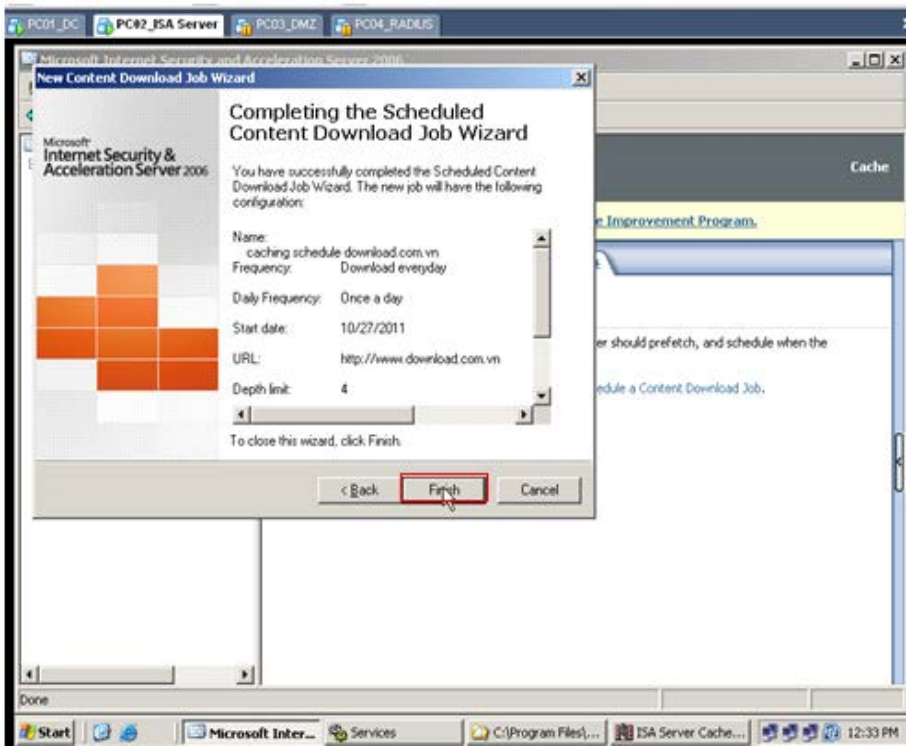
Chỉ định giờ thực hiện Cache chủ động cho ISA trong Daily Frequency, sau đó Click Next



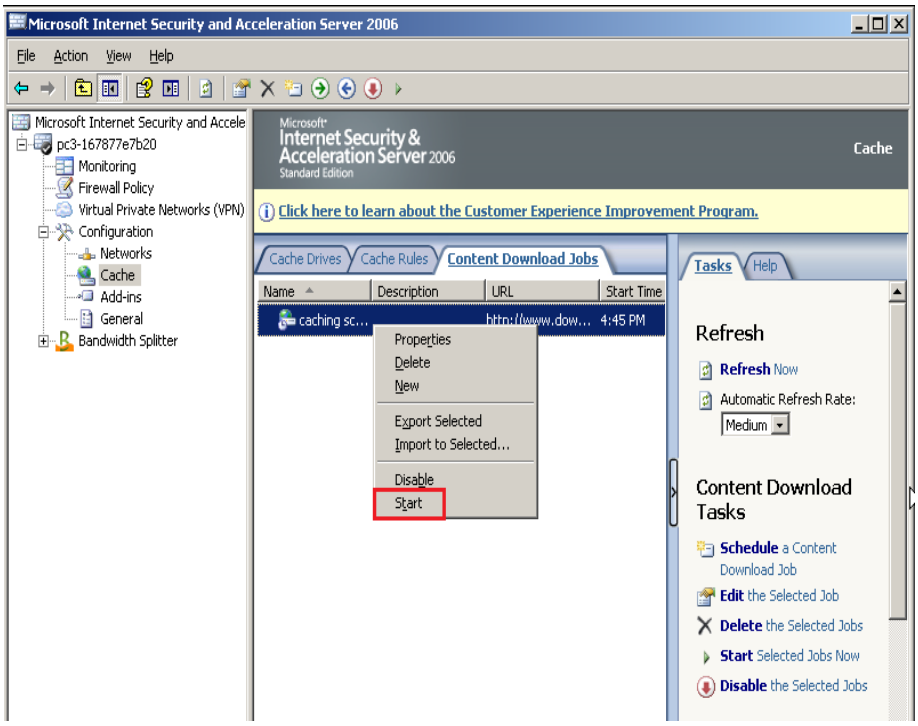
Điền địa chỉ trang Web http://www.download.com.vn, sau đó click Next



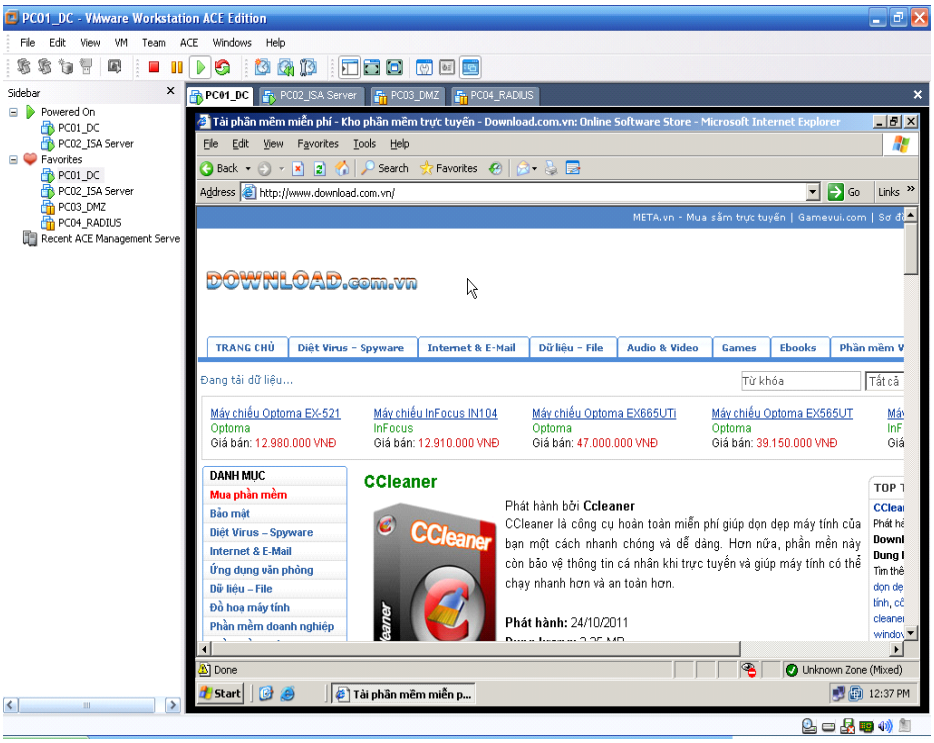
Giữ nguyên mặc định, sau đó Click Next



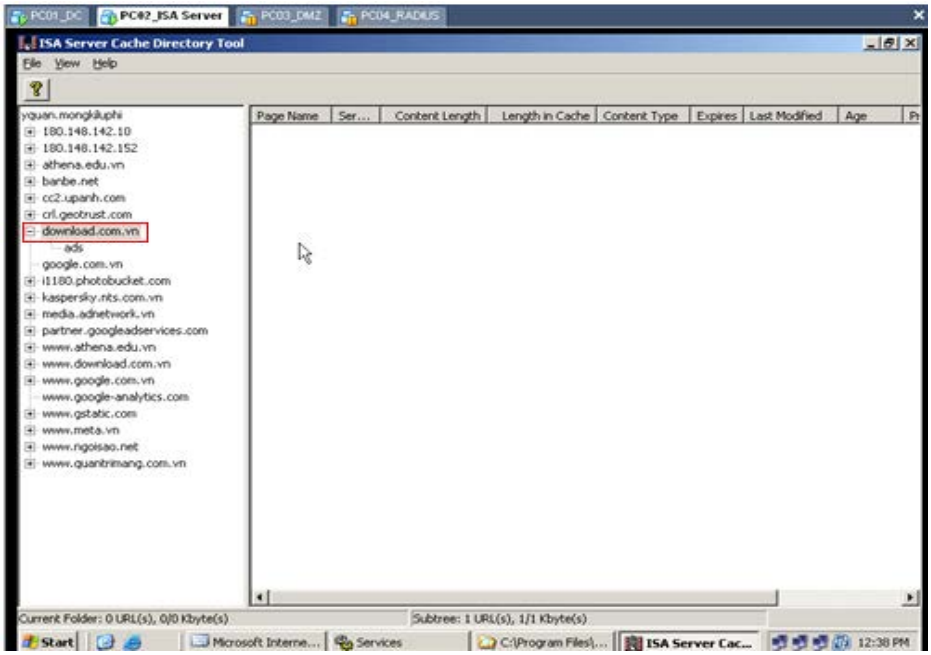
Click Finish để hoàn tất



Sau khi hoàn thanh R_Click Content Download Jonbs vừa xét, sau đó Click Start



Vào máy DC điền địa chỉ trang Web http://www.download.com.vn



Ta thấy http://www.download.com.vn đã có trong danh sách

11. Quản lý băng thông với Bandwidth Splitter

Đây là một chương trình support với ISA 2004 và 2006. Dùng rất hiệu quả trong việc giới hạn băng thông và hạn ngạch dung lượng truy cập Internet.

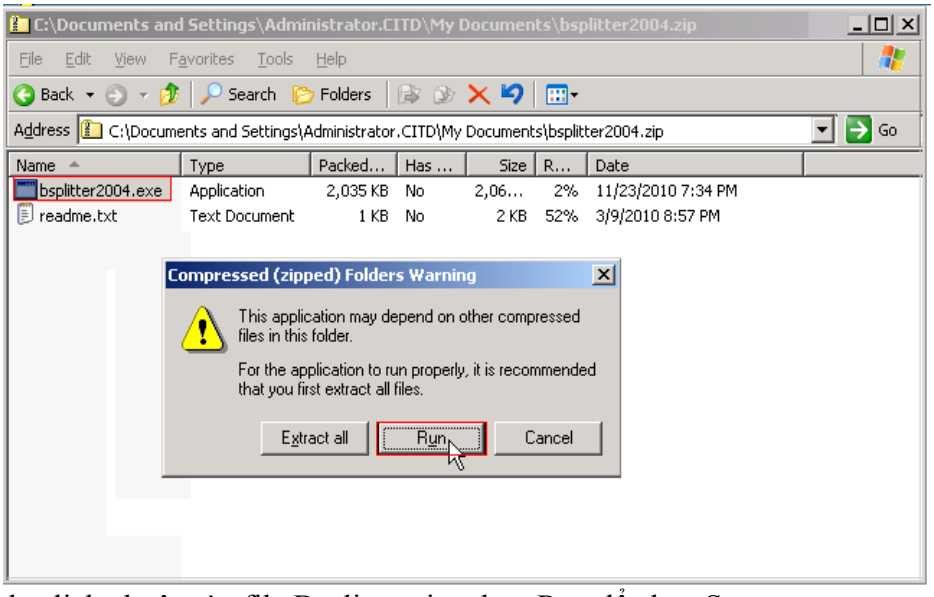
Các tính năng chính của Bandwidth Splitter là:

- Hạn chế của băng thông kết nối Internet được sử dụng bởi cá nhân người dùng và máy chủ, cũng như các nhóm người sử dụng host (hình thức lưu thông, throttling)
- Thiết lập hạn ngạch cho phép Internet tối đa giao thông sử dụng (đơn vị MB) trong một thời gian thiết lập thời gian (một ngày, một tuần hay một tháng) cho người dùng cá nhân và máy chủ, cũng như các nhóm người dùng và máy chủ
- Real-time giám sát của tất cả người dùng và các kết nối của họ thông qua ISA Server bởi người quản trị, bao gồm cả băng thông sử dụng bởi người dùng cá nhân và kết nối

Với Bandwidth Splitter bạn sẽ nhận được những điều sau đây lợi ích:

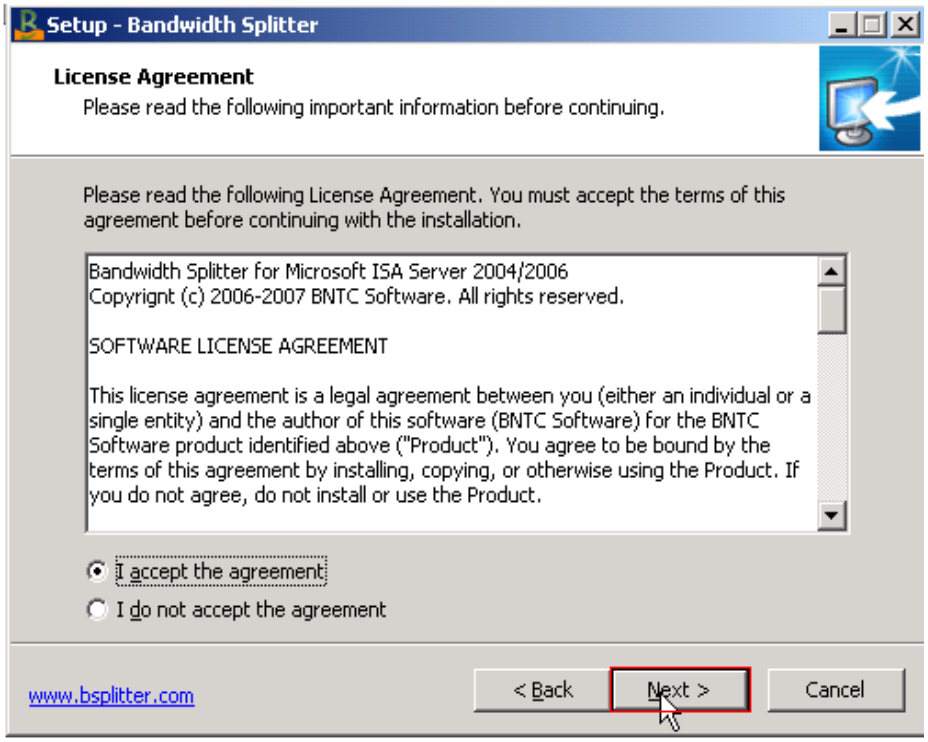
- Khả năng giám sát thời gian thực cho phép quản trị viên kiểm soát có hiệu quả sử dụng giao thông (xem ảnh chụp màn hình)
- Hợp lý phân phối băng thông kênh Internet (Bạn thiết lập các quy tắc)
- Giảm chi phí Internet vì giới hạn không ưu tiên giao thông (trao đổi peer-to-peer, tải dụng lượng, vv)
- Thoải - mái làm việc đối người sử dụng quan trọng
- Giới hạn lưu lượng sử dụng của người sử dụng lãng phí
- Tiết kiệm thời gian làm việc của người sử dụng vì được đảm bảo hơn phân bổ băng thông.
- Người dùng có thể theo dõi hoạt động internet của họ trong thời gian thực bằng cách sử dụng tiện ích đặc biệt (xem ảnh chụp màn hình).
- Tiết kiệm thời gian của bạn bởi vì bạn không cần phải tạo các báo cáo mỗi khi bạn muốn biết chi tiết về việc sử dụng băng thông. Bạn có thể nhìn thấy nó trong thời gian thực.

11.1. Cài đặt Bandwidth Splitter:

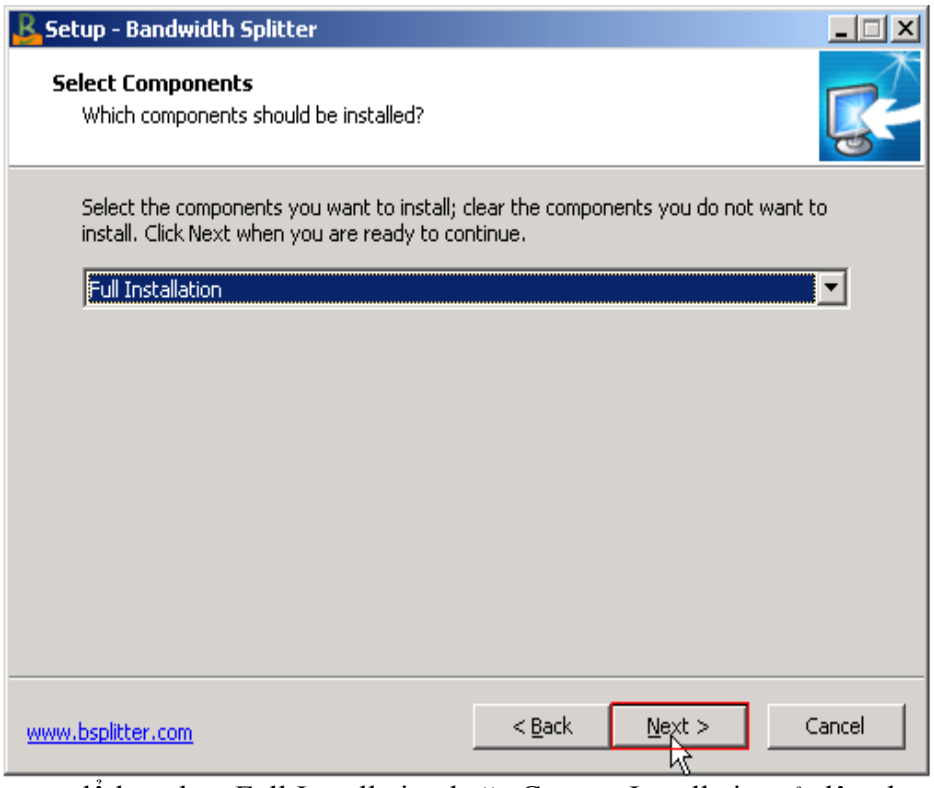


Double click chuột vào file Bsplitter.zip, chọn Run để chạy Setup

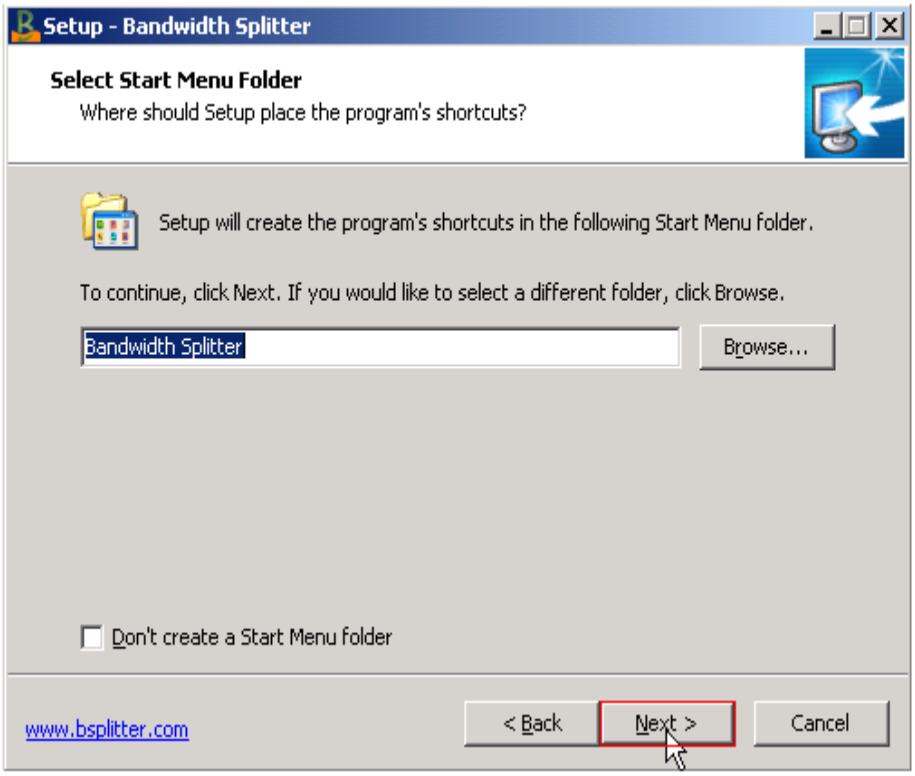
Ta có giao diện như hình bên dưới, click Next để tiếp tục cài đặt



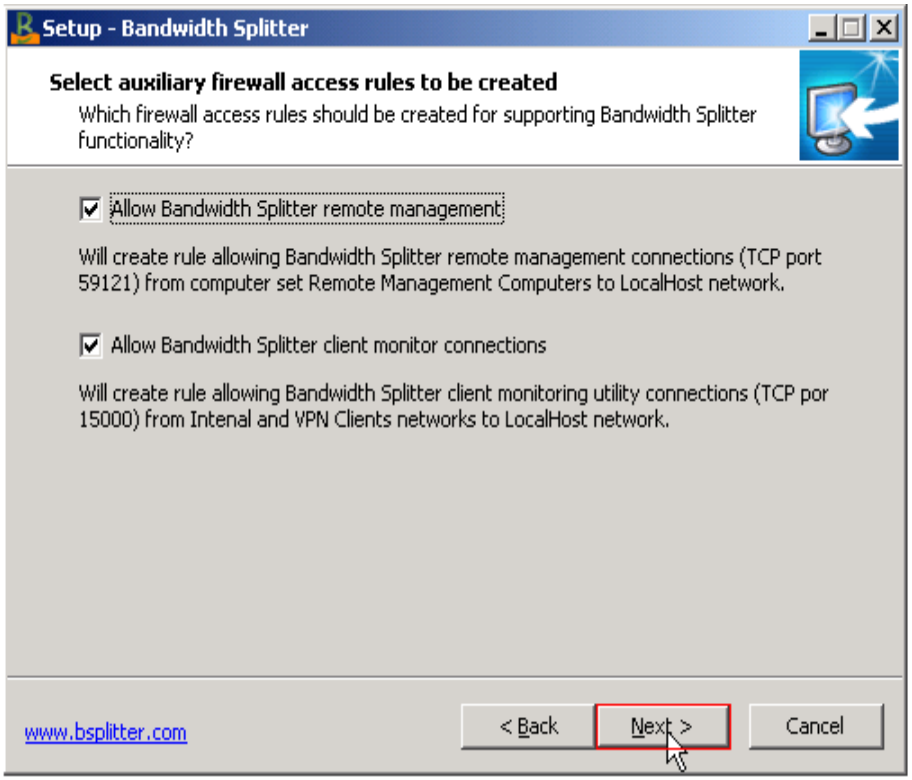
Click chọn Option đồng ý cài đặt, rồi nhấn Next để tiếp tục



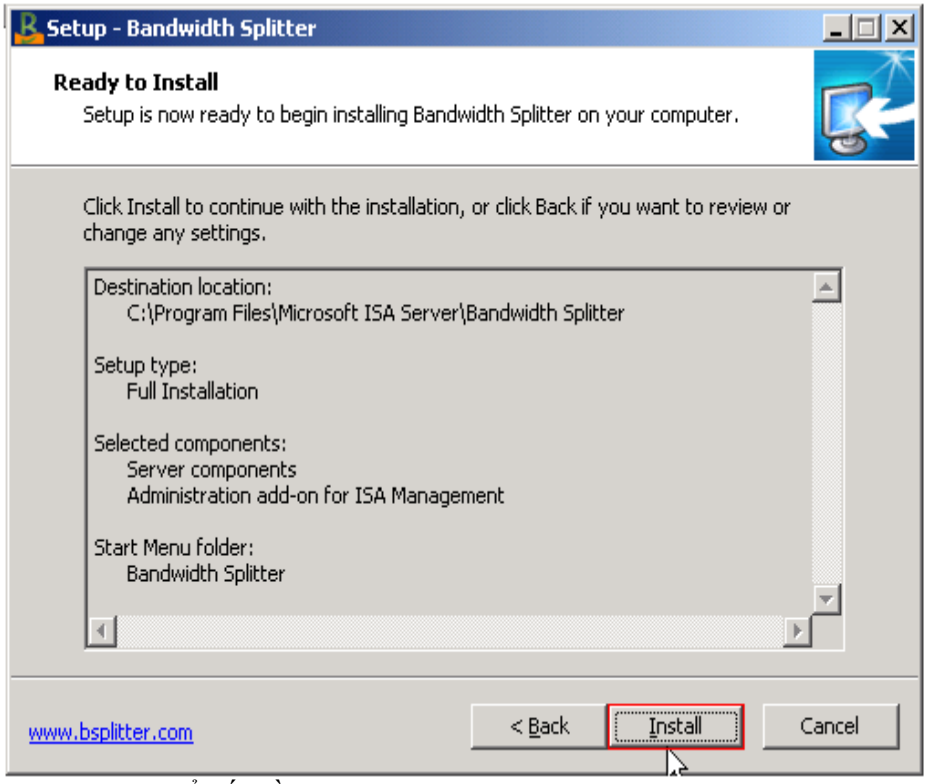
Có 2 mục để lựa chọn,Full Installation hoặc Custom Installation, ở đây chọn Full Installation, click Next để tiếp tục



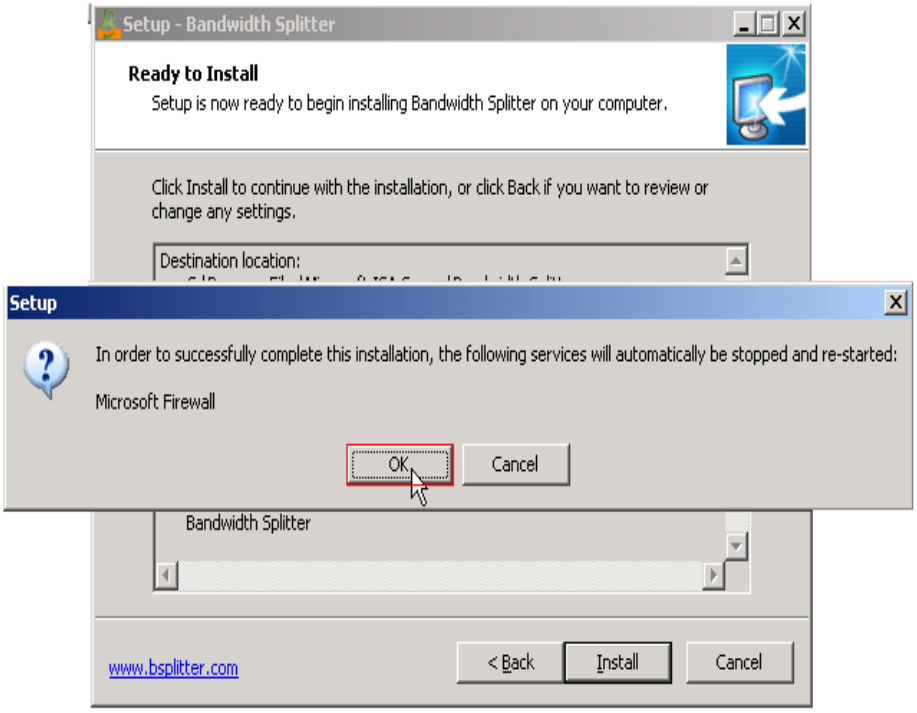
Tiếp tục click Next



Ở giao diện này, ta để mặc định các Options và click Next để tiếp tục

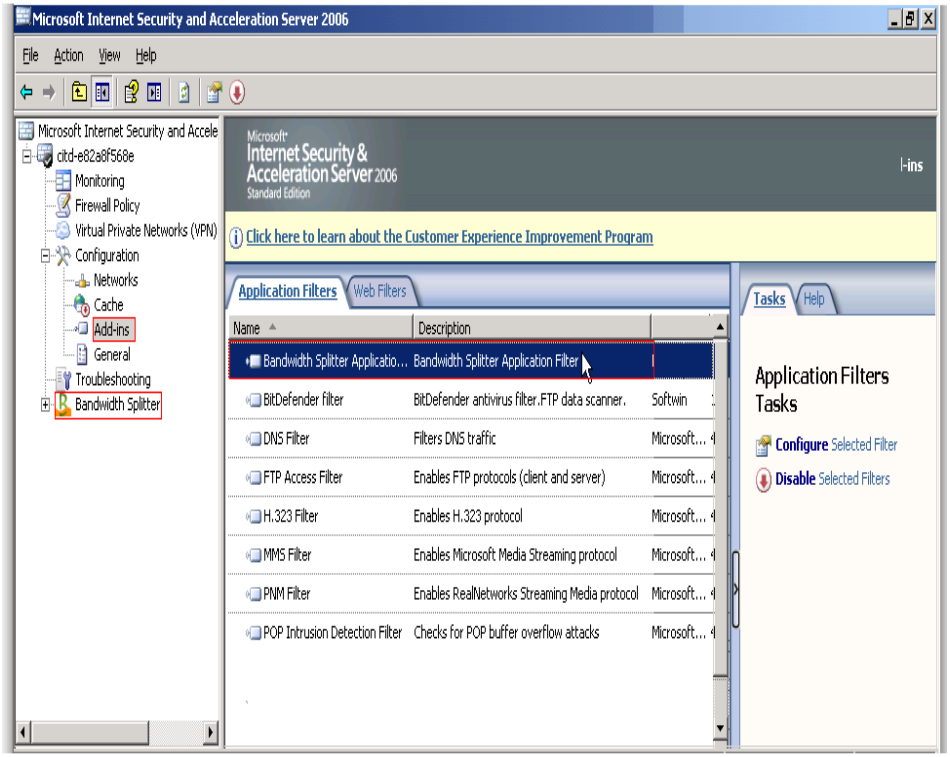


Click chọn Install để bắt đầu cài đặt



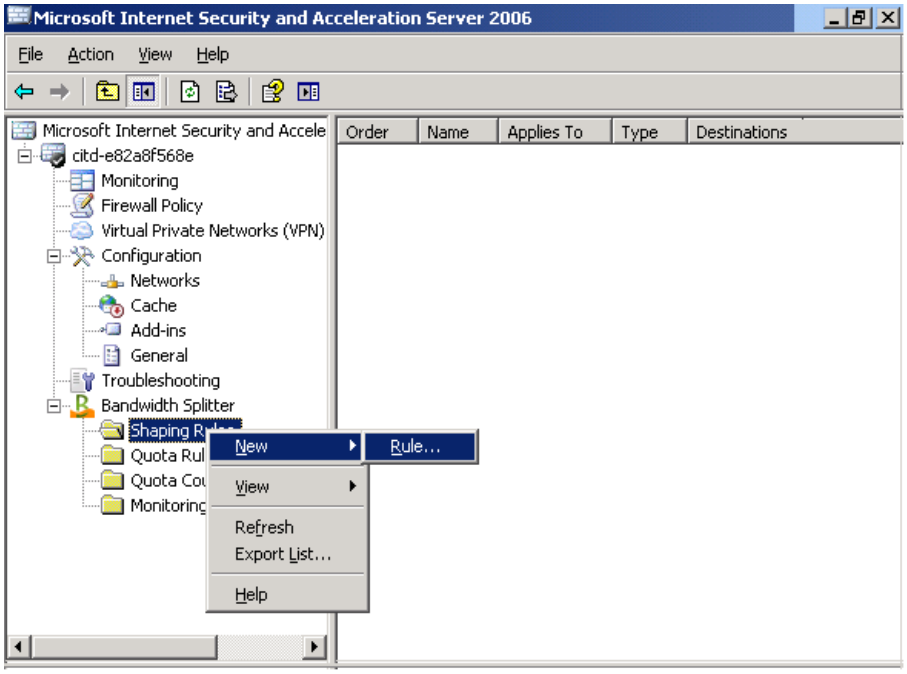
Click chọn Ok để tiếp tục

Click chọn Finish để kết thúc cài đặt



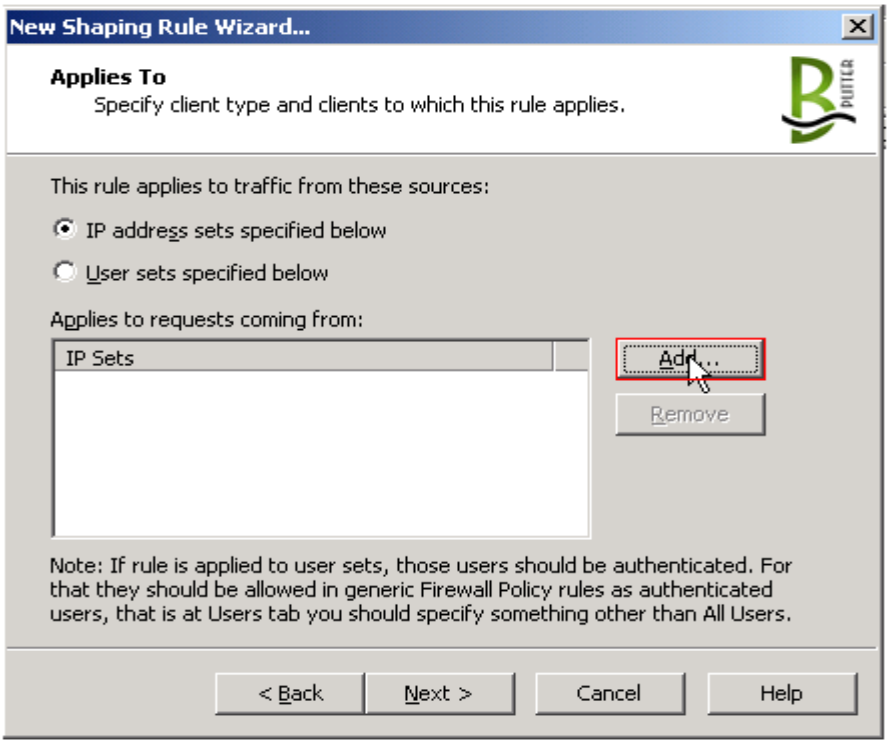
Vào giao diện Isa Management, chọn phần Add-ins, ta thấy Bsplitter đã được tích hợp vào

11.2. Xét Rule giới hạn băng thông đối với người dùng nội bộ

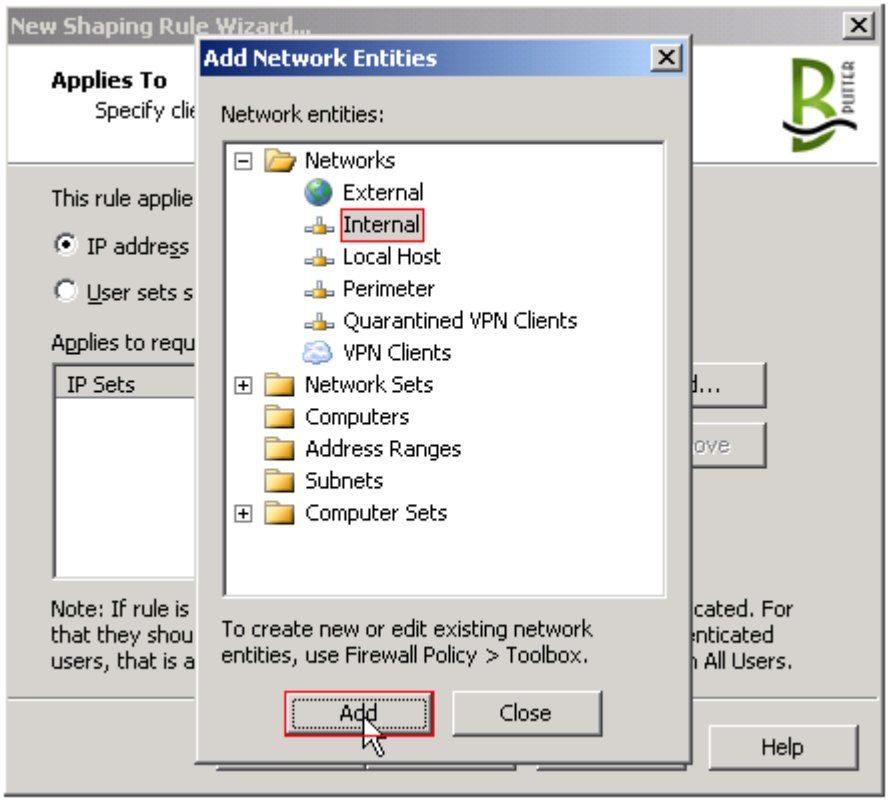


Trong giao diện Isa Management, ở khung bên trái, mở rộng mục Bandwidth Splitter, click chuột phải lên mục Shaping rule, chọn New ---> Rule

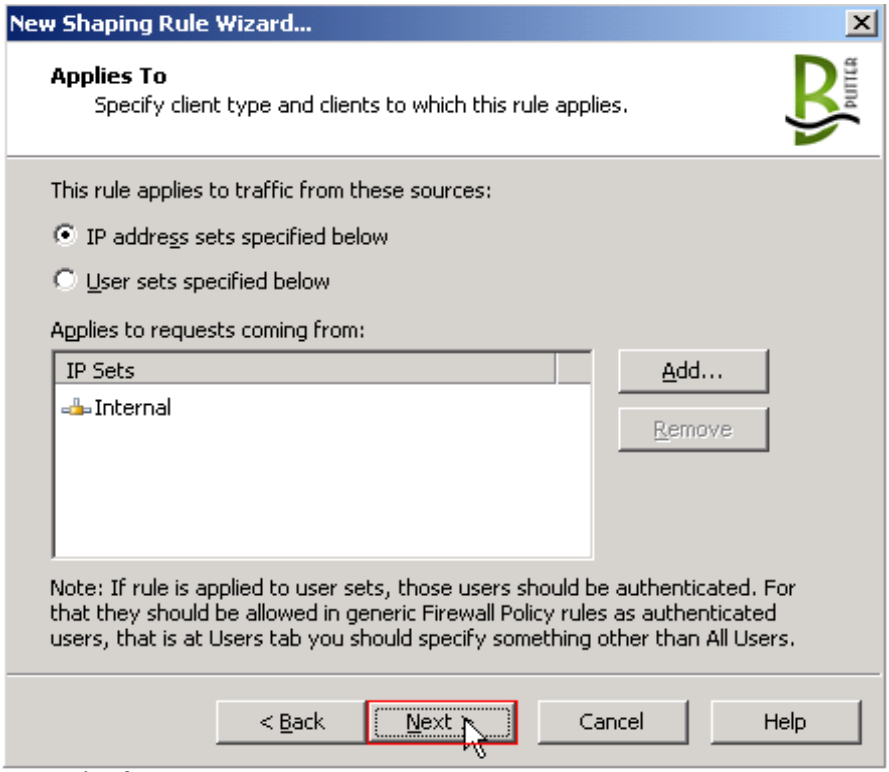
Nhập tên Rule vào mục Shaping rule name, rồi click Next để tiếp tục



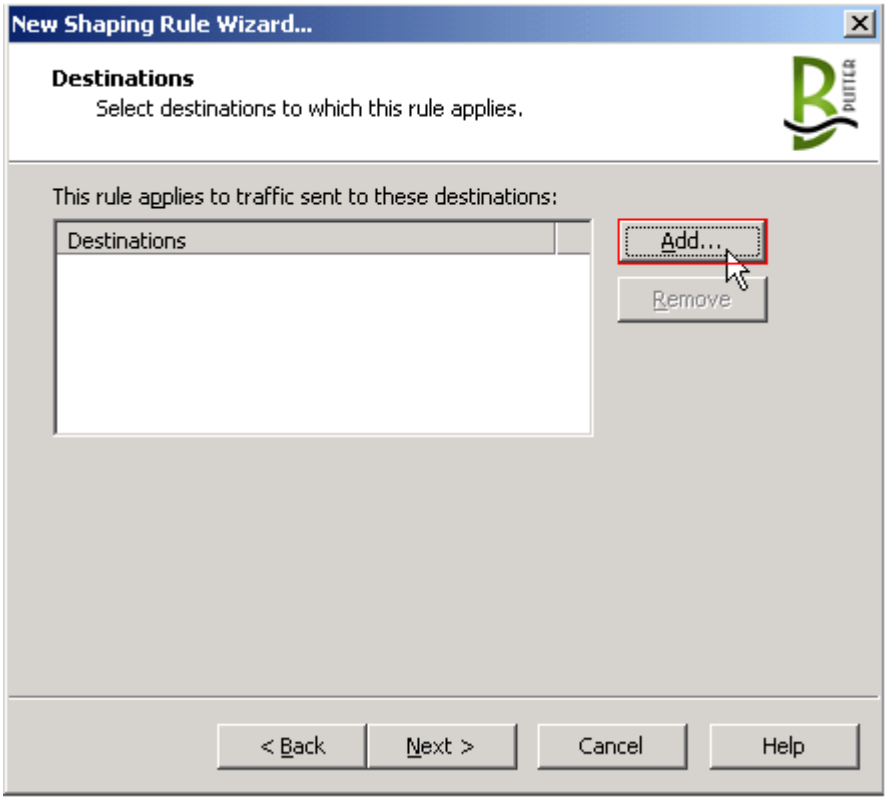
Ở giao diện này, click chuột chọn Add



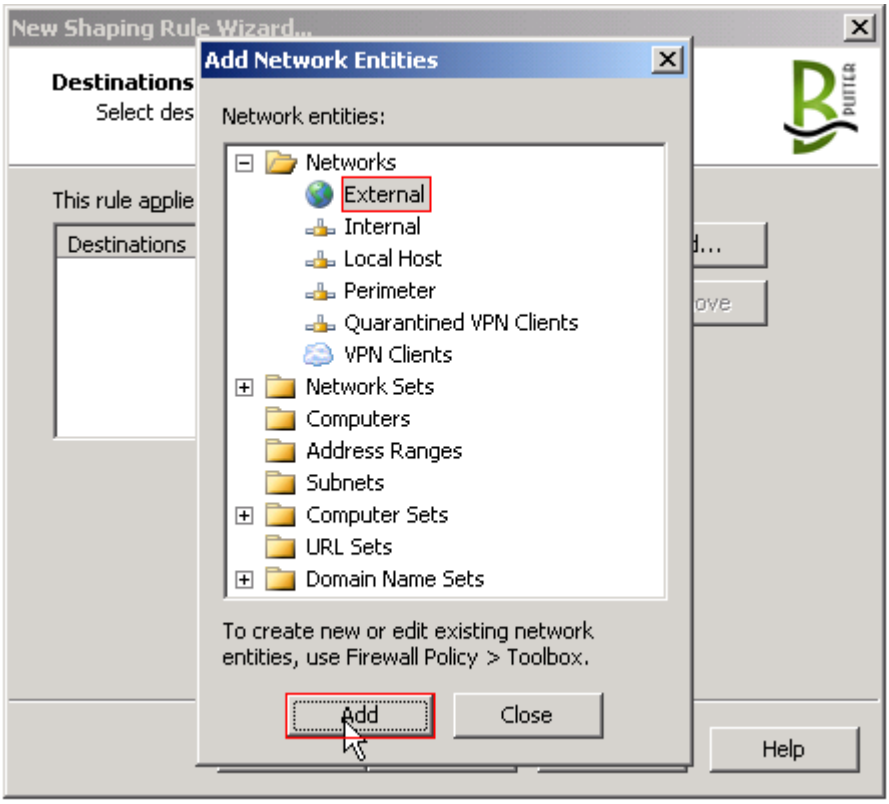
Ở phần Network, chọn Internal rồi nhấn Add để chọn



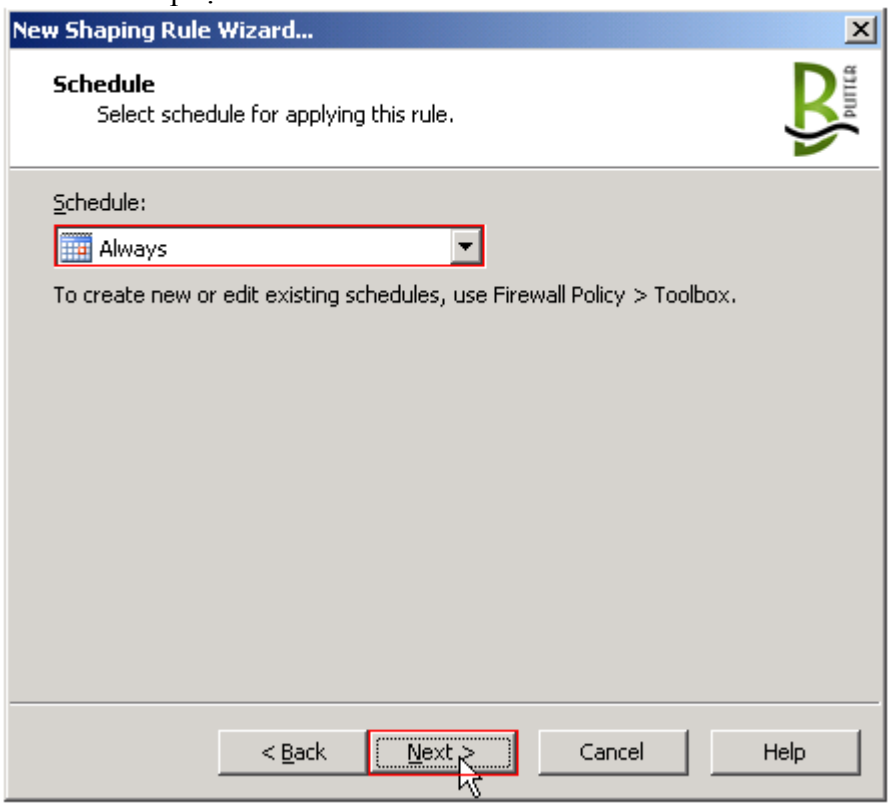
Click Next để tiếp tục



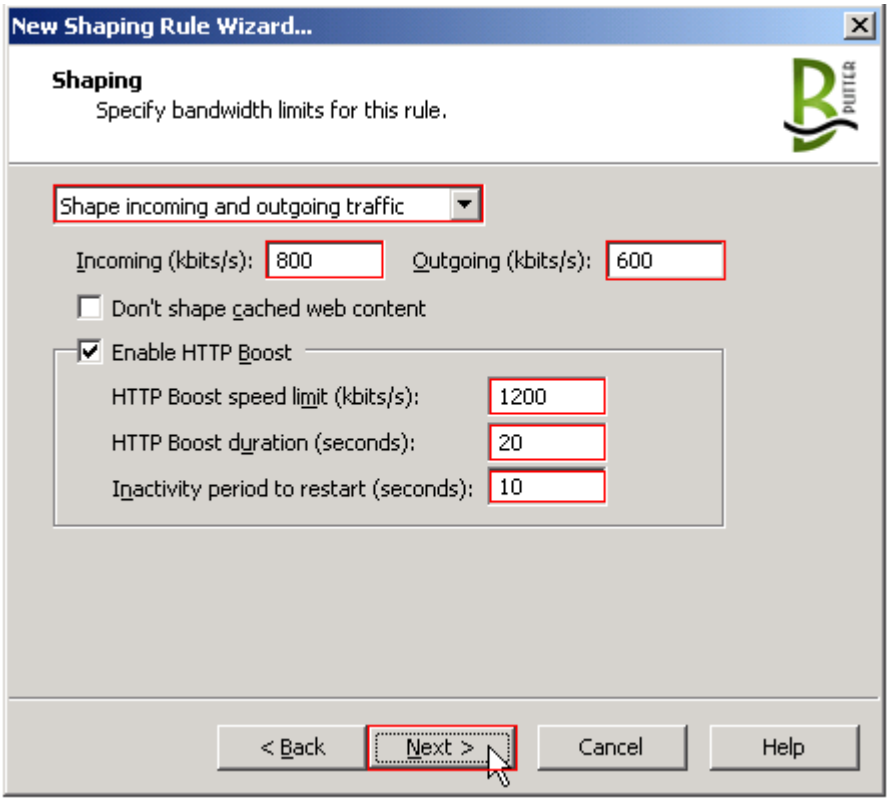
Click chuột chọn Add



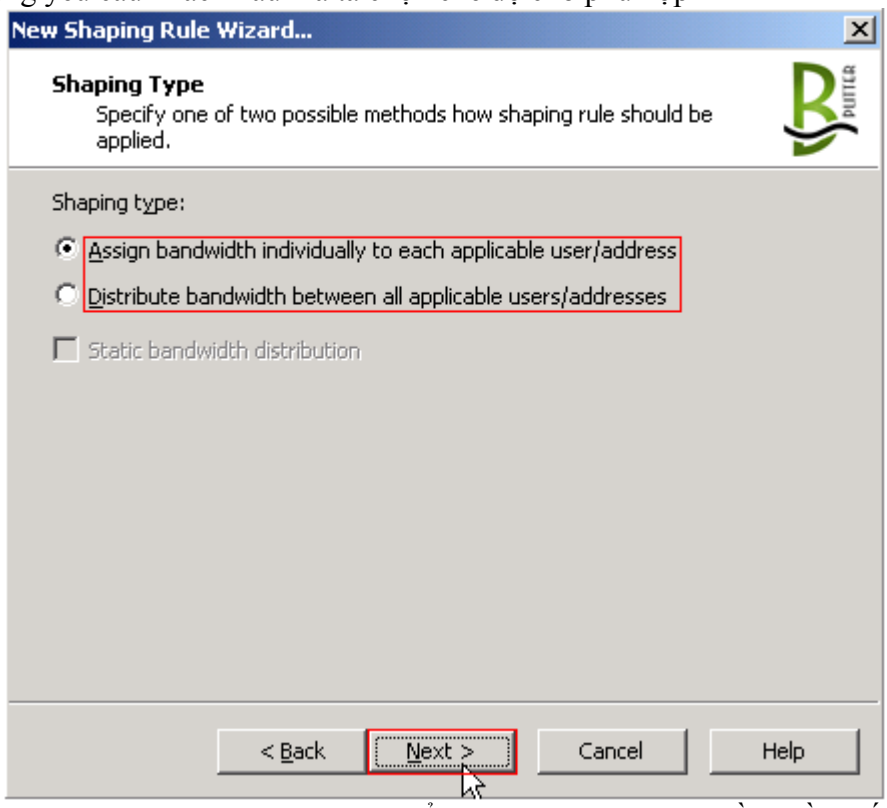
Ở phần Network, chọn External rồi nhấn Add để chọn
Click Next để tiếp tục, đến giao diện Schedule, chọn khoảng thời gian thích hợp, rồi nhấn Next để tiếp tục



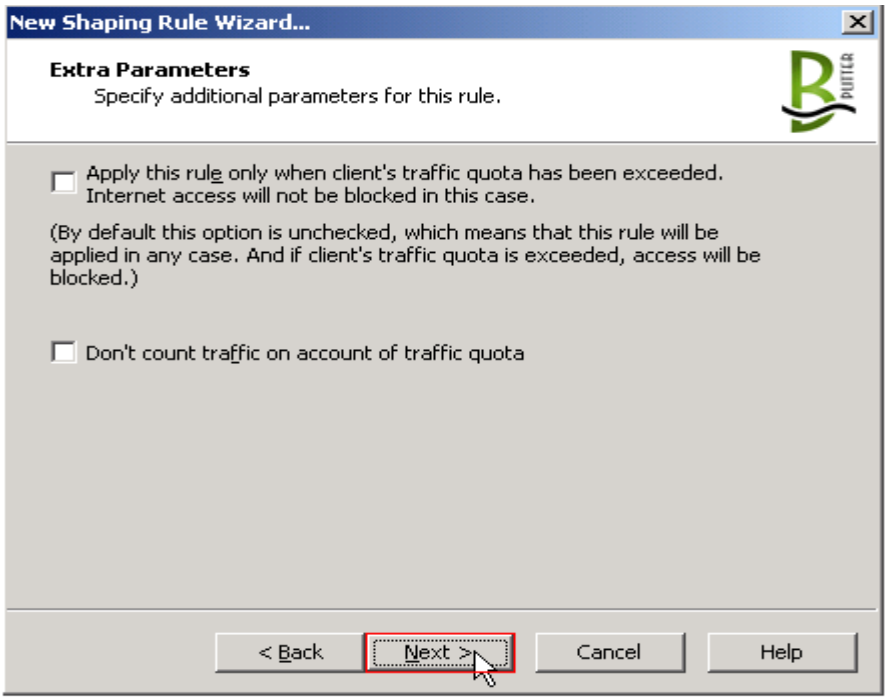
Click Next để tiếp tục, đến giao diện Schedule, chọn khoảng thời gian thích hợp, rồi nhấn Next để tiếp tục



Ở giao diện này, ta chọn chế độ quản lý băng thông để download va upload, tùy theo từng yêu cầu khác nhau mà ta chọn chế độ cho phù hợp



Chọn Options như mặc định hoặc có thể chọn lại tùy theo yêu cầu. Rồi nhấn Next để tiếp tục



Để mặc định, tiếp tục nhấn Next

Click Finish để kết thúc việc xét Rule

Trở lại mục Firewall Policy, nhấn Apply Changes để lưu những thay đổi vừa thực hiện

12. Cài đặt và xét Rule cho phần mềm Bitdefender Security

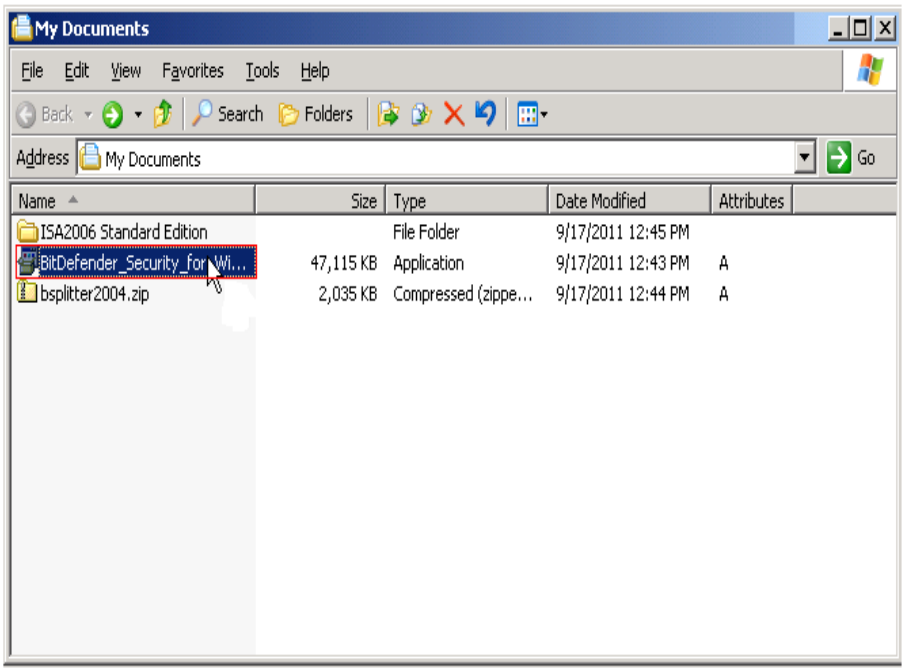
BitDefender là một bộ phần mềm phòng chống và diệt các mối nguy hiểm cho máy tính được phát triển dựa trên phần mềm công ty SOFTWIN,Rumani và được khai trương vào Tháng Mười Một năm 2001.

Các sản phẩm của Bitdefender có tính năng phòng chống và diệt các loại virus, spyware, malware, lọc thư rác, backup, tune-up, kiểm soát người dùng... cho người dùng thông thường và cho các doanh nghiệp.

Một số tính năng chính của "BitDefender Security Scan":

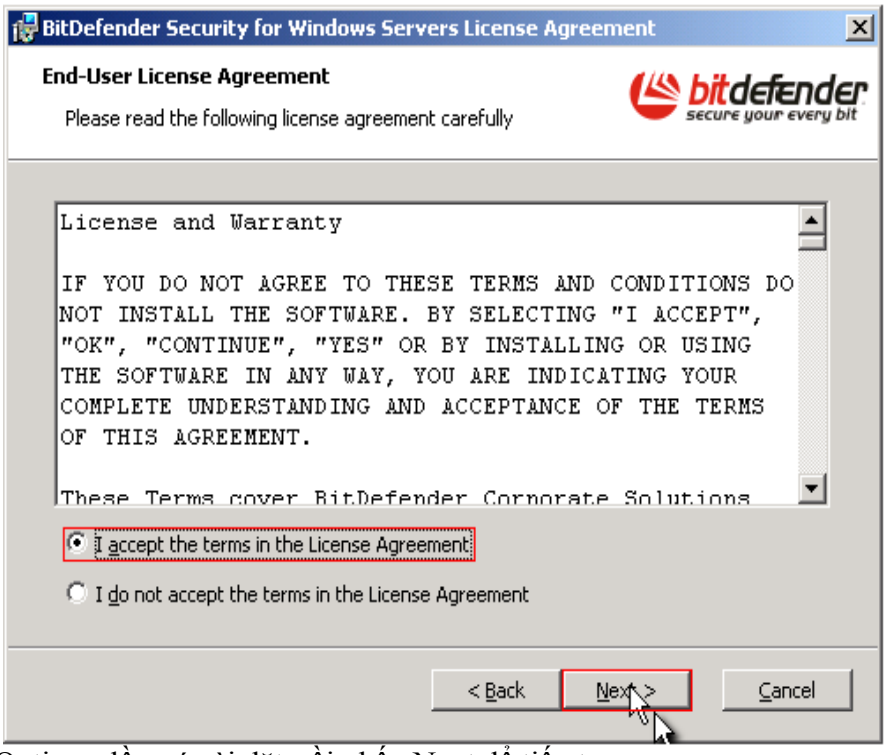
- AV QuickScan - Quét virus
- Registry Tuning - Khắc phục những vấn đề registry làm cho máy chạy chậm, đóng băng hoặc treo máy.
- Cập nhật Watcher.
- Security status - Kiểm tra sự tồn tại và tình trạng của phần mềm bảo mật trên hệ thống.
- Scheduled Scanning - Thiết lập quét định kỳ để đảm bảo hệ thống được an toàn. QuickScan sẽ tự động quét máy tính của bạn khi khởi động máy.
- Antivirus Spot Check - Kiểm tra theo yêu cầu của bạn.

12.1. Cài đặt Bitdefender Security

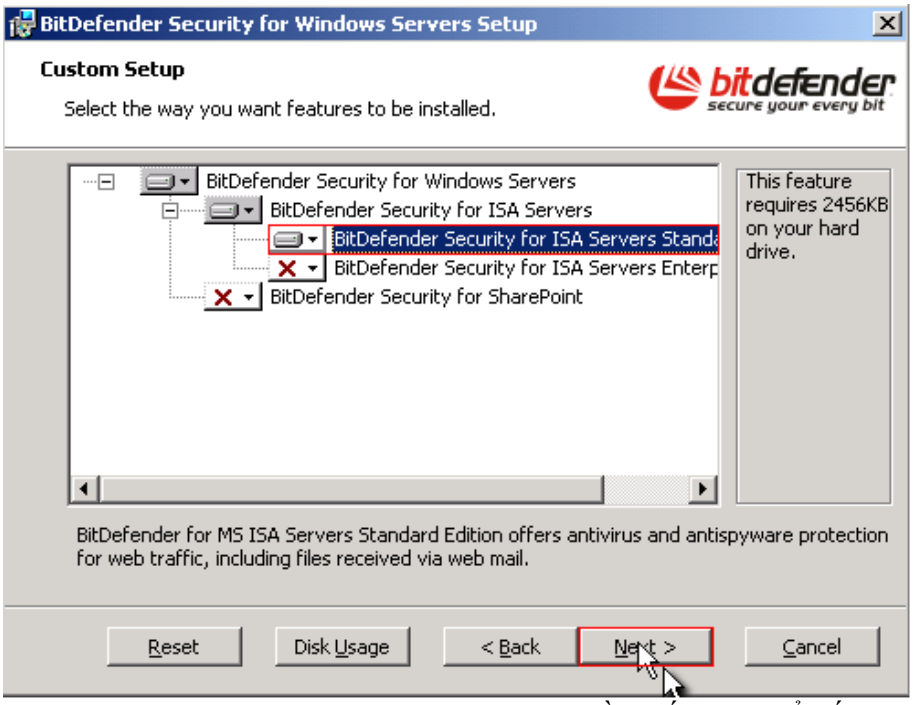


Double click chuột vào file Bitdefender_Security.exe

Click Next để tiếp tục quá trình cài đặt

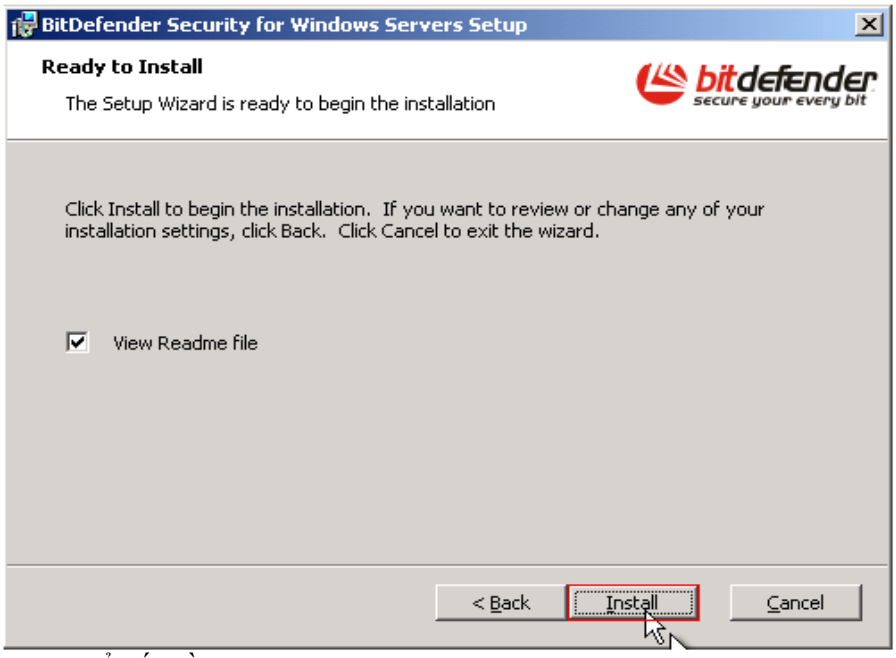


Chọn Options đồng ý cài đặt, rồi nhấn Next để tiếp tục



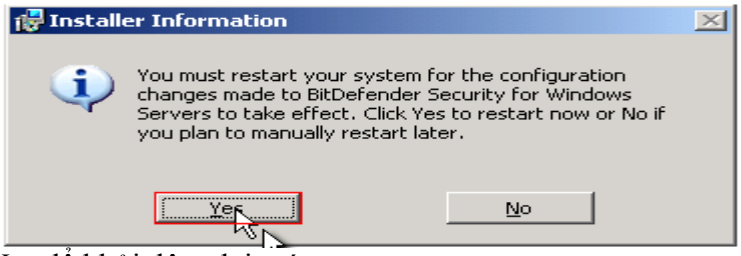
Chọn cài đặt tùy theo bản Isa Server đang sử dụng, rồi nhấn Next để tiếp tục

Chọn mặc định các Options, nhấn Next để tiếp tục

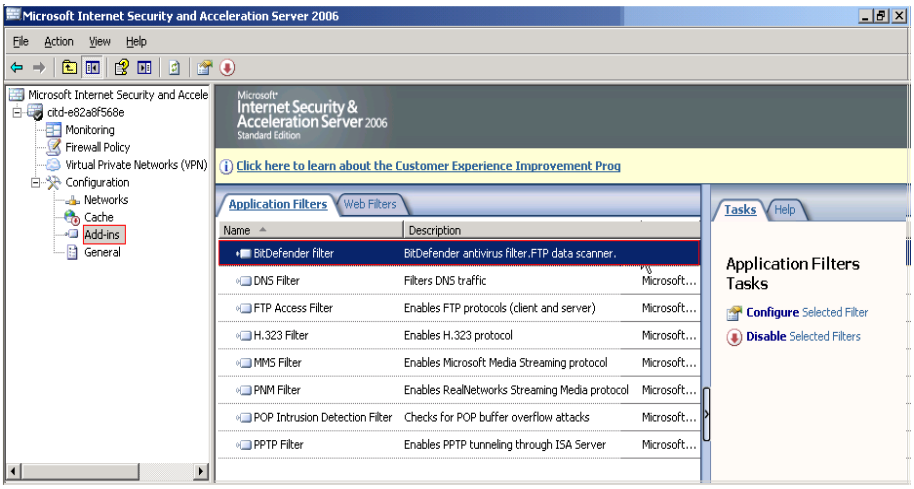


Click Install để bắt đầu cài đặt

Sau khi cài đặt xong nhấn Finish để kết thúc

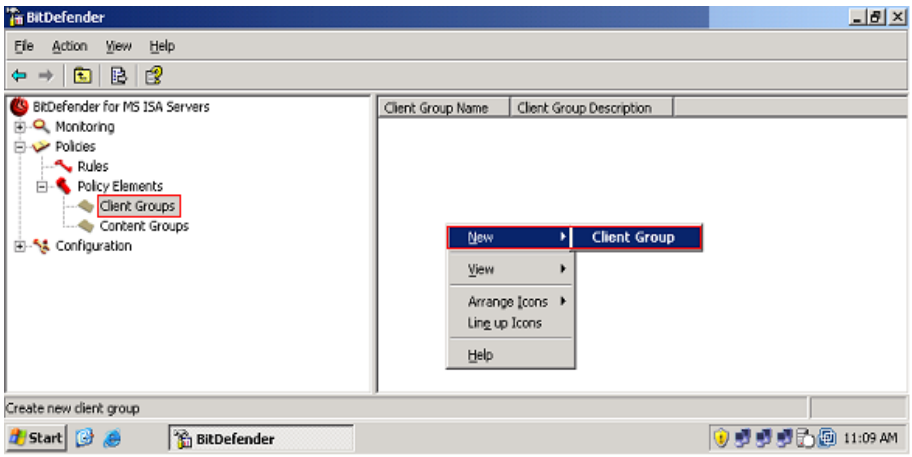


Click chọn Yes để khởi động lại máy

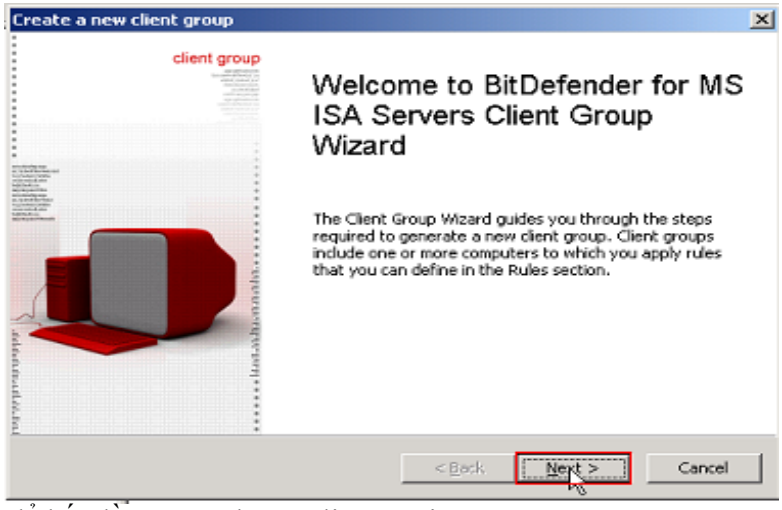


Vào giao diện Isa Management, chọn mục Add-ins, Bitdefender Security đã được tích hợp vào Isa Server

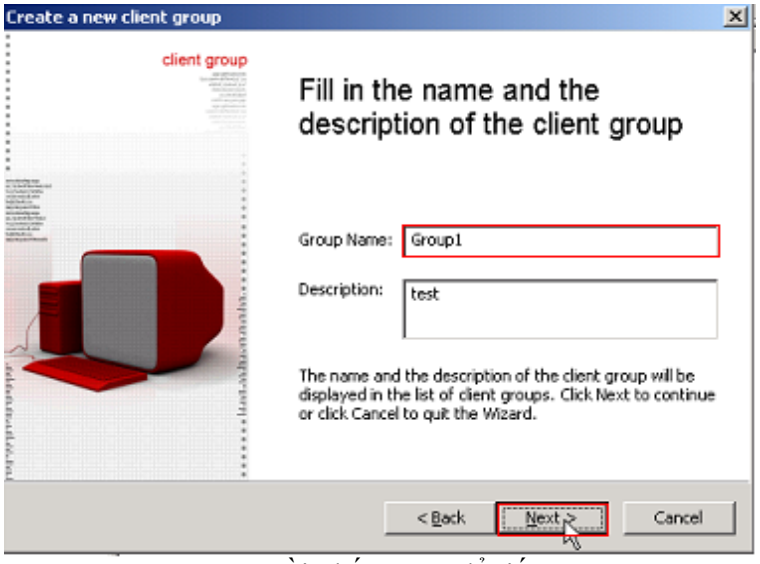
12.2. Xét Rule cấm người dùng nội bộ download tập tin đã được chỉ định bởi Bitdefender Security



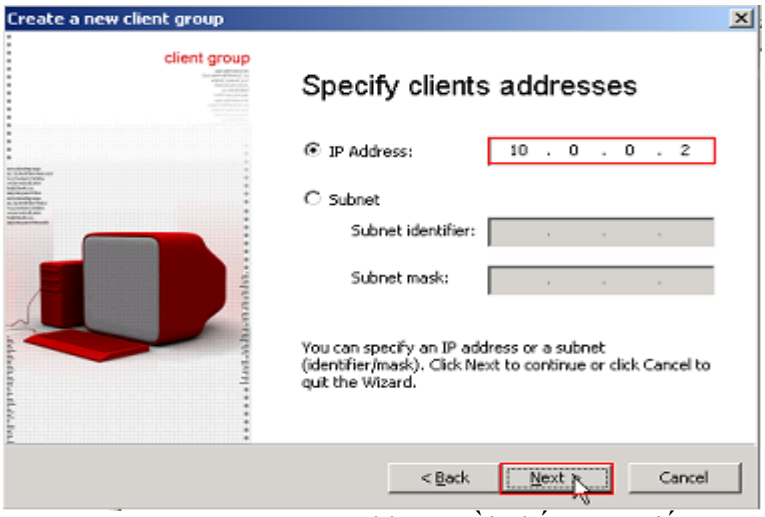
Mở giao diện Bitdefender Security lên, ở khung bên trái nhấp vào mục Policies, sau đó nhấp vào mục Policy Elements, chọn Client Groups, bên khung phải nhấp chuột phải, chọn New \ Client Group



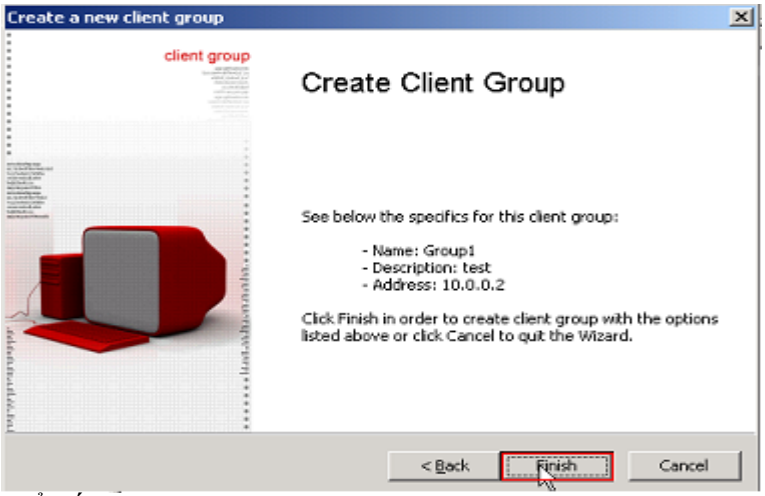
Click Next để bắt đầu tạo 1 nhóm Client mới



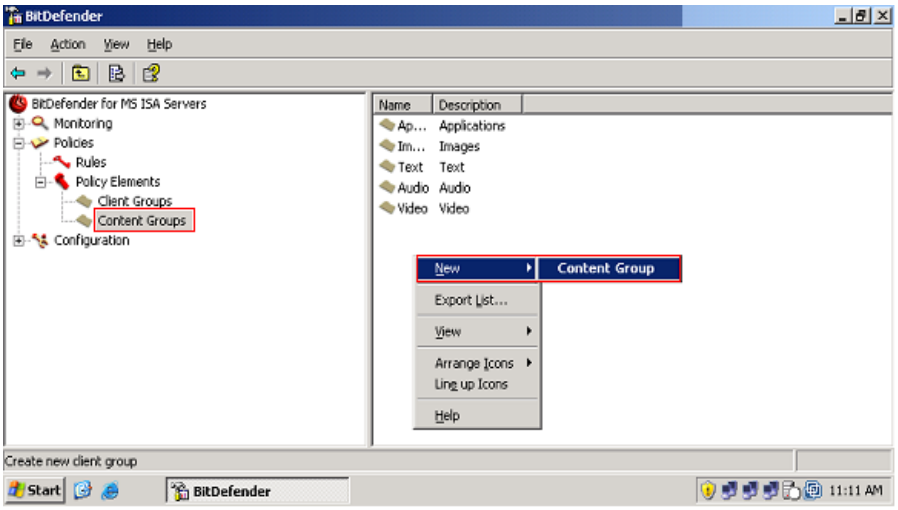
Nhập tên vào mục Group Name, rồi nhấn Next để tiếp tục



Nhập địa chỉ Ip máy trạm vào mục Ip Address, rồi nhấn Next tiếp tục

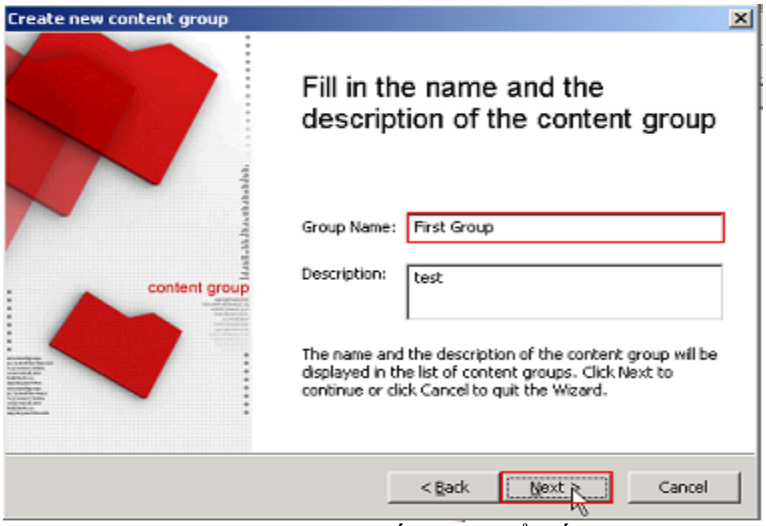


Click Finish để kết thúc

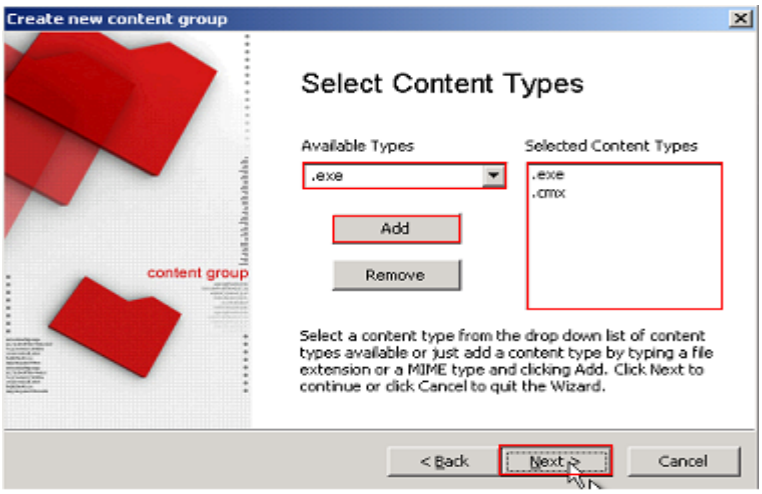


Ở mục Policy Elements, ta chọn Content Groups, bên khung phải ta click chuột phải chọn New \ Content Group, để tạo nhóm nội dung mới

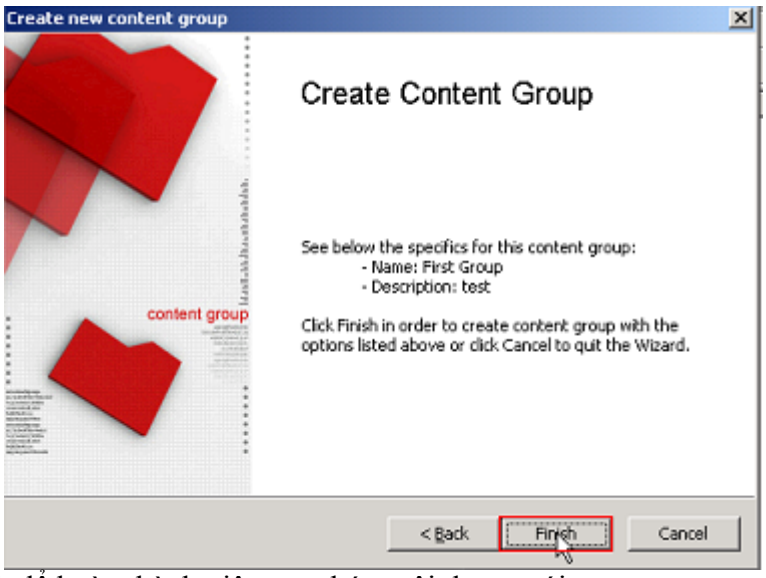
Click Next để tiếp tục



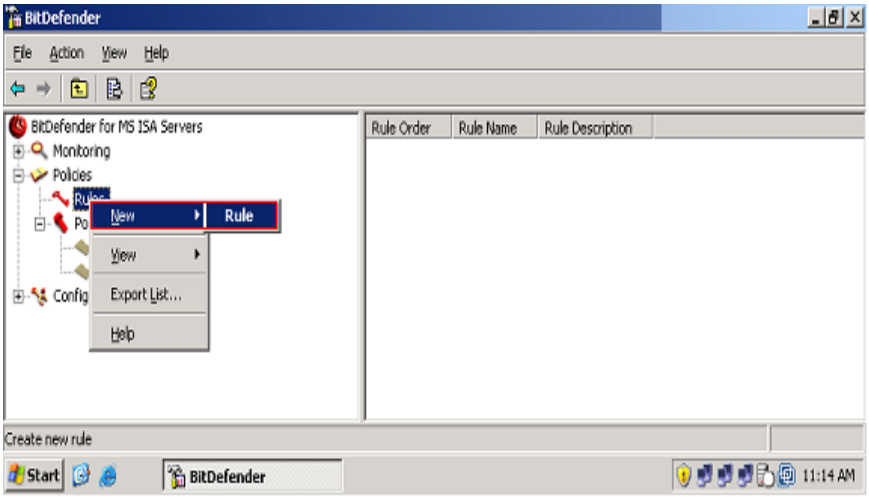
Nhập tên vào mục Group name, sau đó nhấn Next để tiếp tục



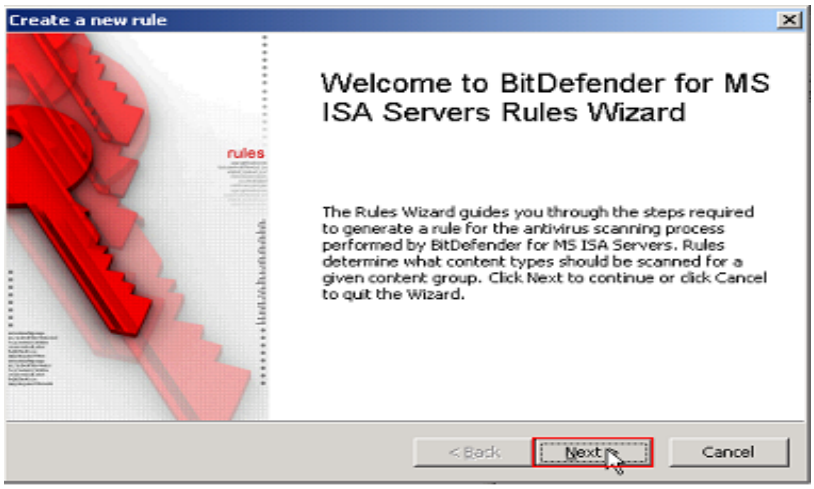
Chọn các đuôi định dạng tập tin, rồi nhấn Add để thêm vào, sau đó nhấn Next tiếp tục



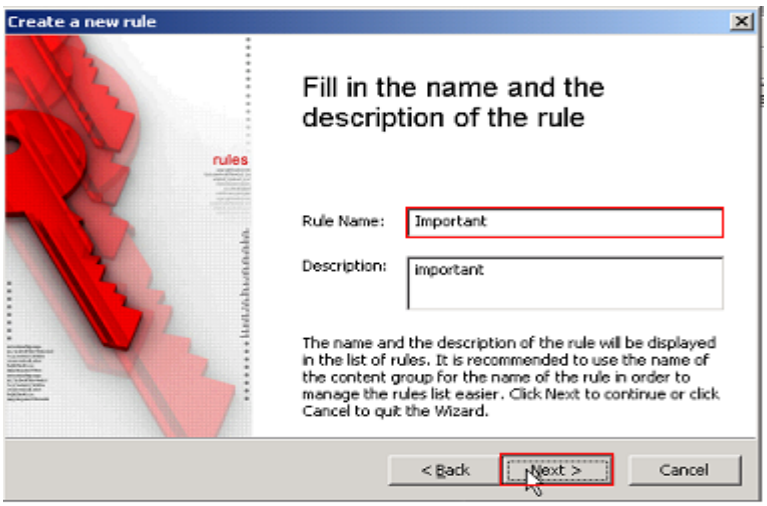
Click Finish để hoàn thành việc tạo nhóm nội dung mới



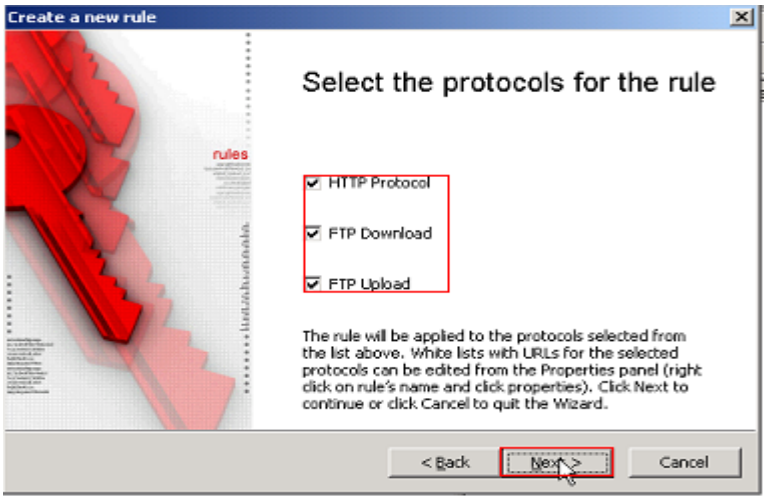
Tiếp tục ở mục Policies, ta click chuột phải vào mục Rules, chọn New\ Rule



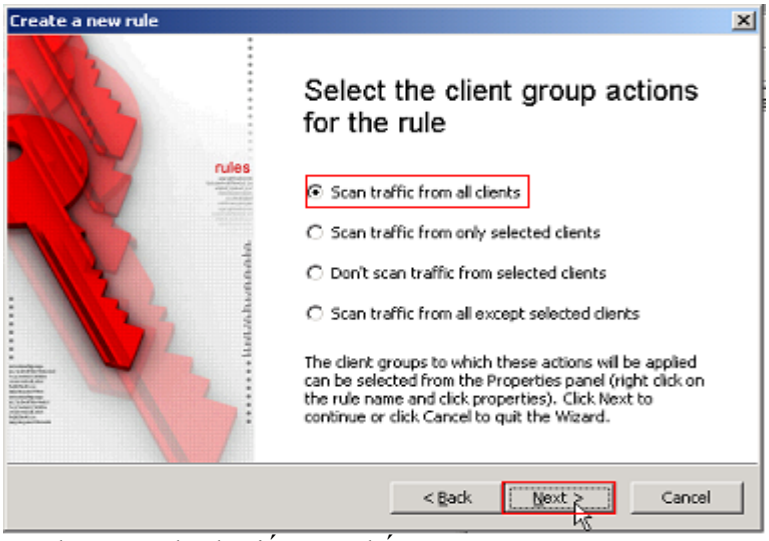
Click Next để tạo luật (Rule) mới



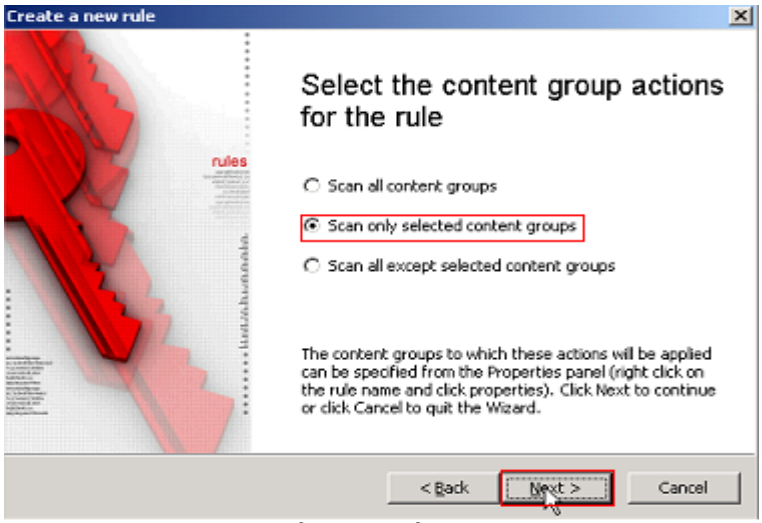
Nhập tên cho luật mới ở mục Rule name, rồi nhấn Next để tiếp tục



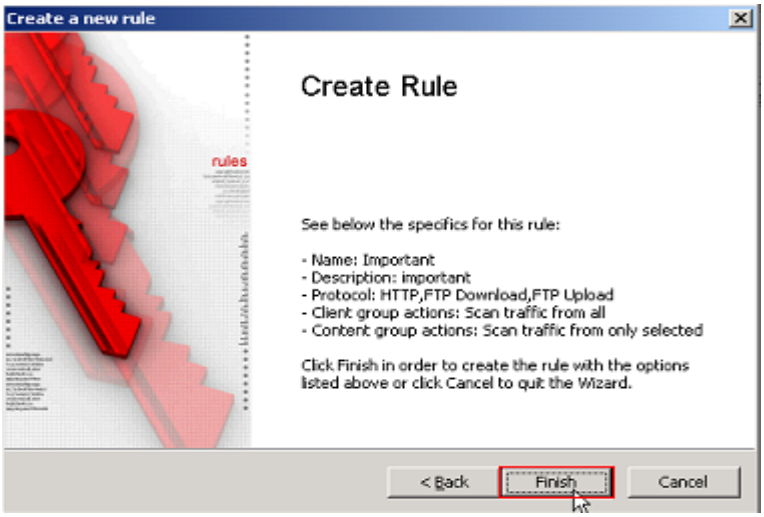
Để các Options như mặc định, hoặc có thể thay đổi tùy theo từng trường hợp, rồi nhấn Next



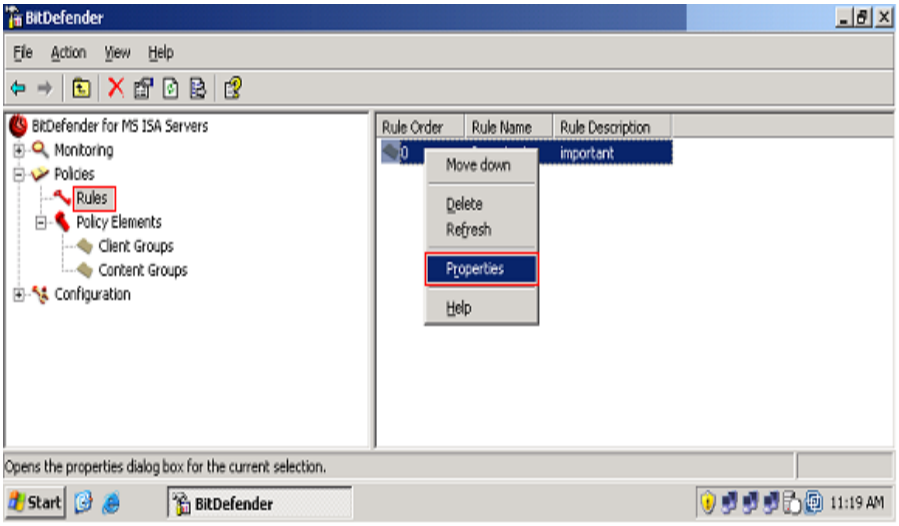
Chọn Options như trong hình, tiếp tục nhấn Next



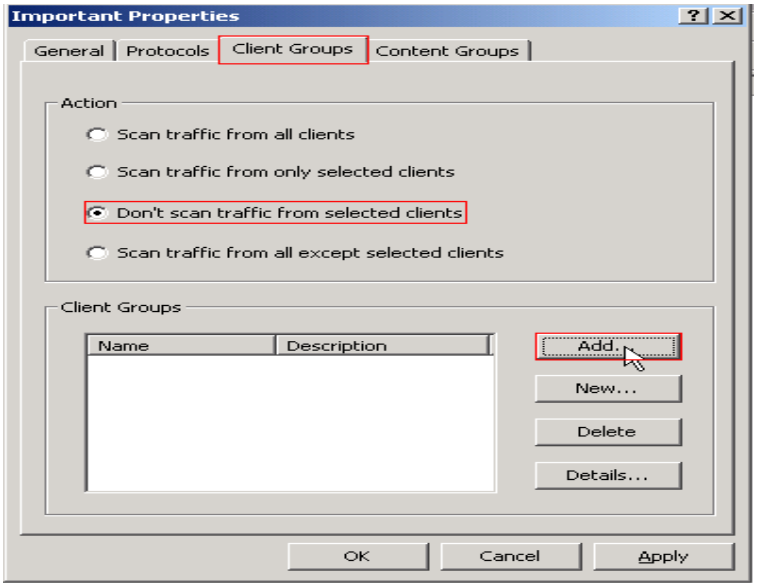
Chọn Options như trong hình và tiếp tục nhấn Next



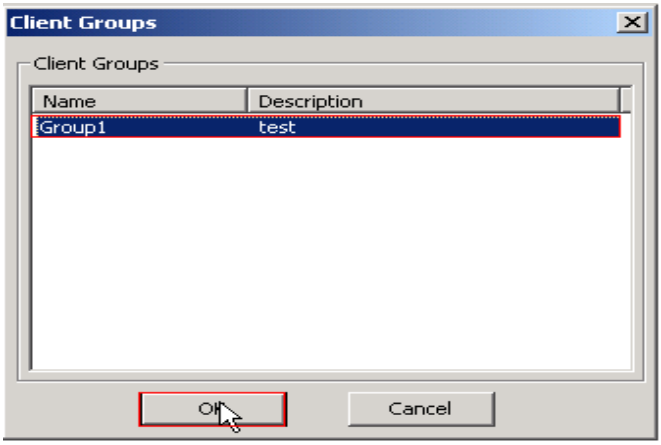
Click Finish để hoàn thành việc tạo Rule mới



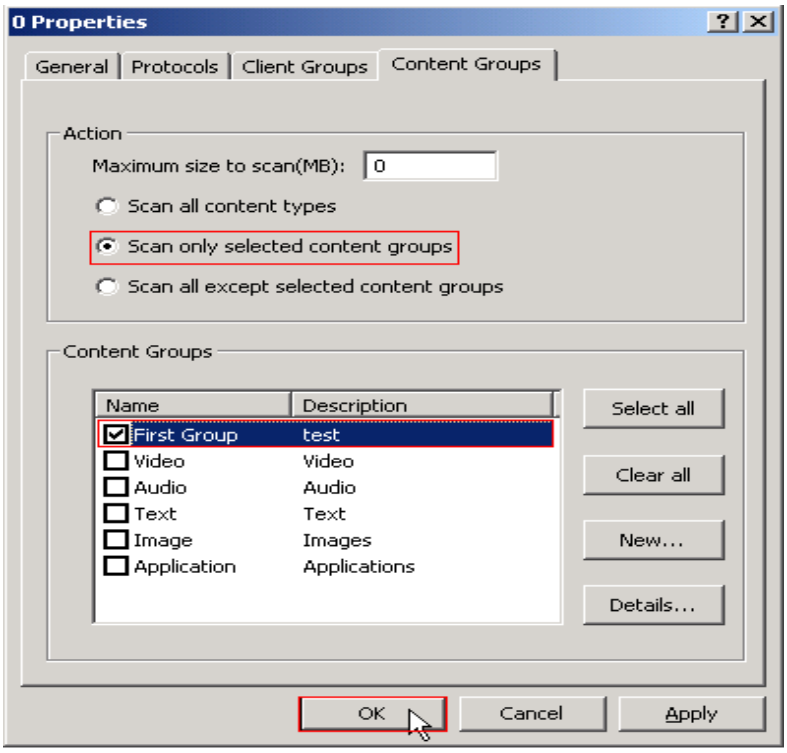
Trên Rule vừa tạo, click chuột phải chọn Properties



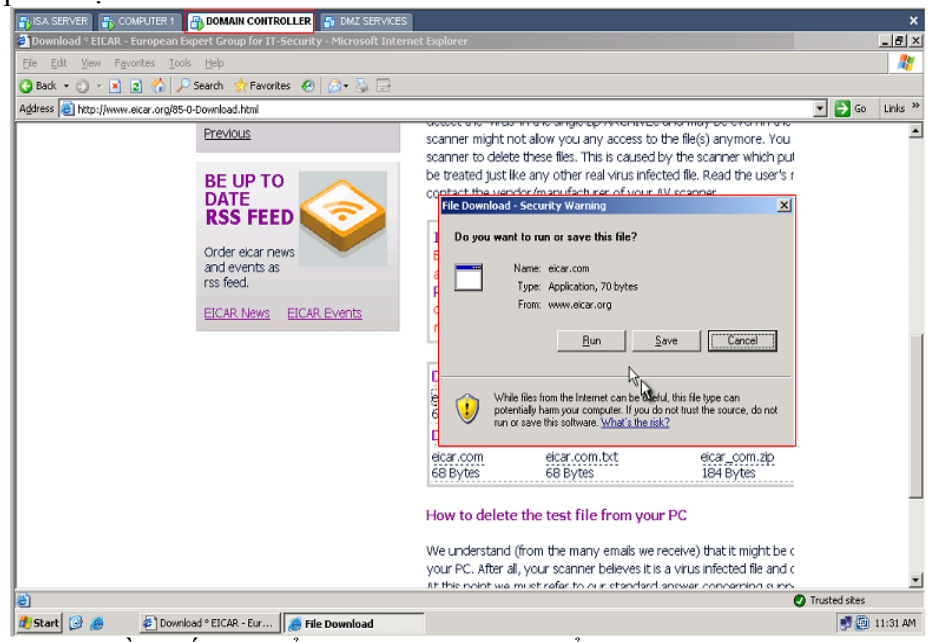
Ta chọn tab Client Group, chọn Option thứ 3 và click Add



Chọn Client Group vừa tạo, rồi nhấn Ok để chọn

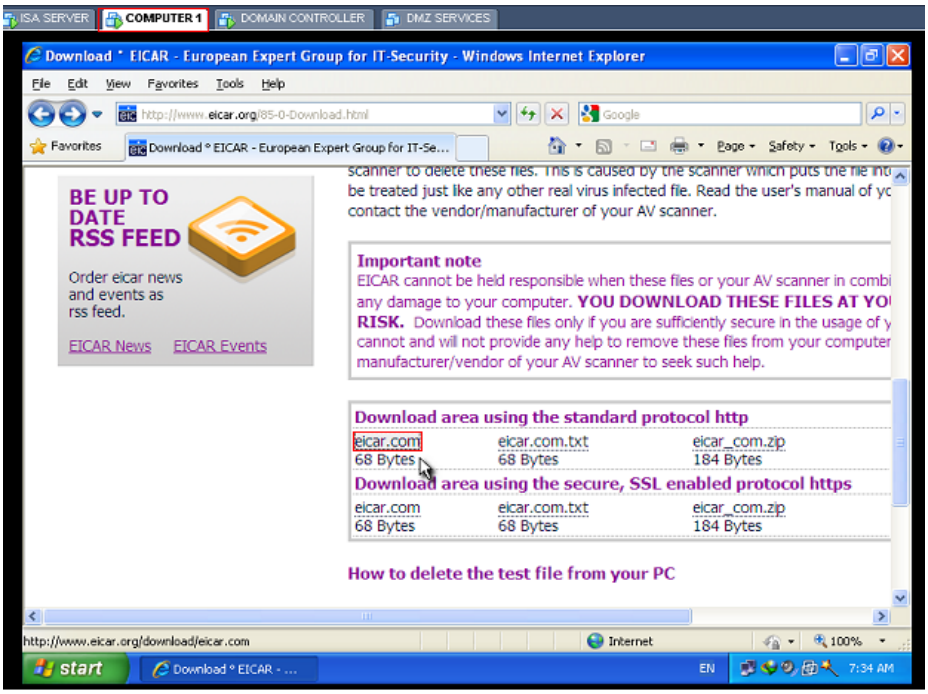


Tiếp tục, qua tab Content Groups, chọn Options dòng thứ 3 và chọn Content Group vừa tạo

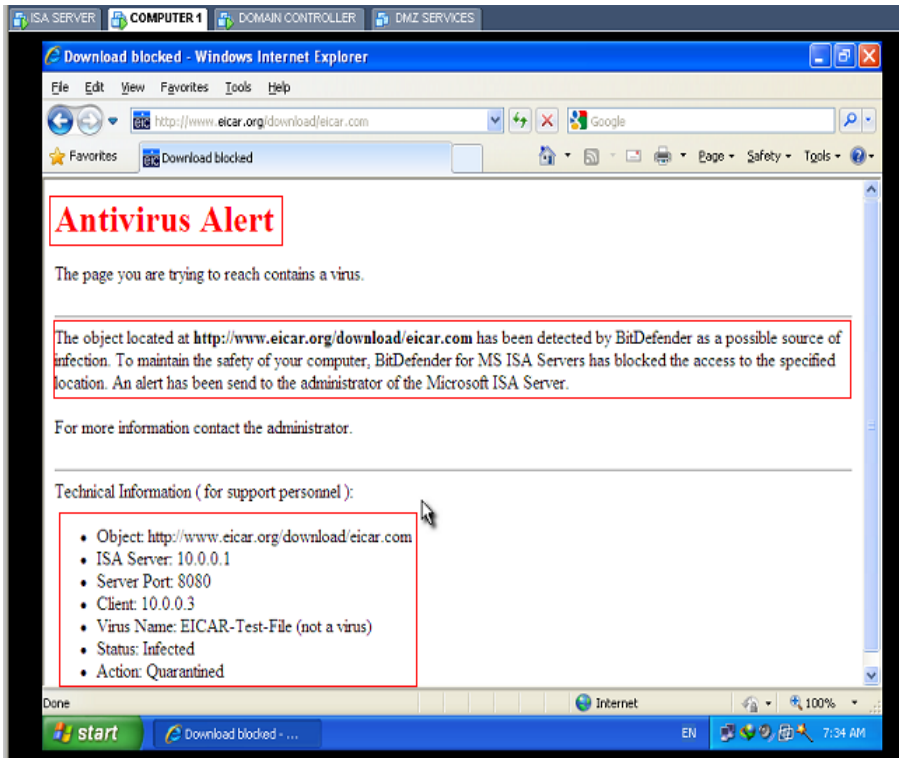


Click Apply, rồi nhấn Ok để lưu lại những thay đổi.

Bây giờ mở máy Domain có địa chỉ IP : 10.0.0.2 lên, vào trang www.eicar.org, chọn mục download, ta thấy có thể save file lại



Tiếp tục mở máy Client Computer 1 có địa chỉ IP:10.0.0.3, vào trang www.eicar.org, chọn mục download



Ngay lập tức sẽ hiện lên 1 trang cảnh báo thay vì hộp lựa chọn save hoặc run file

CHƯƠNG III : Tìm hiểu và triển khai phần mềm

PC MONITOR CONSOLE

1. Khái quát:

PC Monitor Console là một công cụ cho phép bạn quan sát màn hình của những máy tính được nối trong mạng. theo cách này bạn có thể quan sát những điều nhân viên của bạn đang xem. Không những thế bạn có khả năng kiểm soát máy tính từ xa bằng chuột và bàn phím.

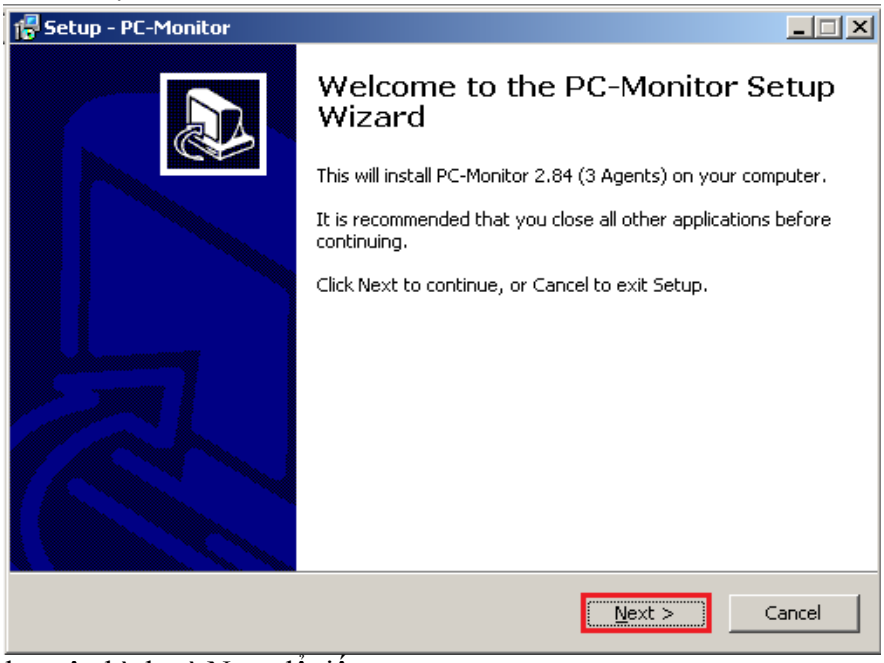
Ngoài ra bạn có thể ghi lại màn hình máy tính từ xa thậm chí cả khi bạn không quản lý chúng. Khi nhân viên của bạn cần chỉ dẫn, bạn có thể hướng dẫn họ qua màn hình PC của mình

Khi bạn cần sự chú ý, bạn có thể gửi thông điệp đến nhân viên và/hoặc khóa máy tính từ xa. Việc truyền thông sử dụng chế độ mã hóa. Những ứng dụng làm việc thông qua mạng Internet, LAN, WLAN hoặc VPN. Những phần mềm hoạt động theo lịch(như sắp xếp email, thu thập thông tin) có thể được cài từ xa.

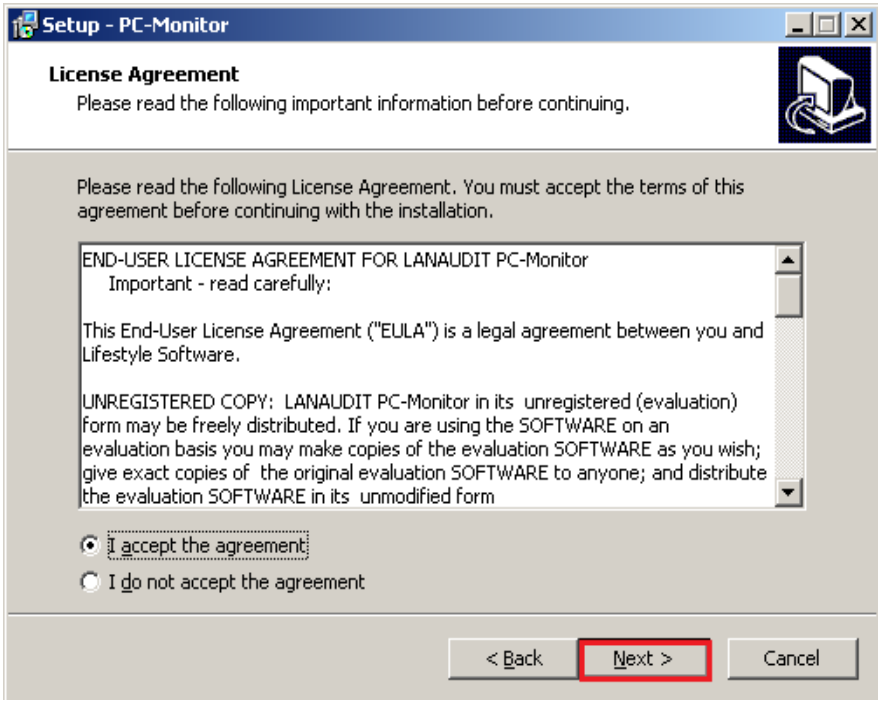
2. Cài đặt và Triển khai

- **Cài đặt PC Monitor Server**

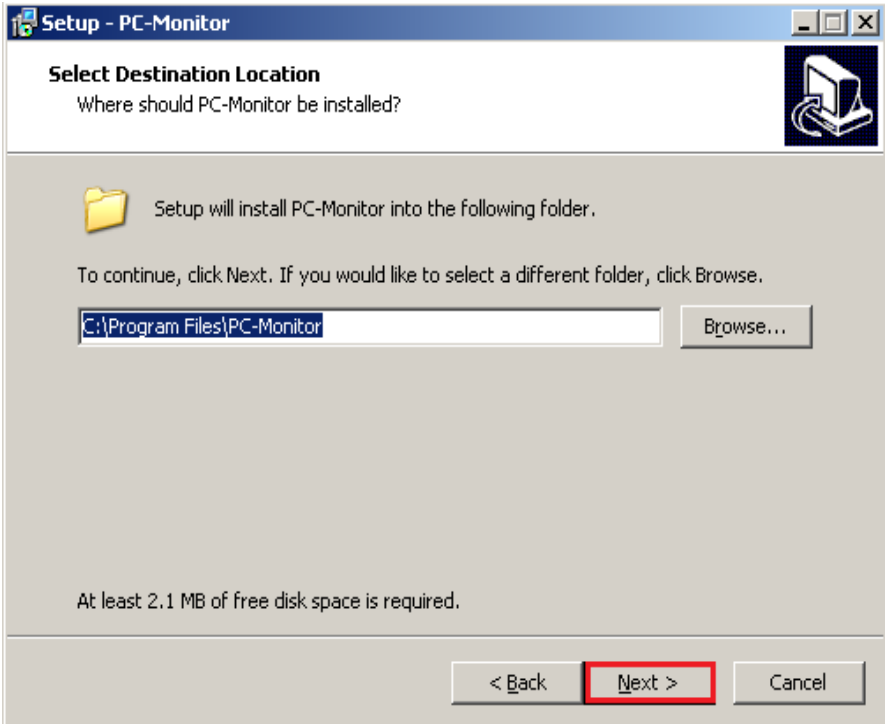
Console Server có thể chạy trên windows server 2003/2000/XP.Chạy server.exe để bắt đầu cài đặt



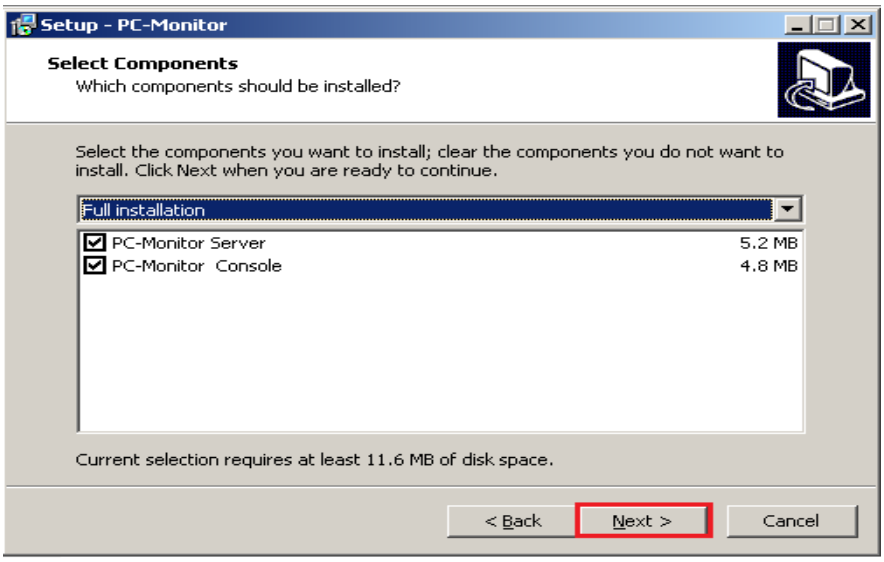
Chọn như trên hình và Next để tiếp tục



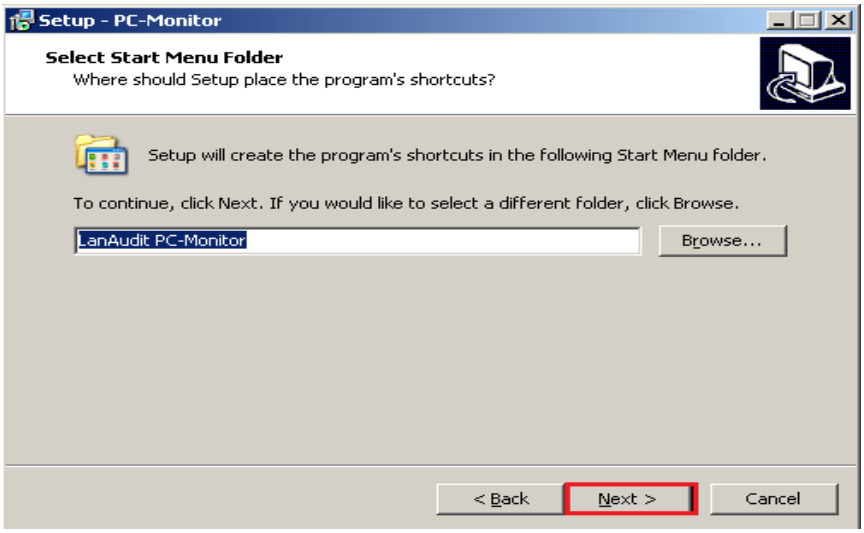
Click Next



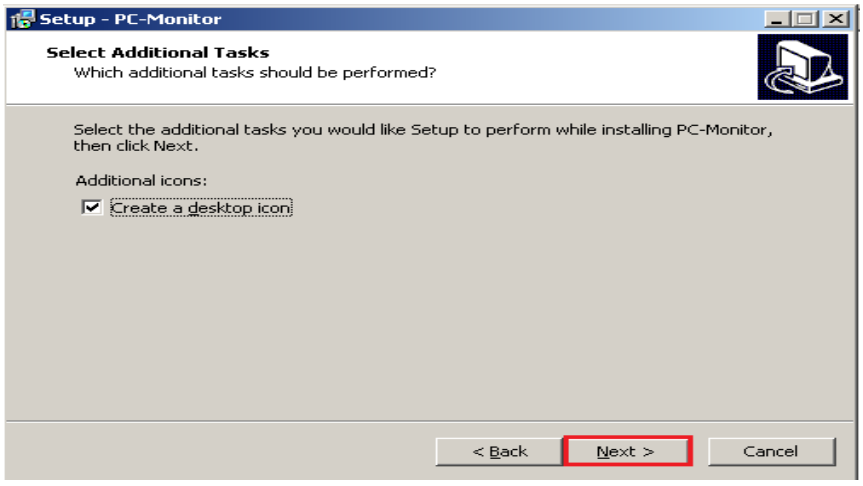
Chọn mặc định theo hình sau



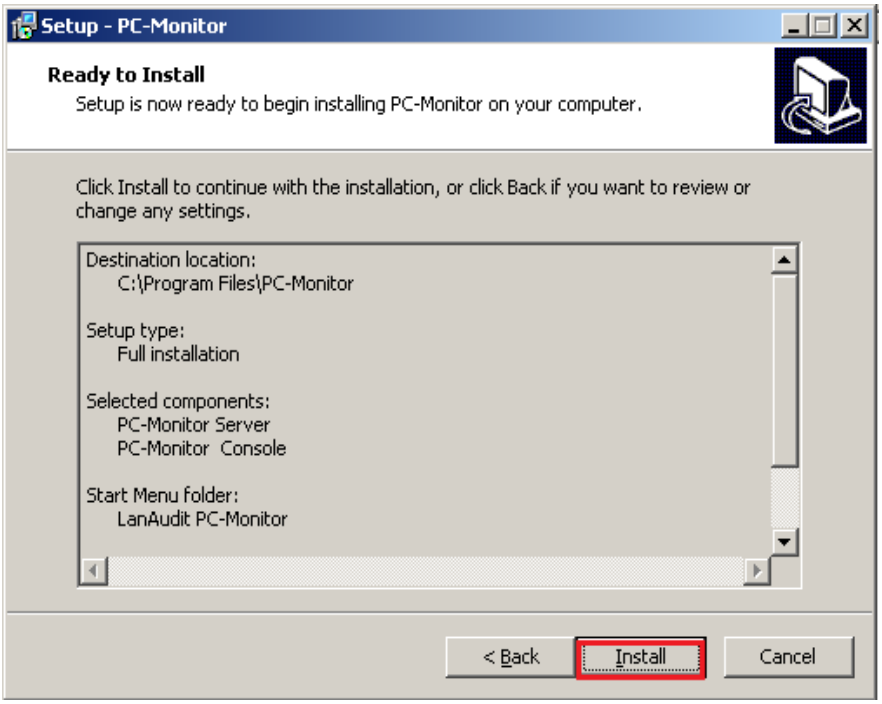
Click Next



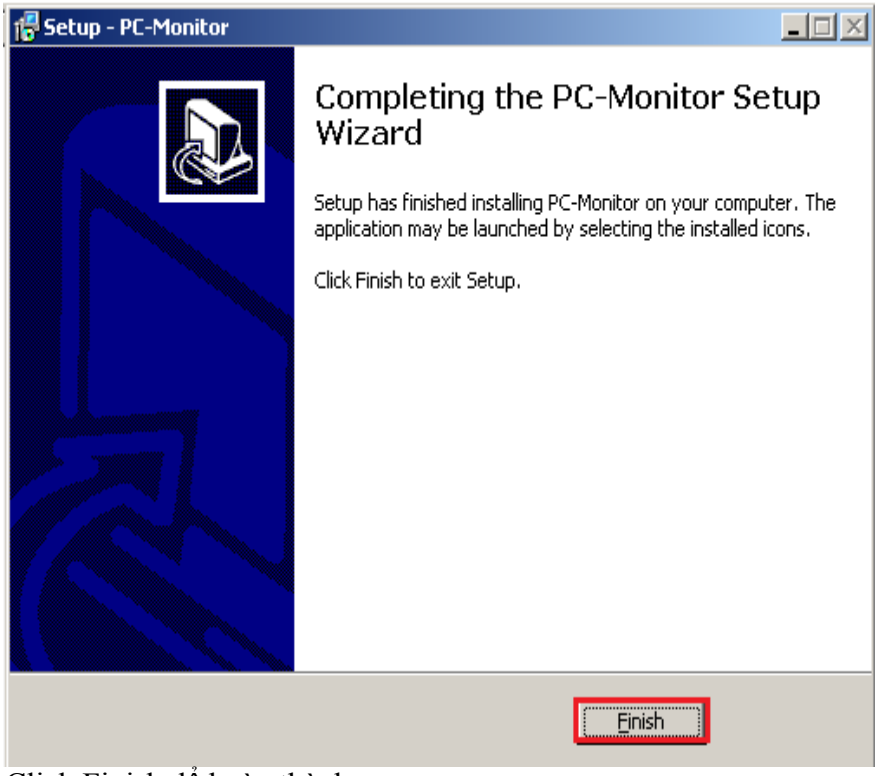
Click Next



Click Next



Click Install



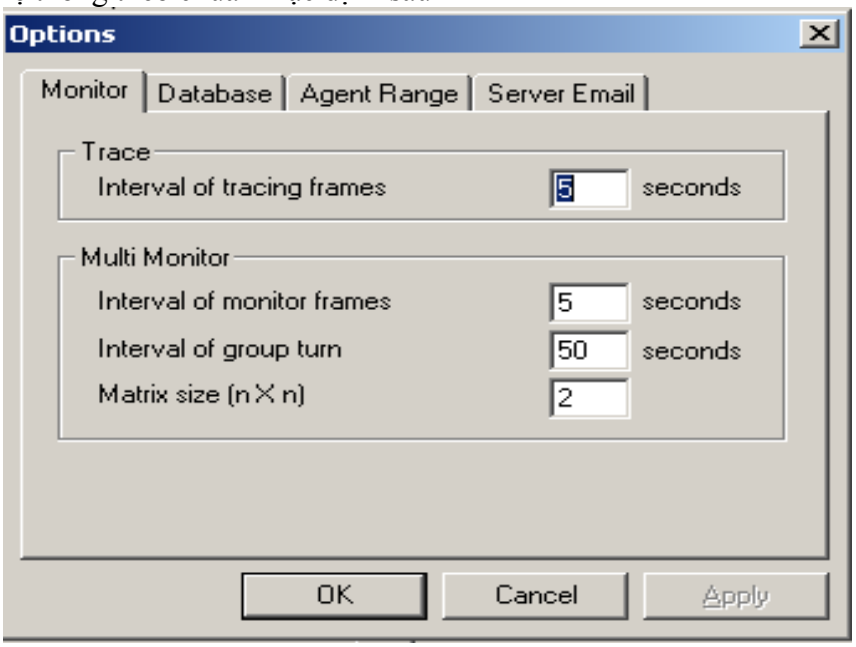
Click Finish để hoàn thành

- **Cài đặt PC Monitor Agent**

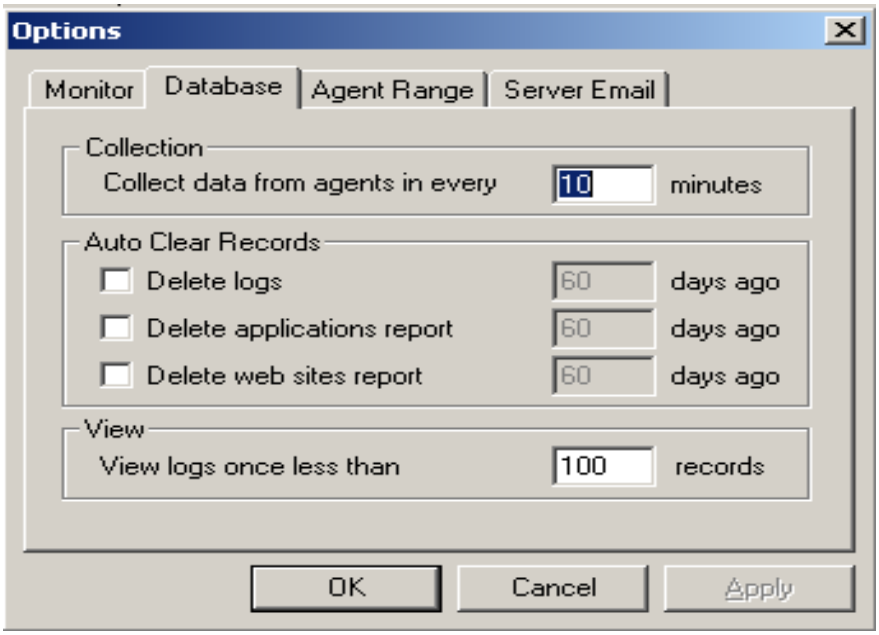
Tương tự như cài đặt trên máy server, trên máy Client chạy file Agent.exe và Next tiếp và hoàn thành với Finish.

- **Cài đặt hệ thống**

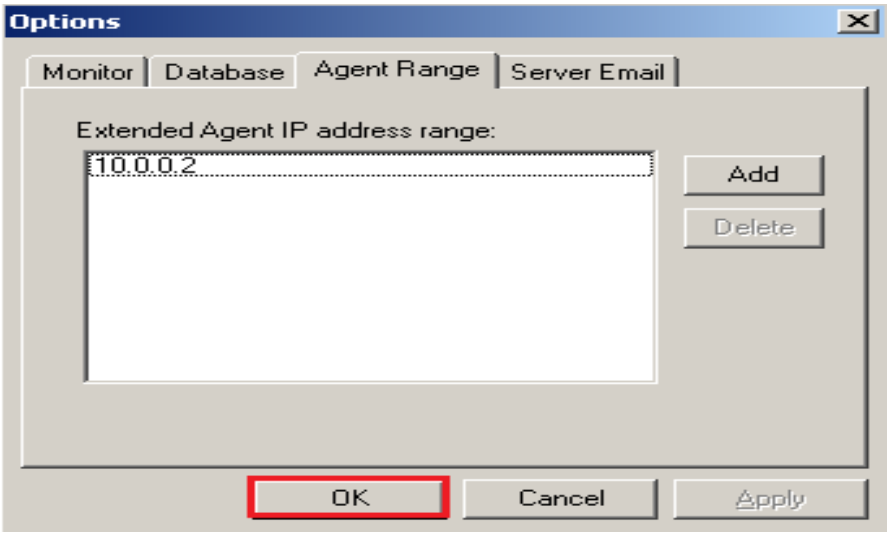
Cài đặt hệ thống theo chuẩn mặc định sau



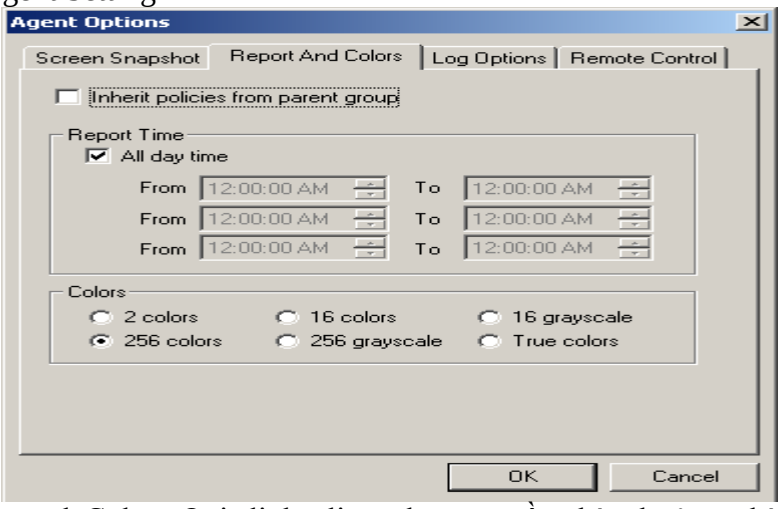
Vào File\System Option…



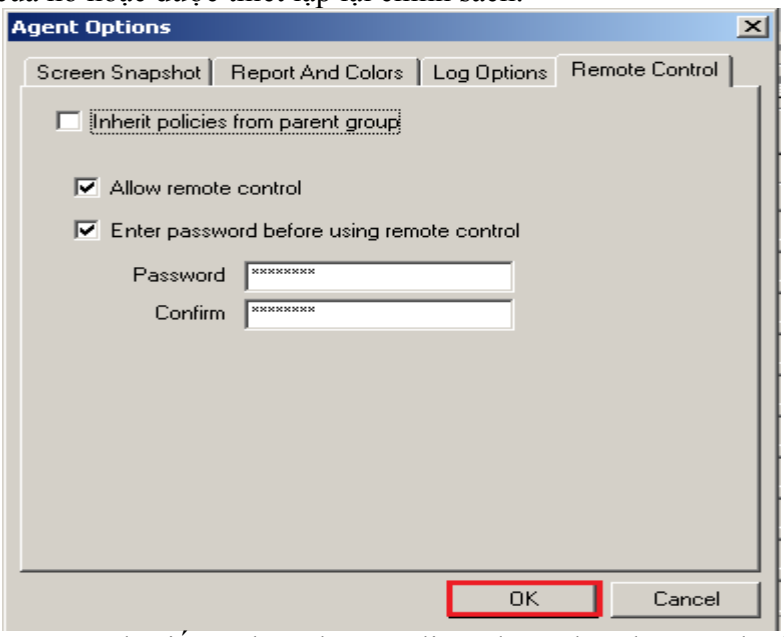
Trên tab Agent Range tìm 1 hoặc dãy địa chỉ IP của các máy Client cần điều khiển add chúng vào.



Vào File\Agent Setting



Tab Report and Color: Qui định client được quyền thừa hưởng chính sách từ nhóm cha của nó hoặc được thiết lập lại chính sách.



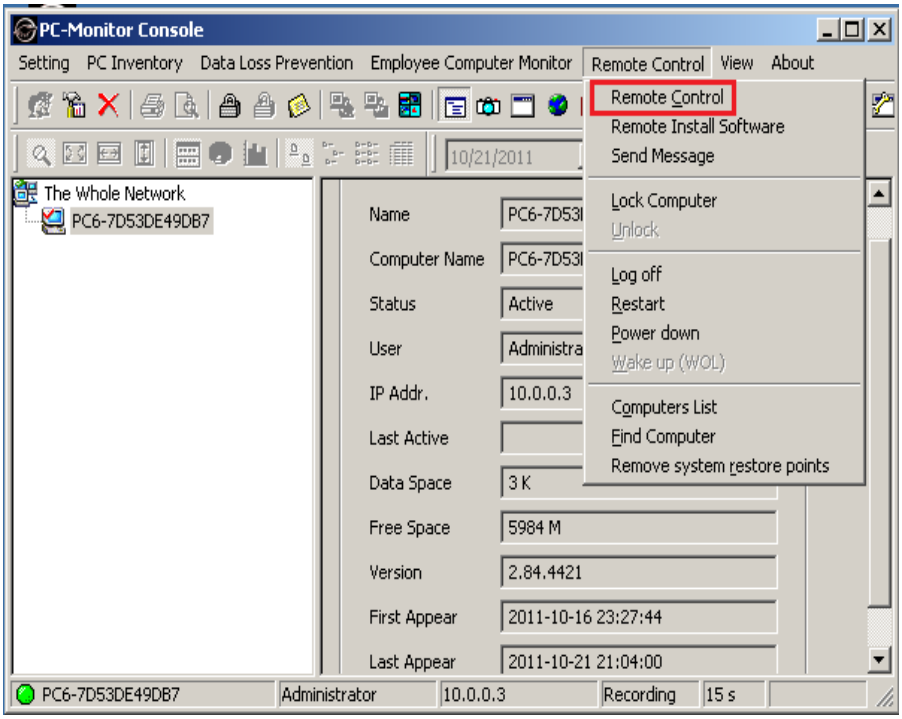
Tab Remote Control: giống như tab trên client được thừa hưởng chính sách của nhóm cha hoặc được thiết lập lại chính sách.

3. Tính năng

- **Hiển thị hành động của máy tính từ xa.**

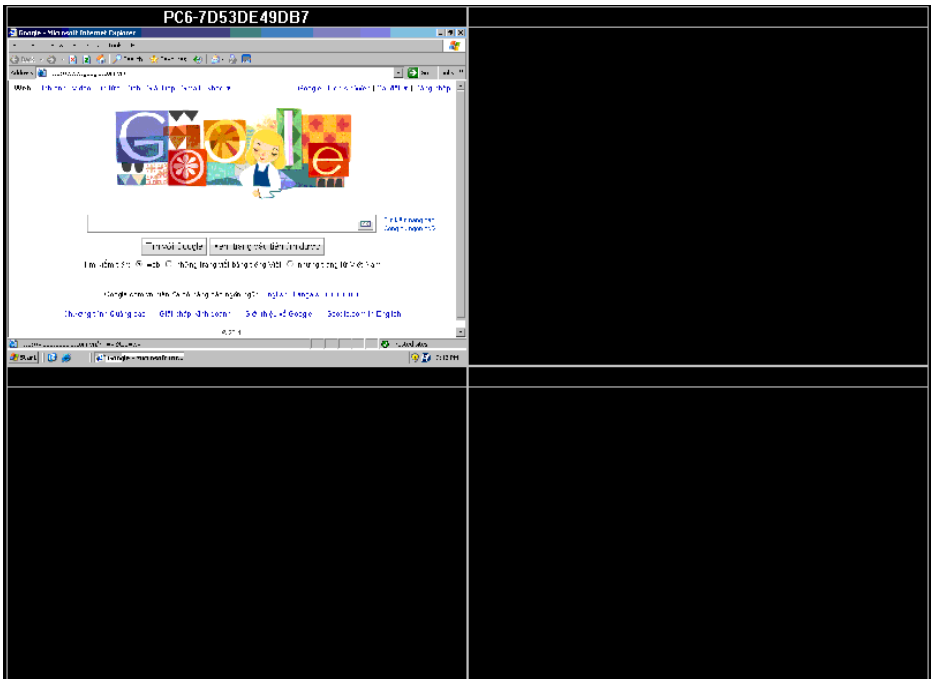
Trên máy Server ta sẽ theo dõi được Client đang làm gì

- **Điều khiển máy tính từ xa bằng chuột và bàn phím**

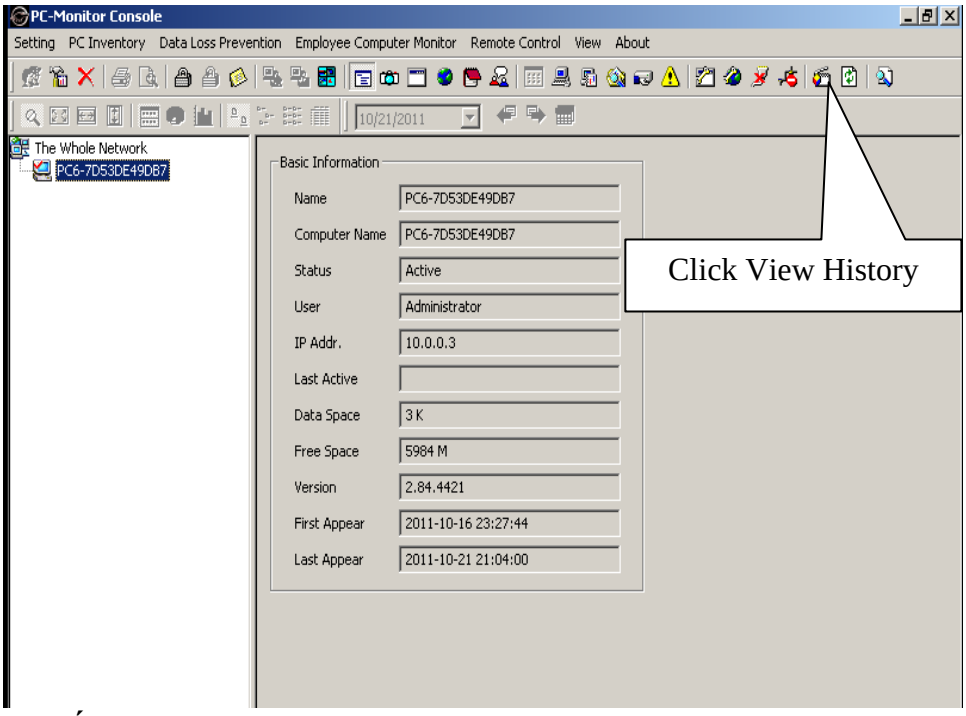


Vào tab Remote Control, sau đó Click Remote Control

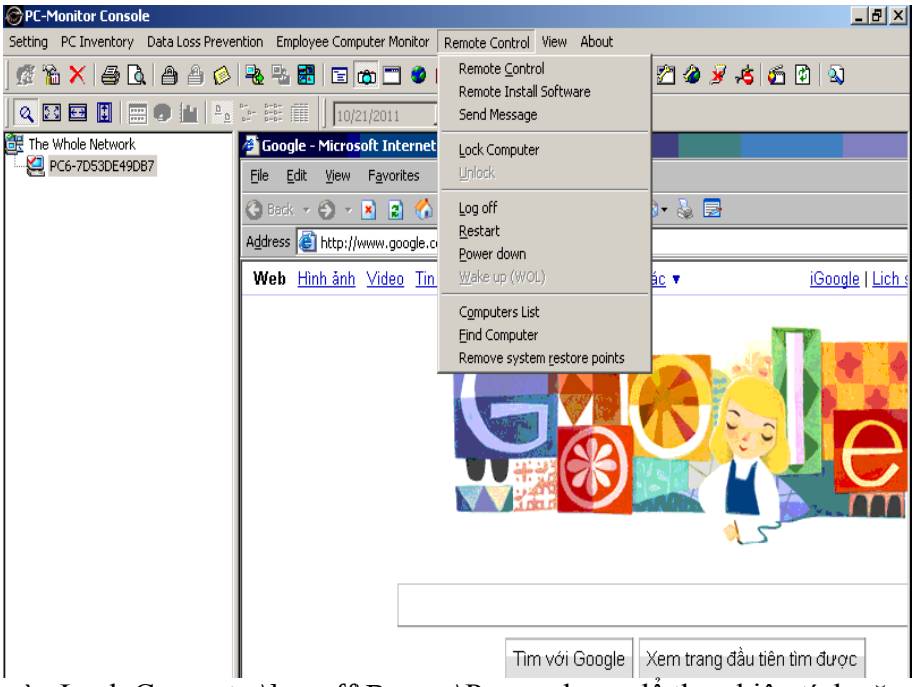
- **Nhiều màn hình từ xa có thể hiển thị trên màn hình.**



- **Tự động ghi màn hình các máy Client khi cần thiết máy chủ có thể mở lại để xem**

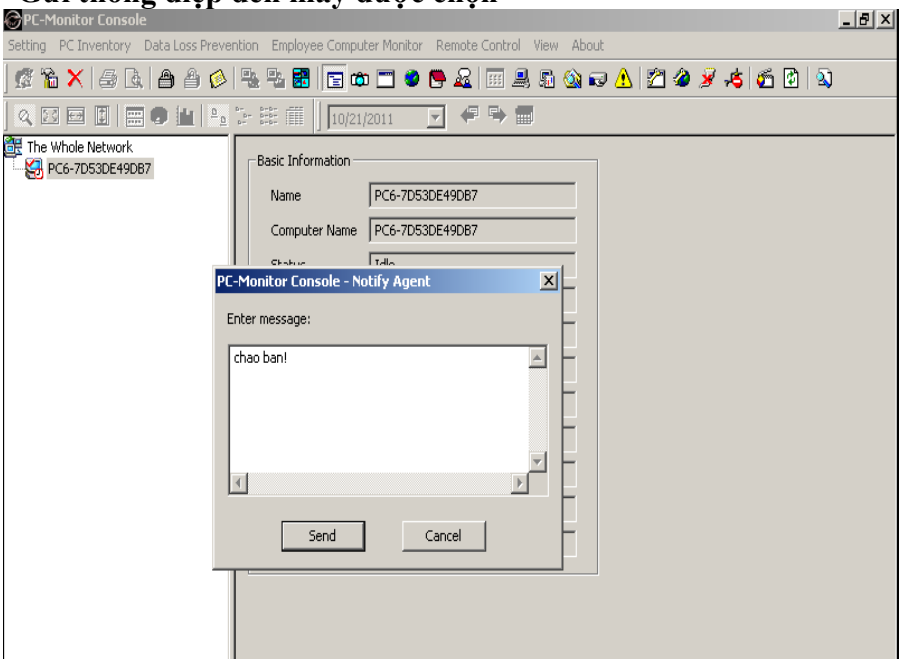


- **Tắt máy, khóa máy, khởi động lại, ngừng máy mạng từ xa**

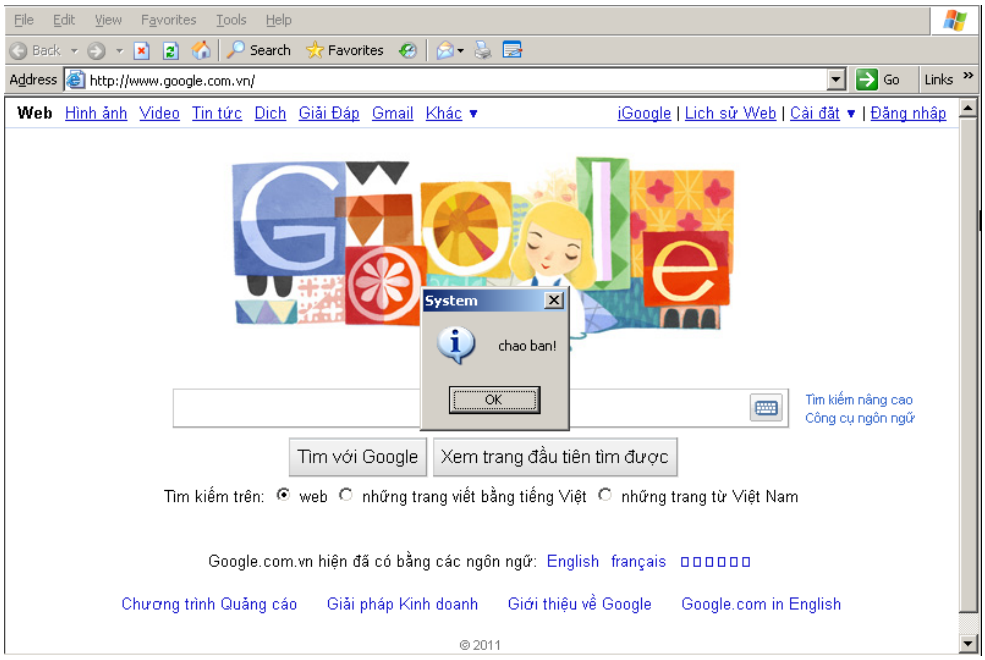


Chọn vào Lock Computer\log off\Restart\Power down để thực hiện tính năng trên

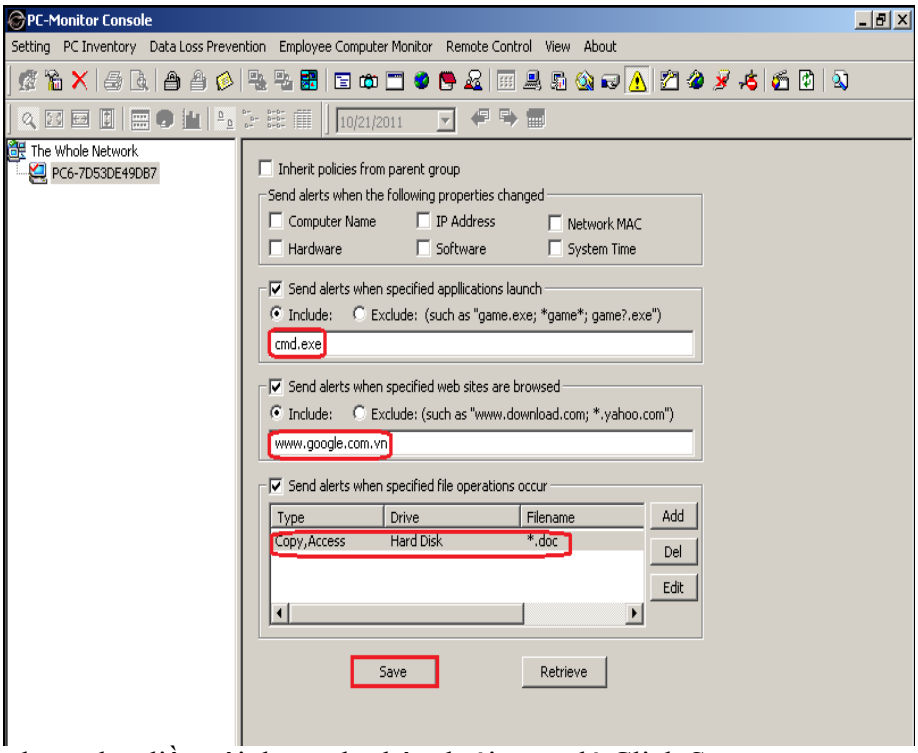
- **Gửi thông điệp đến máy được chọn**



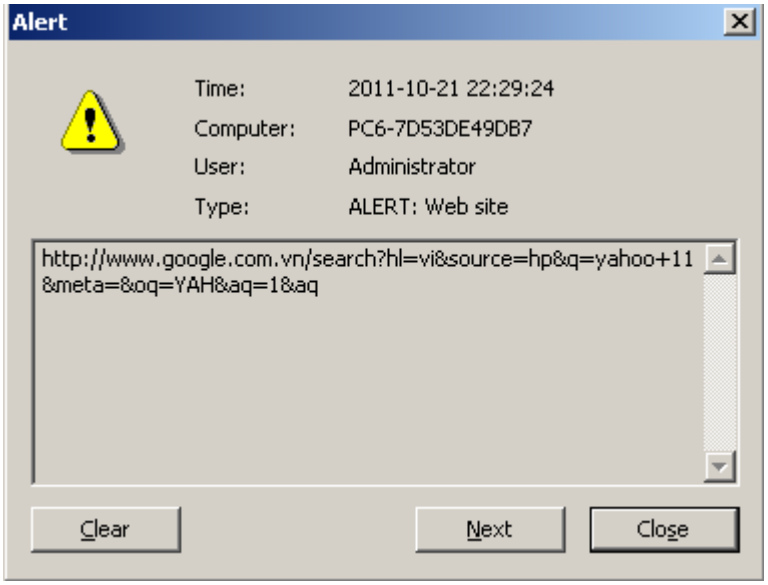
Nhập thông điệp, sau đó Click Send



- **Gửi thông báo khi client truy cập vào ứng dụng, web site và file đã được qui định**



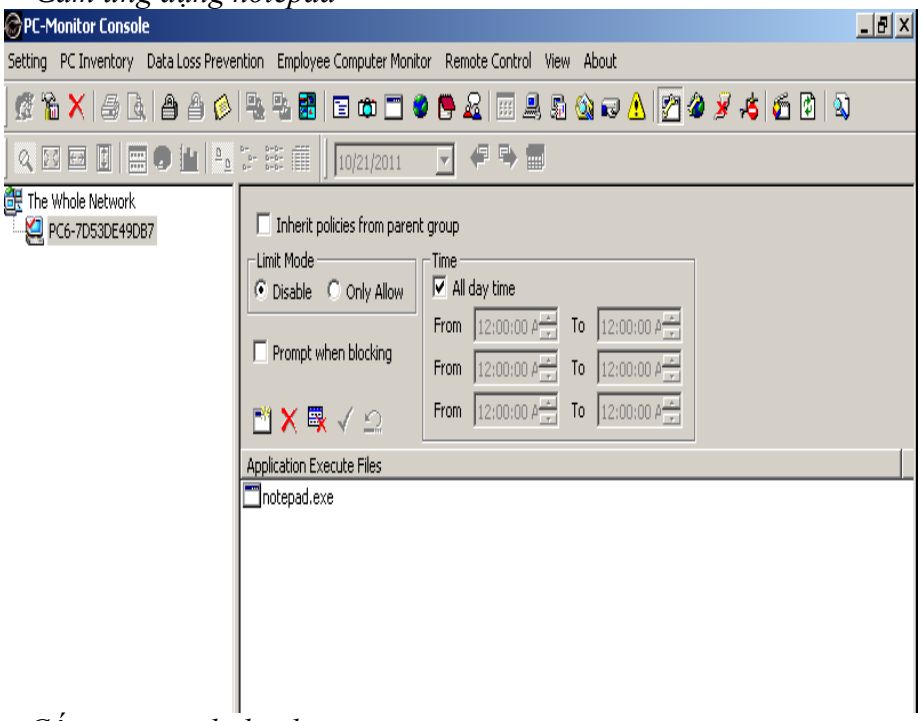
Click alert rules điền nội dung như bên dưới , sau đó Click Save



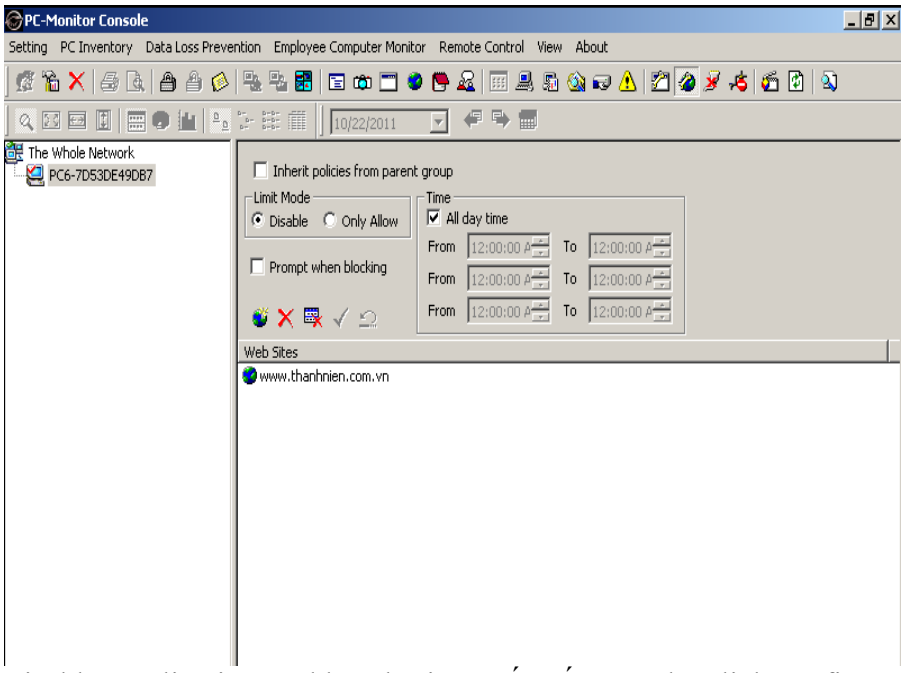
Xuất hiện hội thoại thông báo

- **Cấm trang web site và cấm ứng dụng**

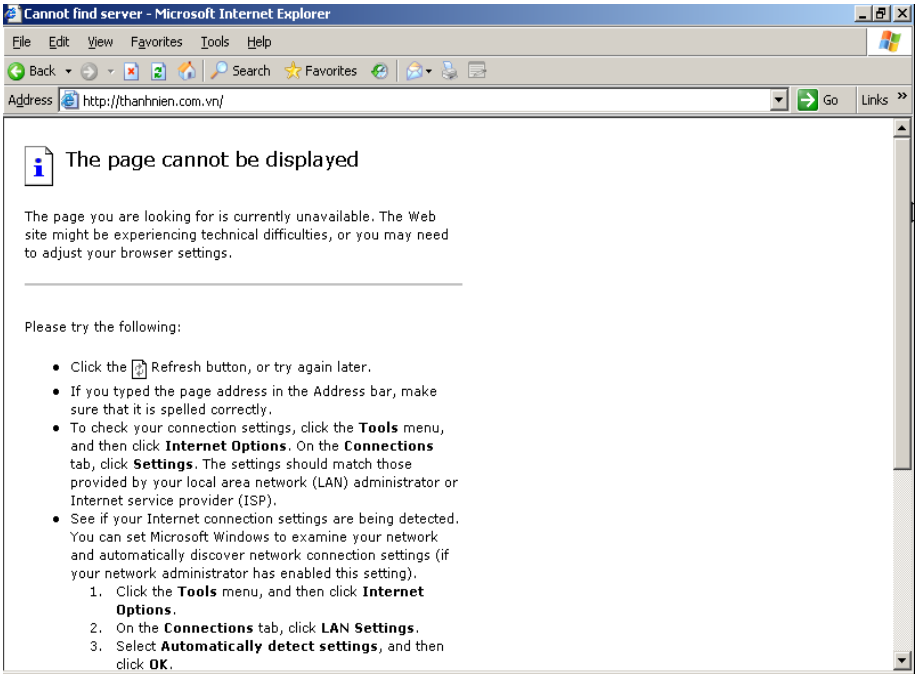
Cấm ứng dụng notepad



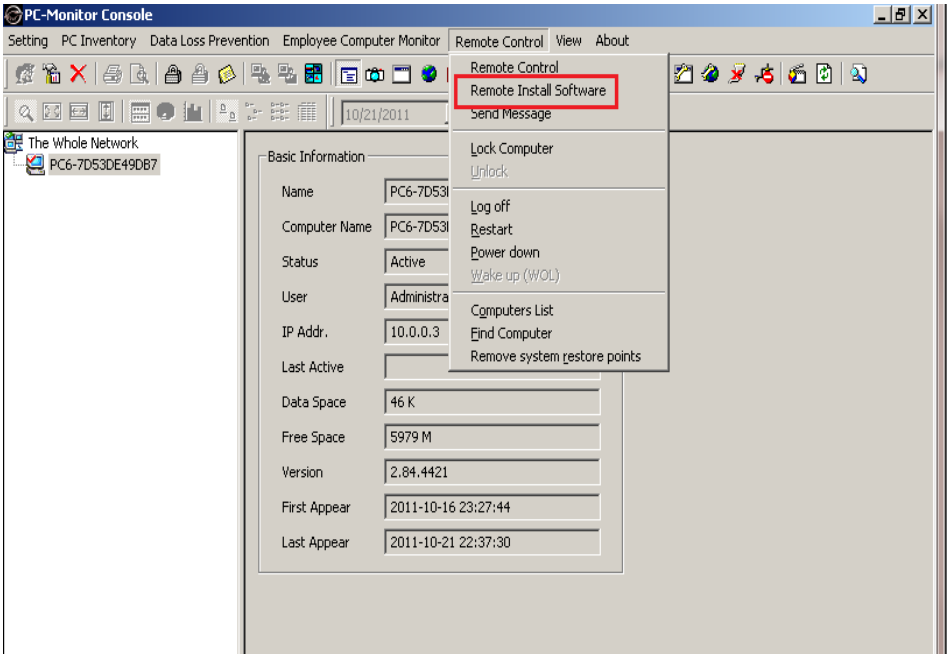
Cấm trang web thanhnien.com



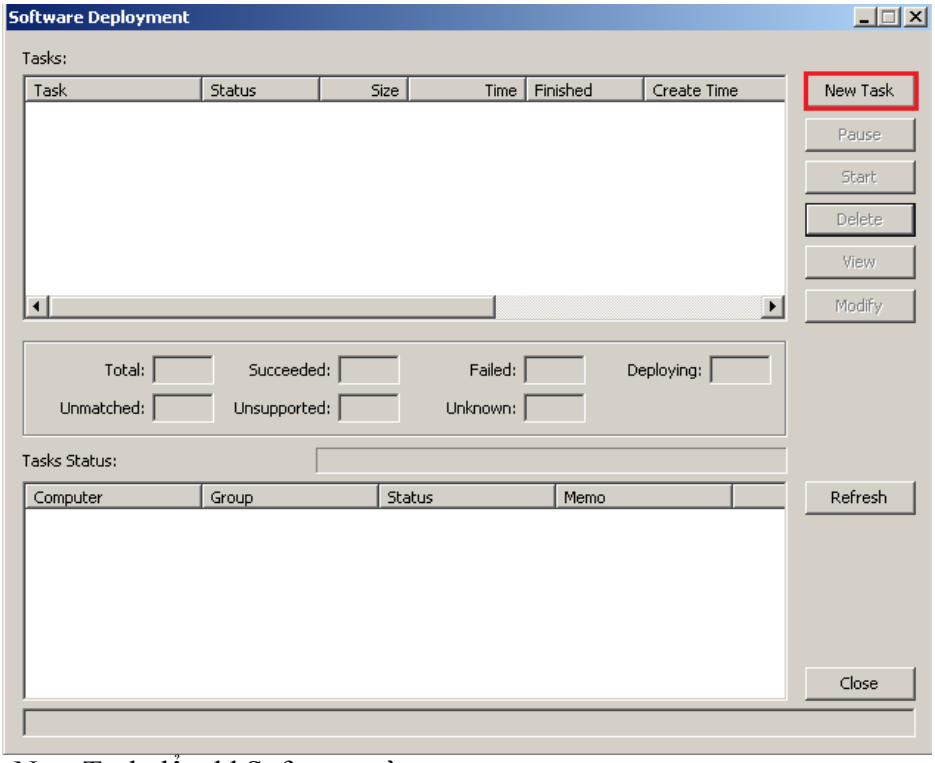
Click Disable Applications, add Web Site muốn cấm sau đó Click confirm



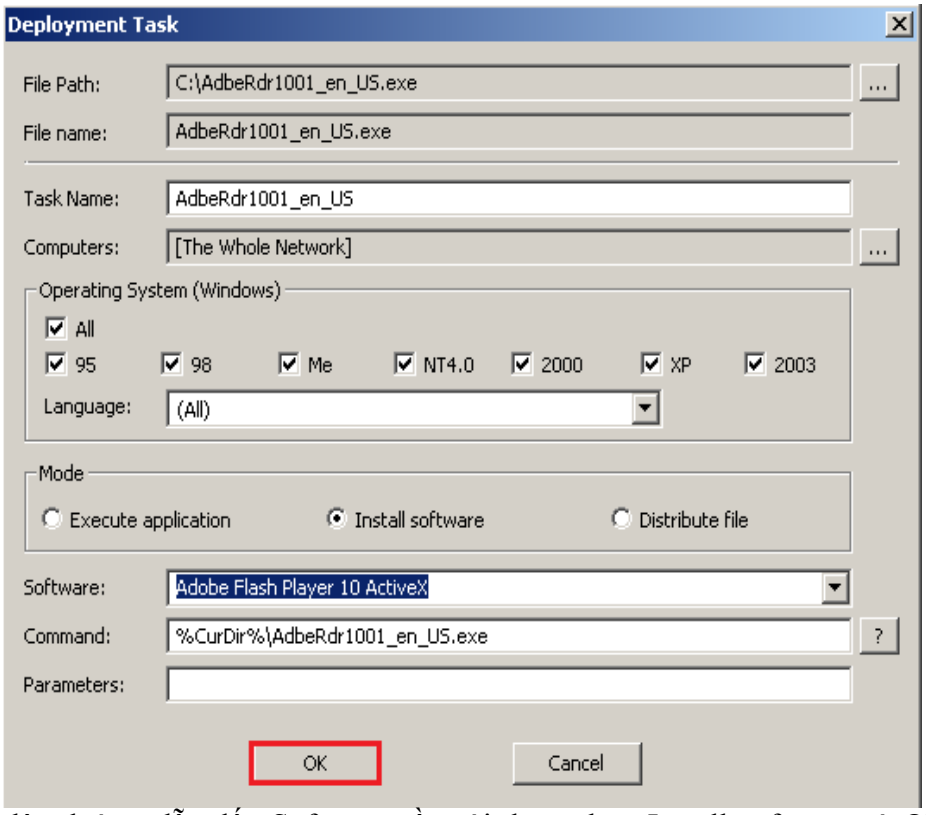
- **Cài đặt Software từ xa**



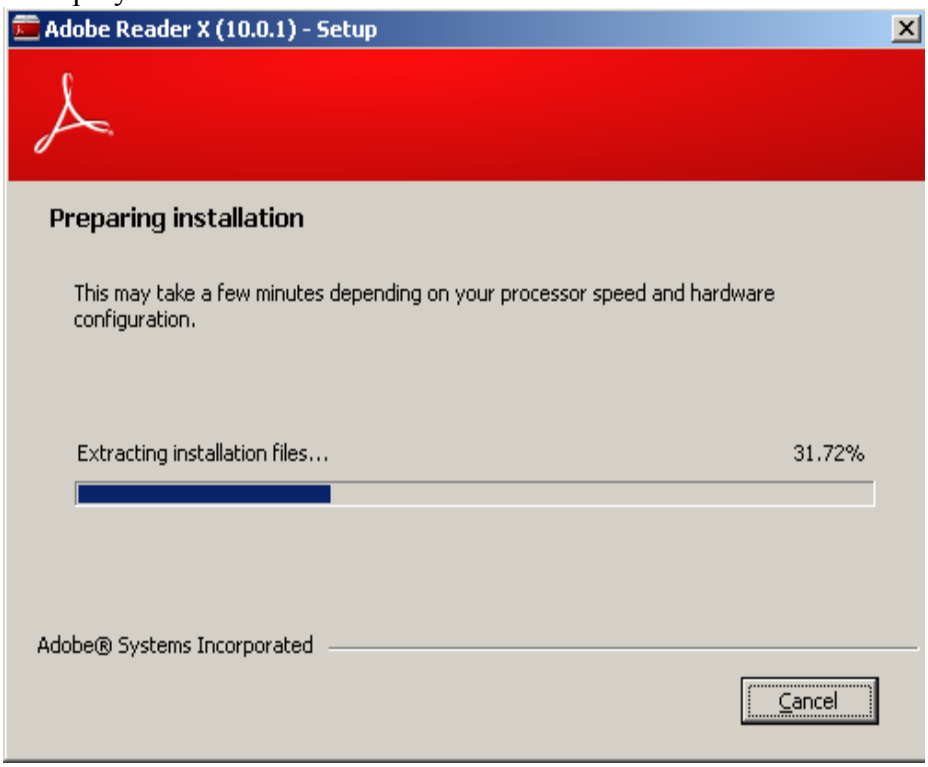
Vào Tab Remote Install Software…



Chọn New Task để add Software vào…



Thiết lập đường dẫn đến Software cần cài đặt…chọn Install software và OK để bắt đầu Deploy cho các client.



CHƯƠNG IV : Tổng quan về Mdaemon

1. Khái niệm

Mail Server là máy chủ dùng để nhận và gửi mail.

Mdaemon Là phần mền quản lý thư điện tử chạy trên window và được thiết kế có thể sử dụng từ sáu account đến hàng nghìn account. MDaemon rất đơn giản và dễ cấu hình, đồng thời là một phần mền có giá thành rất hợp lý như lại có rất nhiều đặc tính cho phép dễ quản lý hơn các hệ thống thư điện tử khác trên thị trường.

2. Công dụng

- Groupware Functions in MDaemon (Chức năng làm việc nhóm trong Mdaemon)

Tính năng nhóm của MDaemon đã đến với cả những đặc tính mới và nâng cao được thiết kế để hỗ trợ các công việc cần sự cộng tác. Được tích hợp vào trong WorldClient web mail platform của MDaemon, khả năng làm việc nhóm này cho phép người dùng chia xẻ các calendar, contact, task list và email messages, cộng với bất kể những gì người dùng có thể đặt vào trong các thư mục email cá nhân. Lịch làm việc được cập nhật cho phép người dùng thiết lập chính xáccác cuộc hẹn và các sự kiện định kỳ hàng ngày , hàng tuần, hàng tháng và hàng năm nữa. Người dung cũng có thể thêm vào danh sách những người được mời tham dự một cuộc họp và gửi giấy mời đến họ, tất cả từ thư mục lịch làm việc. Nói tóm lại, chức năng lập lịch biểu của WorldClient khiến cho việc quản lý thời gian của người dùng nhanh và dễ dàng hơn.

- Sender Policy Framework in MDaemon 7.1+

Những địa chỉ email giả mạo sẽ thúc đẩy gia tăng nhanh sự lan tràn thư rác và những virus khi ẩn giấu sự nhận dạng thực sự của những kẻ phải chịu trách nhiệm trong việc này. Những kẻ giả mạo này sử dụng những địa chỉ email của người khác không hề được phép và những người này cũng không hề hay biết. Bằng cách này bất cứ ai cũng có thể gửi email giả mạo cho bất cú người nào. Bắt đầu từ phiên bản 7.1, MDaemon đưa ra SPF như một tuỳ chọn bảo mật. Sender Policy Framework (SPF) là một tiêu chuẩn mở của giao thức bảo mật được thiết kế để dò tìm những địa chỉ email giả mạo. SPF có thể xử lý các email được gửi đến theo trình tự ưu tiên để download các message, do đó nó tiết kiệm thời gian xử lý và băng thong cho người dùng.

- Address Book Sync

Việc triển khai một hộp địa chỉ dùng chung cho tất cả những người dùng của một email domain cung cấp những thuận lợi như sự nhất quán và hiệu quả của việc duy trì tập trung nguồn thông tin. Sổ địa chỉ dành của Mircosoft Outlook và Outlook Express dành cho những ứng dụng chỉ định cụ thể thường không hỗ trợ việc chia sẻ thông tin với những gói phần mềm khác. Dành cho dịch vụ web mail WorldClient của nó, MDaemon 6.5 giải quyết vấn đề này bởi việc sử dụng công nghệ chuẩn XML cho sổ địa chỉ dung chung. Bằng việc sử dụng công cụ ComAgent miễn phí của MDaemon, mỗi người dùng Windows có thể đồng bộ giữa thông tin liên hệ của cá nhân họ với những sổ địa chỉ Outlook (MAPI) hoặc Outlook Express (WAB) và XML. Điều đó có nghĩa là thông tin liên hệ dành cho máy khách email chạy trên nền Windows và email dựa trên nền web WorldClient là như nhau.

- Calendaring Group Scheduling (Lịch Group Scheduling)

MDaemon Calendar kết hợp các chức năng của personal calendar và wall calendar vào một gói, điều đó tốt hơn là để cả hai tồn tại riêng rẽ. Bởi vì phần mềm lịch này thuận tiện và dễ dàng sử dụng, nó thích hợp để nhìn thấy hoạt động thực tiễn của nhóm hơn là những hoạt động của người dùng trước trên một tờ giấy . Hơn nữa nó gắn kết để chuẩn hoá với các sự điều hành nội bộ của các hệ thống khác.

- Content Filtering (Lọc nội dung)

Chức năng lọc nội dung trên server chắc chắn rằng nội dung trên server đã được lọc. Khả năng lọc của MDaemon có nhiều loại khác nhau, dễ dàng thay đổi và dễ dàng học để sử dụng. Những người gửi, người nhận và người quản trị có thể nhận được thông báo cho những hoạt động lọc qua những message cá nhân chi tiết. Chức năng lọc có thể giảm bớt những chi phí phân phát email bằng việc loại trừ và giảm bớt những message không mong đợi để giảm thiểu việc sử dụng băng thông.

- Email Gateways

Cổng giao tiếp email sẽ tập hợp, lưu trữ và chuyển tiếp các message đến một domain server sơ cấp. Một cổng giao tiếp điển hình không có những trương mục cá nhân. Những cổng giao tiếp email có thể giúp cả doanh nghiệp lớn và nhỏ giải quyết những vấn đề phải tiếp nhận từ các dịch vụ Internet email. Dành cho những tổ chức nhỏ, một cổng giao tiếp có thể làm một email domain cá nhân được thoả mãn. Điều đó có thể đạt được là vì nhà cung cấp dịch vụ sẽ cung cấp một cổng giao tiếp với một chi phí hợp lý khi chia sẻ phần cứng và phần mềm cho những người dùng nhỏ hơn. Những domain sơ cấp trong những trường hợp như vậy có thể có cả những đường kết nối thường trực và đường kết nối dialup tới Internet . Với sự thiết lập lớn hơn có thể sử dụng các cổng giao tiếp làm nhiệm vụ nhiệm vụ bảo mật phức tạp hơn khi cung cấp một sự bảo vệ và lọc nội dung cho những hệ thống mail dễ bị tổn thương hơn khi bị tấn công. Các cổng giao tiếp cũng có thể được cấu hình để cung cấp việc sao lưu phục hồi và chứa dữ liệu của email theo thời gian thực khi một domain sơ cấp offline vì bất kể lý do nào Một bản sao của MDaemon có thể điều hành đồng thời nhiều cổng giao tiếp của nhiều email domain thậm chí ngay cả khi đang điều hành domain server sơ cấp của chính nó.

- MDaemon Standard vs. Pro

MDaemon có hai phiên bản - Standard và Pro. MDaemon Standard giới thiệu một dịch vụ email cơ bản được xây dựng trong phạm vi một SMTP server để truyền mail, và một POP3 server để phân phối các message đến người dùng. Phiên bản Pro có thêm các tính năng đẳng cấp cao hơn dành cho người quản trị và những người đăng ký sử dụng email

- Public Folders Concepts and Applications (Khái niệm thư mục công cộng và các ứng dụng)

Các thư mục email dùng chung thúc đẩy và làm cho việc chia xẻ các thông tin tập trung được dễ dàng. Các hộp thư đến của các nhóm thảo luận, các thông báo, và các nhóm làm việc chung được hỗ trợ bởi các thư mục dùng chung email Các thư mục dùng chung có thể được mở cho bất kỳ ai với một trương mục người dùng được hỗ trợ trên mail server. Việc truy cập cũng có thể bị hạn chế đối với những nhóm nhỏ hơn. Trạng thái đánh dấu của message trong các thư mục dung chung có thể được yêu cầu cho mỗi người dùng hoặc được chia xẻ cho tất cả các thành viên của nhóm. Người quản trị email tạo

những thư mục dùng chung và qui định các quyền hạn truy cập. MDaemon hỗ trợ các thư mục chung dành cho email. Khi đượcánử dụng cùng với InsightConnector, các thư mục dùng chung cũng có thể được sử dụng cho Outlook Calendar và chia sẻ tài liệu trực tiếp. Thu mục Email dung chung là một tính năng của các máy chủ Internet Message Access Protocol (IMAP – Giao thức truy cập thư tín internet).

- Security Tools for Spam Control (Công cụ bảo mật kiểm soát thư rác)

Những tin nhắn không được yêu cầu gửi đến - Unsolicited Bulk Email (UBE), cũng bị coi như là thư rác, tiêu tốn của các doanh nghiệp và cá nhân hàng tỷ đô la mỗi năm Nó làm tiêu tốn thời gian và những nguồn lực trong khi các tài nguyên này thì lại bị giới hạn hay có giá trị. Một trong những công cụ chính của những kẻ tạo thư rác là sử dụng không phép server của bên thứ ba không liên quan với chức năng chuyển tiếp email mở. Điều đó có nghĩa là bất kỳ ai cũng có thể gửi một email thông qua server này đến một người khác thậm chí ngay cả khi người gửi và người nhận đều không có một trương mục trên server này. Thư rác cũng có thể đến từ nhiều người dùng được chứng thực với những trương mục trên server. Để giúp đỡ việc ngăn chặn thư rác, những email server hiện đại phải được cấu hình với các tuỳ chọn để chặn những kẻ thứ ba không liên quan chuyển tiếp thư ráåttí phép qua server cũng như kiểm soát việc truy cập bằng nhiều những công cụ khác nữa. Những tất cả những công việc này cũng vẫn tiếp tục phải cho phép người dùng hợp lệ gửi và nhận mail từ những vị trí từ xa. MDaemon bao gồm những lựa chọn được yêu cầu này để chặn việc chuyển tiếp email trái phép, trong khi cho phép người dùng sử dụng server từ bất kỳ một vị trí nào trên thế giới. Một sự thiết lập server để chống lại thư rác cũng bảo vệ hệ thống thoát khỏi nhiều kiểu tấn công khác nhau bao gồm cả việc bẻ khoá đột nhập vào hệ thống.

- MDaemon GroupWare (an alternative to MS Exchange(một thay thế cho MS Exchange))

MDaemon GroupWare cho phép doanh nghiệp sử dụng tất cả các chức năng groupware của Microsoft Outlook mà không phải chịu chi phí của Microsoft Exchange Server. Công việc kinh doanh, các tổ chức từ thiện, trường học, và các cá nhân sử dụng Outlook bởi các công cụ thiết thực của nó trong việc quản lý thời gian, liên lạc, tài liệu và email. Tuy nhiên hầu hết các đặc tính tốt nhất của Outlook - bao gồm cả việc chia xẻ thông tin - chỉ làm việc đầy đủ khi đươ9ực kết hợp với Microsoft Exchange, một phần mềm email server. Dành cho những tổ chức vừa và nhỏ, Microsoft Exchange trở nên quá đắt về những yêu cầu cho phần cứng, phần mềm và giấy phép của nó, thêm vào đó là đòi hỏi cao cho sự đào tạo đối với người quản trị hệ thống. MDaemon GroupWare đã giải quyết vấn đề này khi đưa ra tập hợp các tính năng hoàn chỉnh của Outlook, bao gồm cả chức năng chia xẻ. MDaemon GroupWare là một phần mềm ứng dụng khách/chủ với những thành phần trên cả MDaemon server và trên máy trạm. Chúng cho phép chia xẻ các thư mục của Outlook, calendars và contacts và tất cả các "đối tượng" khácủa Outlook nữa. Chúng cho phép các công ty sử dụng các tính năng hoàn chỉnh của Outlook với chi phí tiết kiệm và dễ dàng quản trị của MDaemon.

- Web Administration (Quản trị Web)

WebAdmin for MDaemon là một phần mềm quản trị email chạy trên trình duyệt web. Chúng cung cấp sự truy cập quản trị cho hầu hết các cấu hình hệ thống được sử dụng thông thường và các thiết lập trương mục người

dùng thông qua trình duyệt có thể sử dụng javascript. Thông qua việc quản trị web, người quản trị hệ thống có thể thay đổi các thiết lập cho domain sơ cấp, thêm vào domain thứ cấp bất kỳ. Nó bao gồm trương mục quản trị trong tất cả các domain. Một trong những thuận lợi chính của công việc quản trị teen trình duyệt web là cho người quản trị domain các quyền dành cho việc cấu hình các domain và trương mục người dùng của domain. Thêm vào đó, người dung trương mục cá nhân có thể thay đổi nhiều sự thiết lập cho họ. Cả người quản trị domain và hệ thống có thể điều khiển bất cứ ai có khả năng thay đổi bất kể những gì thông qua sự thiết lập mặc định và tùy biến bên trong domain của họ

- Fax Management (quản lí Fax)

Máy chủ fax đặt một digital spin trong công nghệ analog tuy đã cũ nhưng đáng tin cậy. Nó gửi và nhận fax giữa các máy tính cá nhân trên mạng LAN, WAN hoặc Internet. Nó cho phép người sử dụng chia xẻ máy fax hoặc fax modem hoặc cả hai nếu chúng có thể truy cập được qua mạng. RelayFax tích hợp việc gửi và nhận fax thông qua hầu hết các email server, bao gồm cả email server của Alt-N MDaemon. Thông qua RelayFax, những người có quyền sử dụng email có thể gửi các email có đính kèm file đến mailbox và sau đó chuyển tiếp chúng như là gửi một bản fax tiêu chuẩn đến bất kỳ một thiết bị fax nào trên thế giới. RelayFax sử dụng công nghệ client/server, với server chạy trên nền tảng của phần cứng là mạng và máy trạm là máy tính cá nhân hoặc máy tính xách tay.

- IMAP and POP Summaries (Tóm tắt IMAP và POP)

POP3 và IMAP là hai cách truy cập email thông qua Internet. POP3, là phương thức của tổng hai phương thức, làm việc tốt với người dùng có một máy tính và muốn lưu trữ tất cả mail của họ trên máy tính đó. IMAP cung cấp ứng dụng bao gồm lưu trữ và xử lý mail trên server. IMAP làm việc tốt hơn tại những nơi có nhiều người dùng và nhiều máy tính và cần truy cập mail của họ từ bất cứ máy nào cũng như qua web. Tài liệu này sẽ giải thích cả hai giao thức và lý luận đơn giản cho sự cần thiết triển khai IMAP

- MDaemon AntiVirus

MDaemon AntiVirus là một phần mềm kiểm tra virus hoàn chỉnh, với khả năng tự động cập nhật cho các công cụ quét virus và những file định danh cho một virus đã biết. Khi được kết hợp với nhưng biện pháp phòng ngừa khác MDaemon AntiVirus có thể giảm bớt, hạn chế hoặc loại trừ sự xâm nhập của virus vào văn phòng của bạn. Nó cũng ngăn cản những virus tình cờ bị gửi đi đến những người khác trong hoạt động kinh doanh của bạn. Thêm vào các file định danh virus, MDaemon AntiVirus sử dụng phương pháp dò tìm heuristic, có thể kiểm tra email và những file đính kèm để phát hiện các đặc tính virus MDaemon AntiVirus là phần mềm plug-in chạy trên một dịch vụ độc lập dành cho MDaemon email server của Alt-N.

- Setting Up Email Catalogs (Thiết lập Catalogs Email)

Catalog thường được nhìn nhận như là một công cụ vô cùng hữu ích cho việc phân bố các tài liệu và các file. Catalog hoạt động nhanh được cấu trúc hoá và bảo vệ tốt hơn FTP servers hoặc HTTP servers . Chúng có thể chứa đựng các kiểu file từ hình ảnh, tài liệu cho đến các chương trình ứng dụng và script. E-catalog được thêm vào với đặc tính dễ sử dụng và thay đổi do đó nội dung luôn được cập nhật. MDaemon chứa đựng các công cụ dành cho việc tạo, sửa và xoá các catalog.

- Using ODBC with MDaemon 6.5 (Sử dụng ODBC với MDaemon 6.5)

Có thể duy trì những bản ghi trương mục người dùng trên MDaemon một cách dễ dàng nhưng các bản ghi đó có thể trở nên dư thừa. Việc dư thừa này có thể xảy ra nếu như doanh nghiệp cùng lúc giữ những thông tin được đưa vào máy tính về người lao động hay các email của khách hàng. Các bản ghi dư thừa sẽ làm lãng phí thời gian và thêm vào những rủi ro và mâu thuẫn giữa nhiều nguồn dữ liệu khác nhau. MDaemon 6.5 giải quyết các vấn đề này bởi việc cho phép các bản ghi trương mục người dùng được duy trì trên bất kỳ cơ sở dữ liệu nào với một giao diện Open Database Connectivity (ODBC) - Kết nối các hệ cơ sở dữ liệu mở. MDaemon 6.5 cũng có thể truy cập các bản ghi danh sách email thông qua một kết nối ODBC.

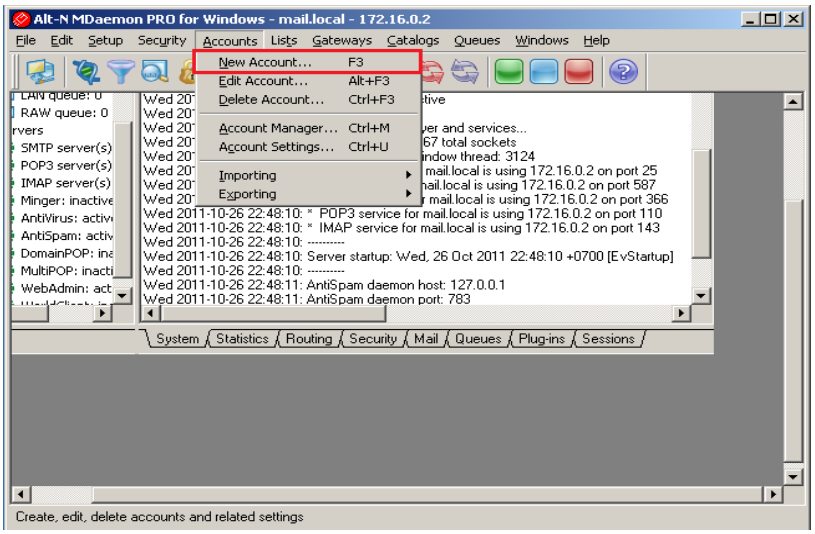
3. Cài đặt ứng dụng(Mdeamon mail server)

(Xem phần publish mail)

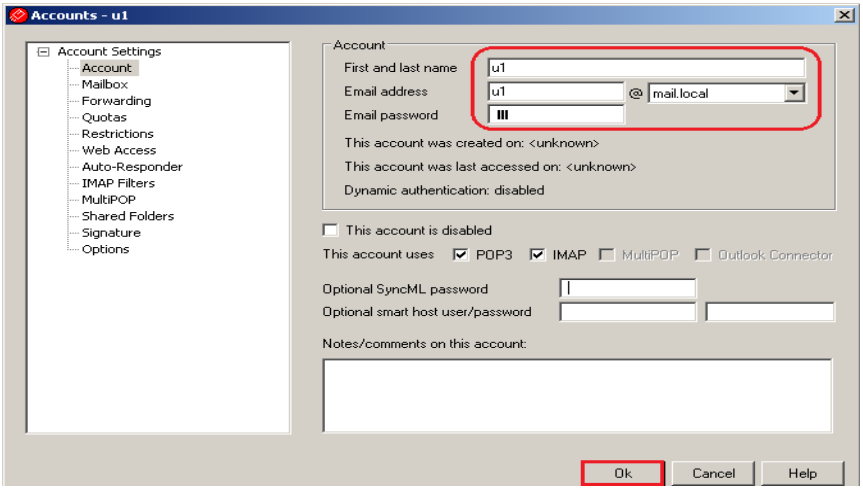
4. Chi tiết và điểm yếu,mạnh của các tính năng của Mdaemon

4.1. Gửi Mail giữa User – User và User-Group :

- *Tạo Account*



Chọn Accounts\ New Account…

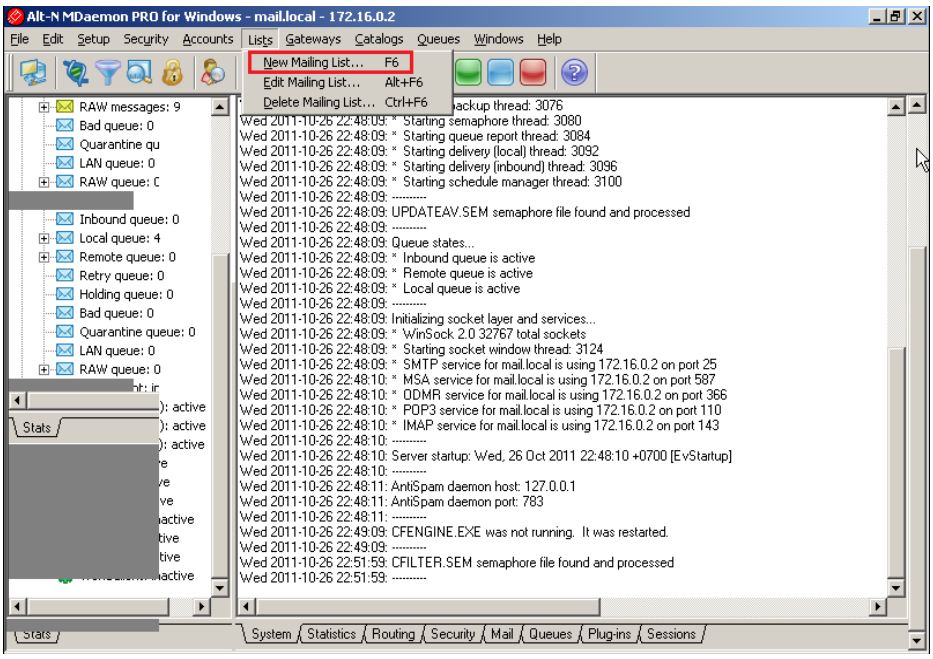


Tạo Account u1 như trên , sau đó kích OK để hoàn tất

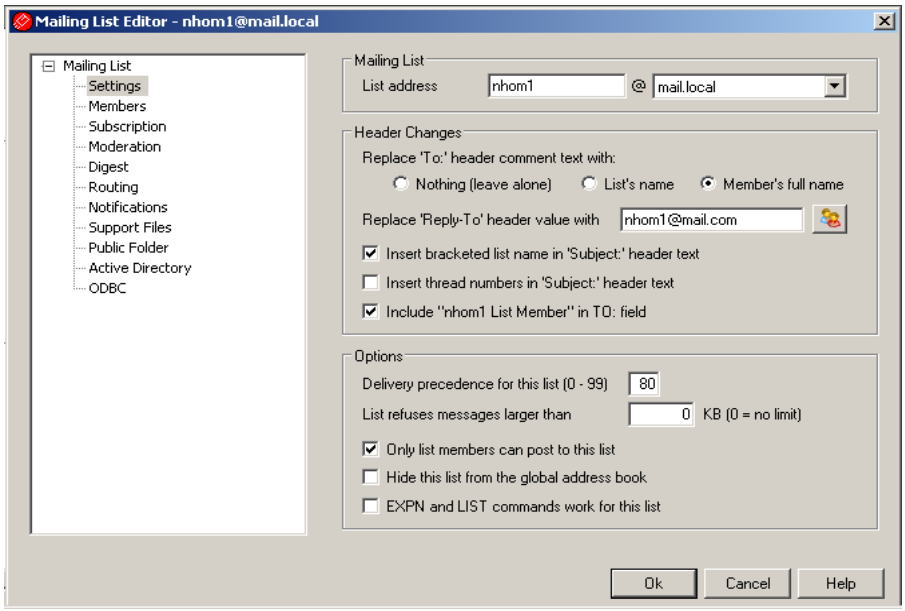
Tạo account khác cũng như vậy.

- *Tạo Mailing list*

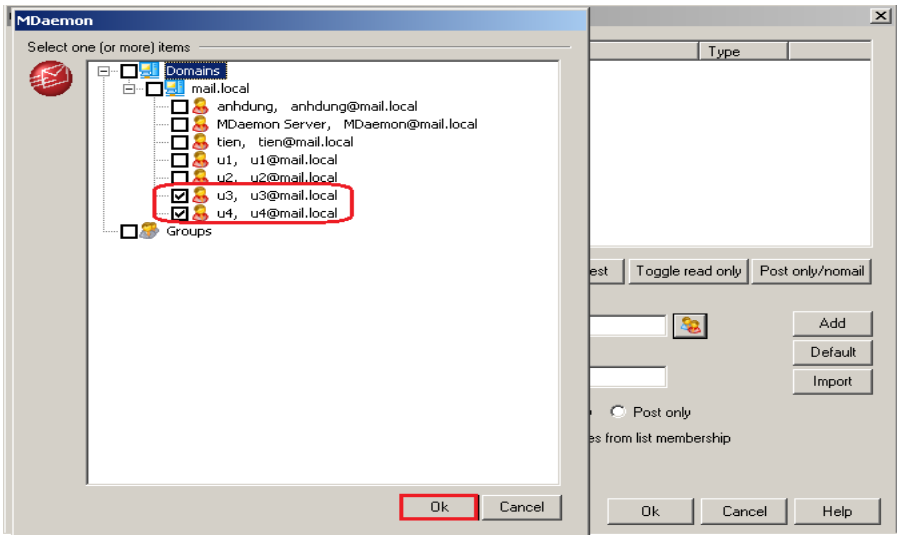
Mailing list còn gọi là email group hoặc distribution list. Mail list cho phép một nhóm người dùng được sử dụng trung một địa chỉ thư trung để bàn luận về một chủ đề nào đó. Khi có thư gửi tới mailing list thì sẽ đươc nhân ra và gửi đến các thành viên của list. Danh sách có thể là các địa chỉ hộp thư của người dùng tại máy chủ thư điện tử và các địa chỉ thư điện tử bất kỳ trên internet.



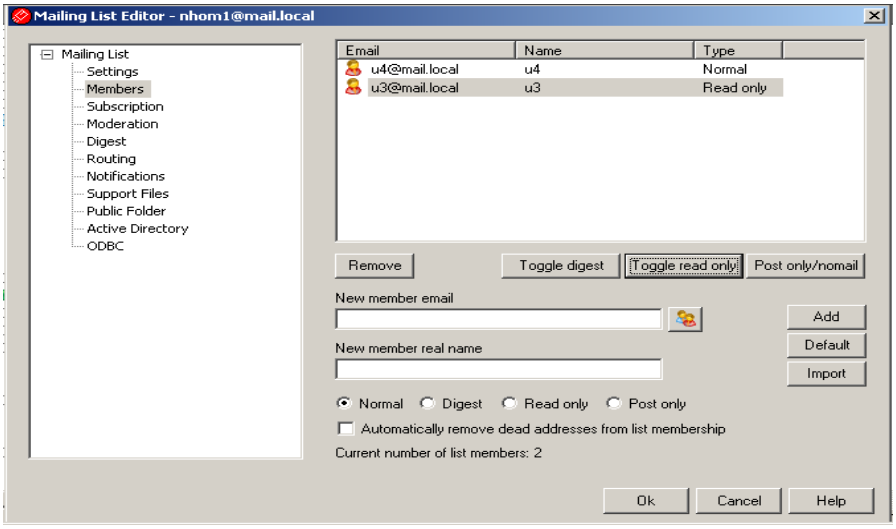
Click Lists\ New Mailing list…



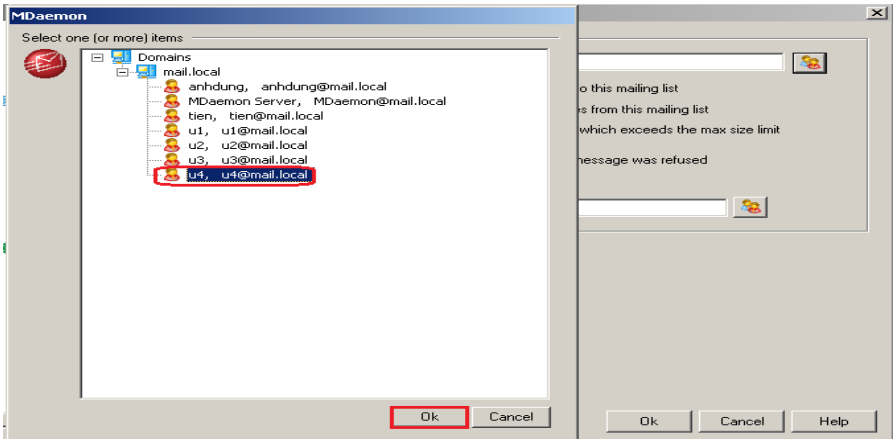
Click settings và điền thông tin như trên



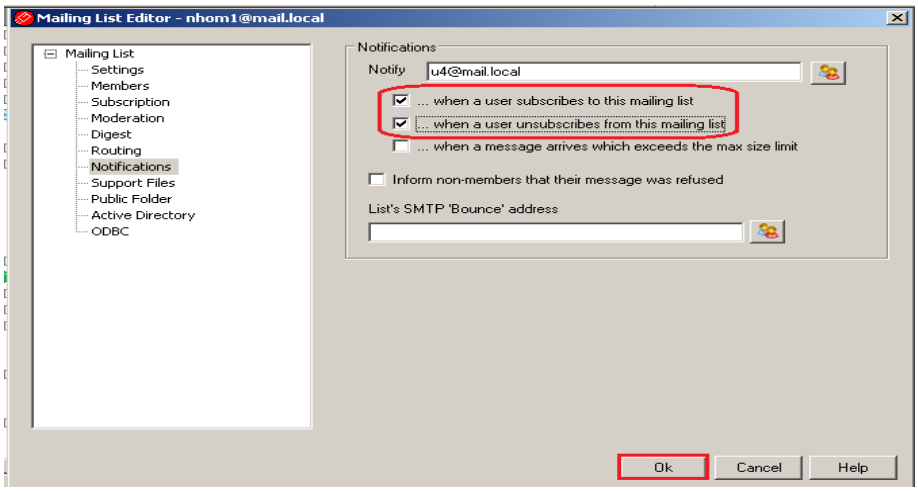
Click members\ nhấp vào biểu tượng 2 người\ chọn những account cần add vào Group\ click vào Ok để chấp nhận



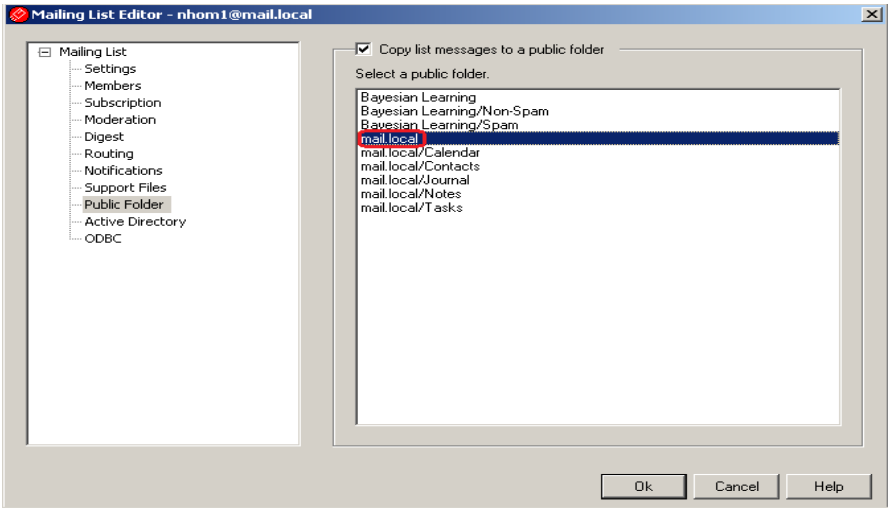
Chọn thông tin như trên



Click Notificatons\ nhấp vào biểu tượng 2 người phía trên\ chọn account cần add vào\ Click OK để chấp nhận

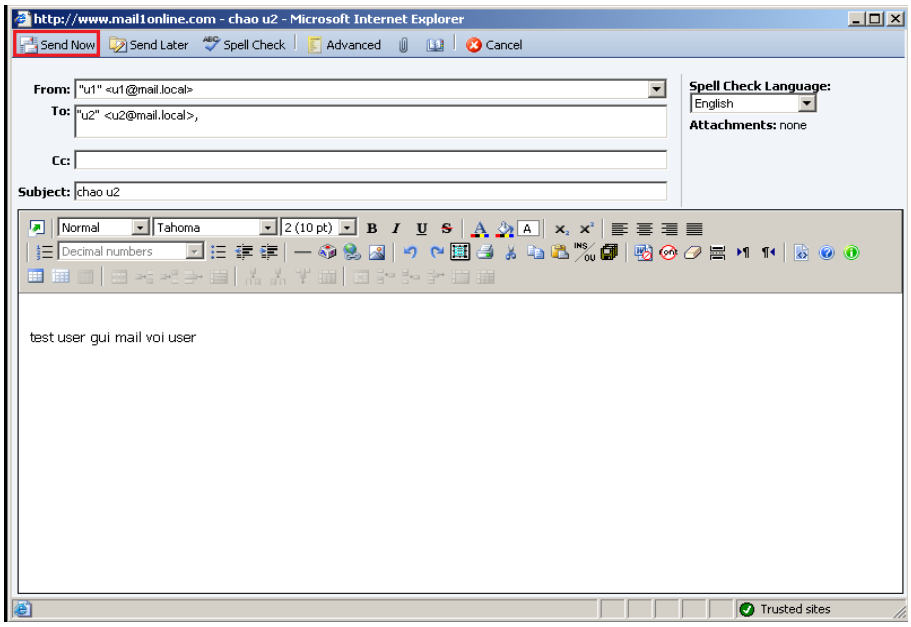


Chọn Options thư nhất và Option thứ hai



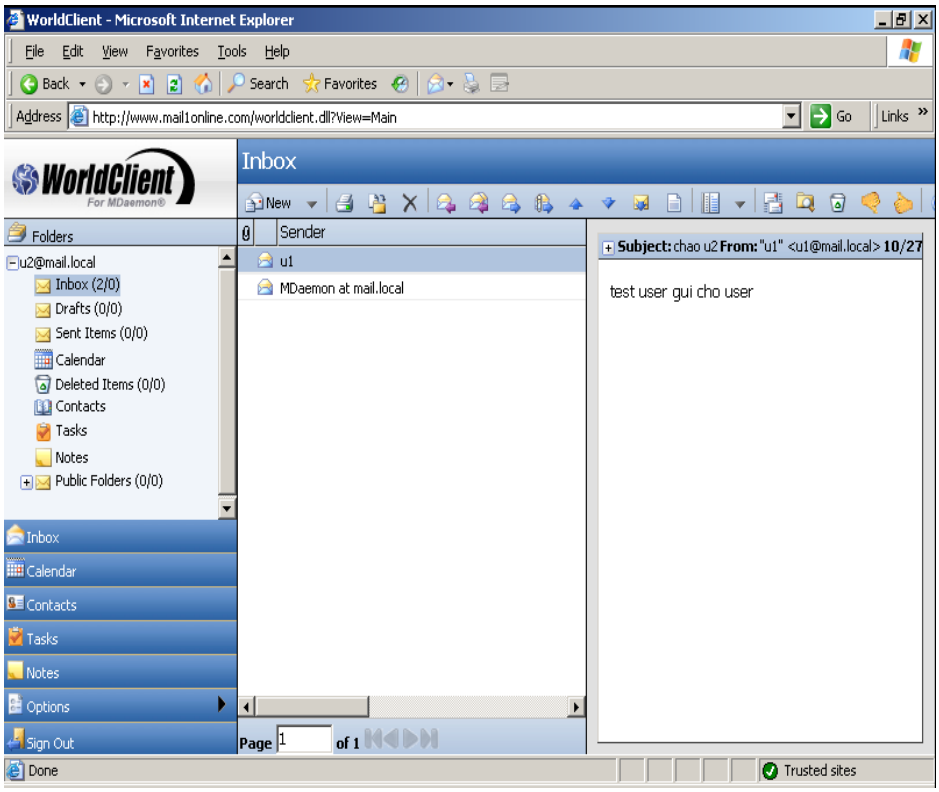
Click Public Folder\ chọn option copy list mssages to a public folder\ chọn citd-cantho.com\ click Ok để chấp nhận

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account u1 và sau đó Click Sign In để chấp nhận



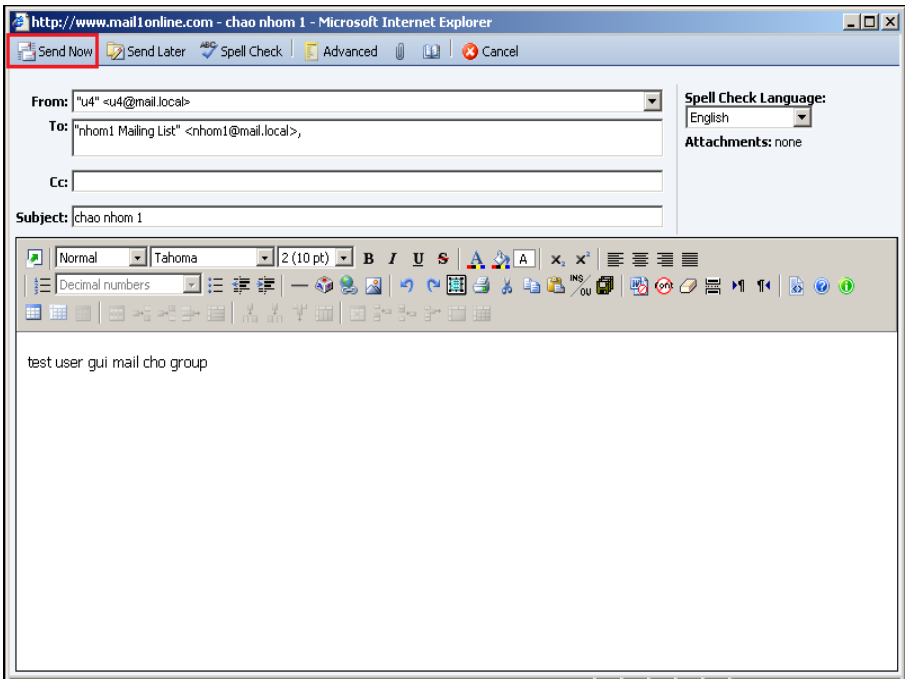
Click New và điền thông tin u1 gửi nhom1, sau đó click Send Now để gửi

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account u2 và sau đó Click Sign In để chấp nhận

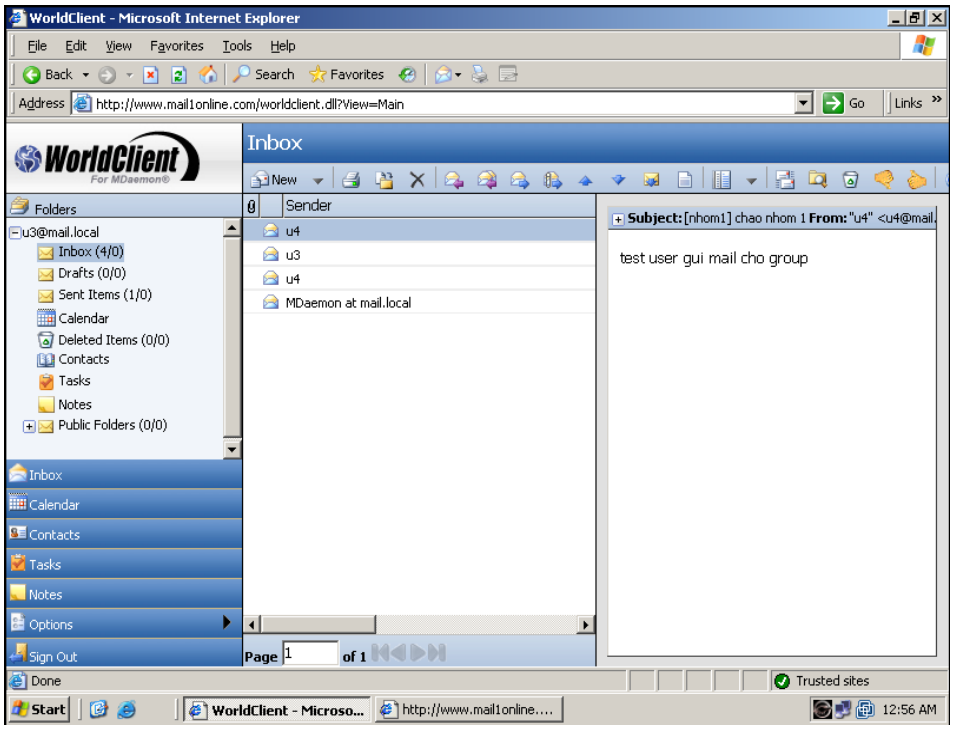


U2 đã nhân được mail từ u1

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account u4 và sau đó Click Sign In để chấp nhận



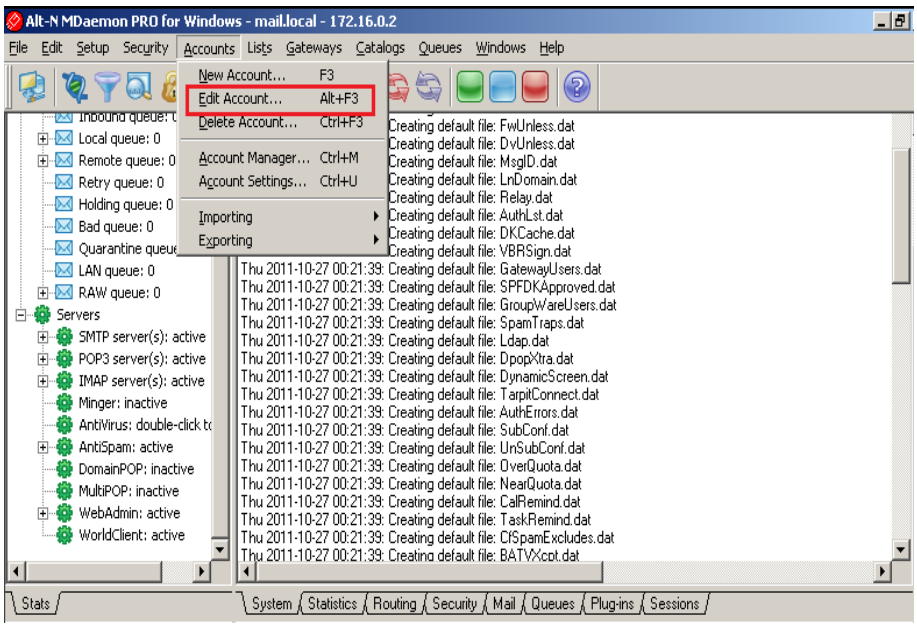
Click New và điền thông tin u4 gửi nhom1, sau đó click Send Now để gửi



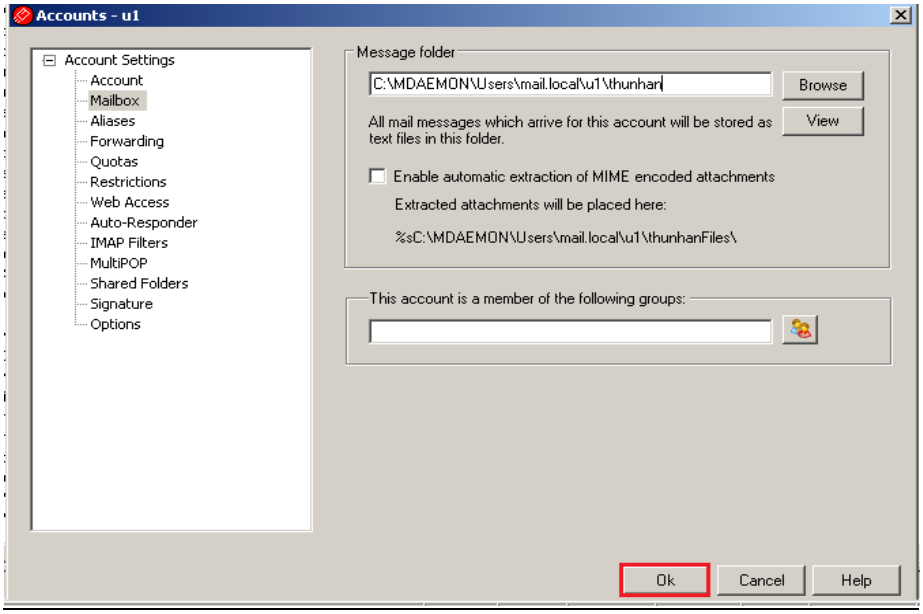
U3 trong nhom1 đa nhận được mail

4.2. Quản lí User (Forwarding, Quota, mailbox, Alias)

- *Mailbox*

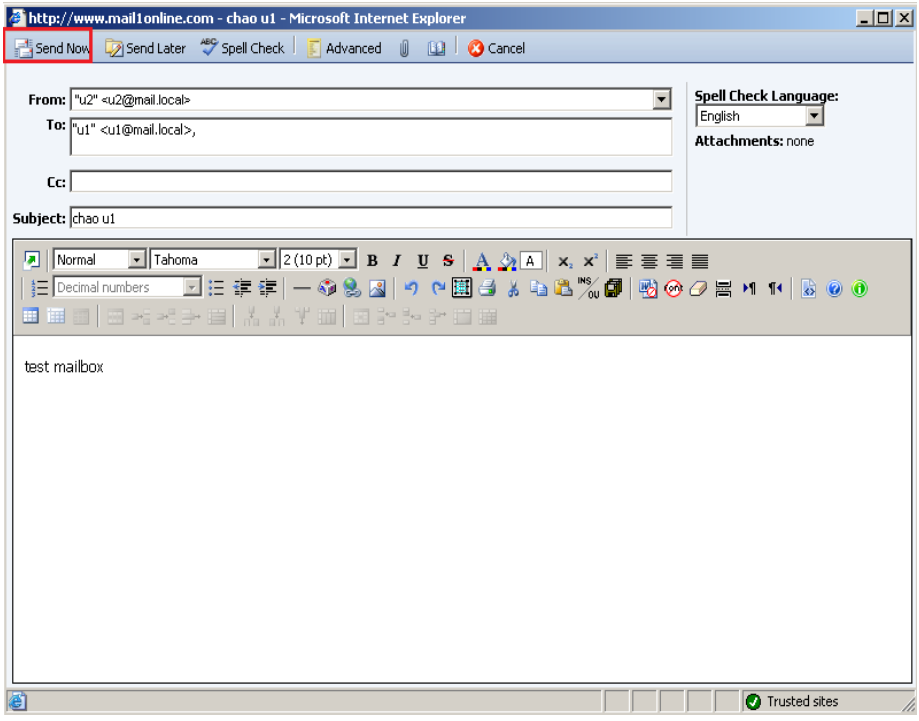


Click Accounts\ Edit Account…

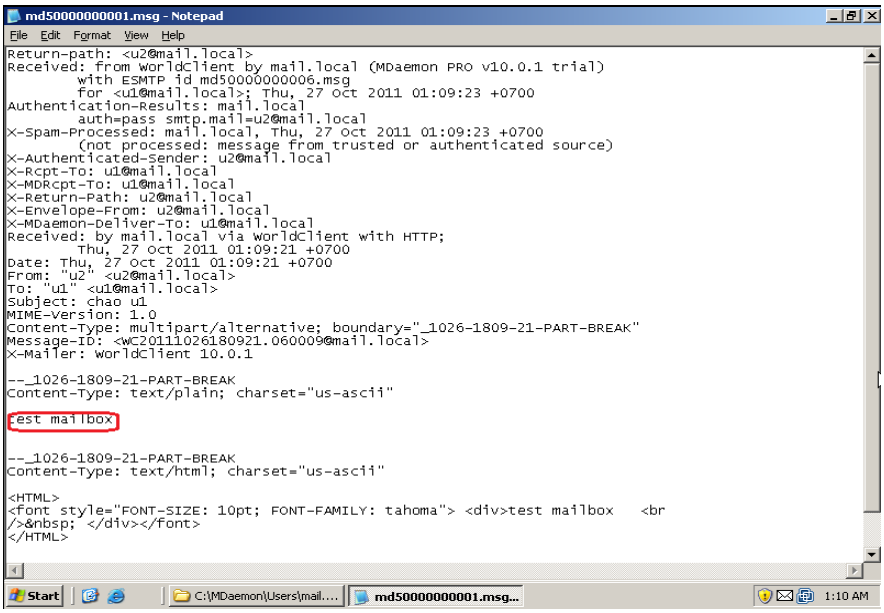


Click mailbox\ chọn đường dẫn như trên, sau đó Click Ok để chấp nhận

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account u2 và sau đó Click Sign In để chấp nhận



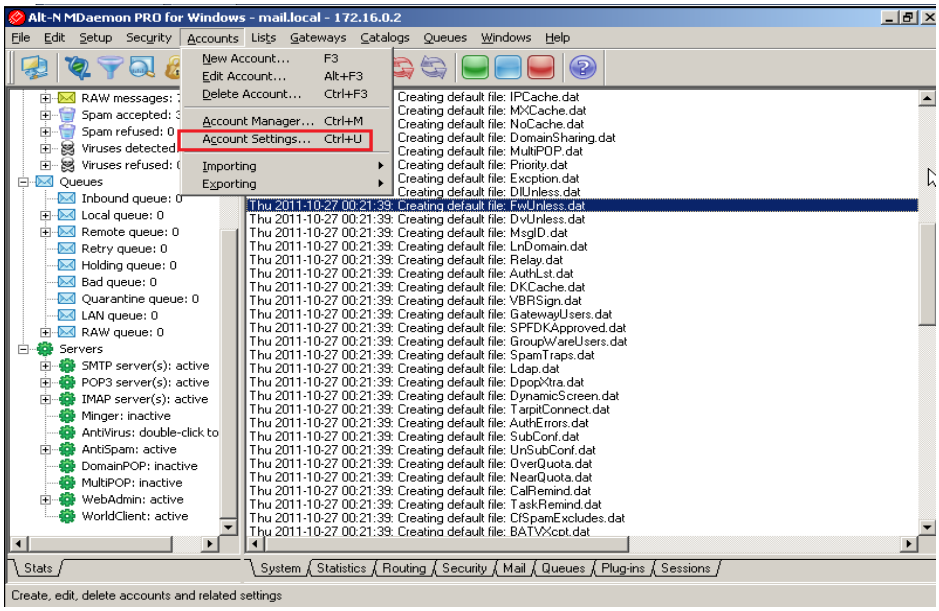
Click New\ điền thông tin như trên, sau đó Click send Now để gửi



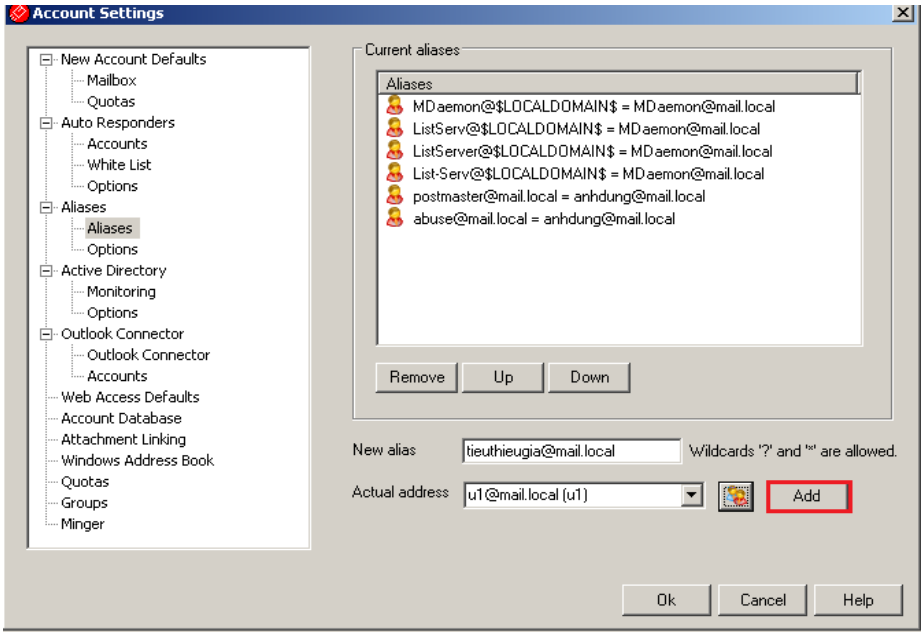
C:\Mdaemon\User\mail.local\u1\thunhan\Click md5000000001.msg để xem nội dung u2@mail.local gửi cho u1@mail.local

Tạo bí danh(Alias)

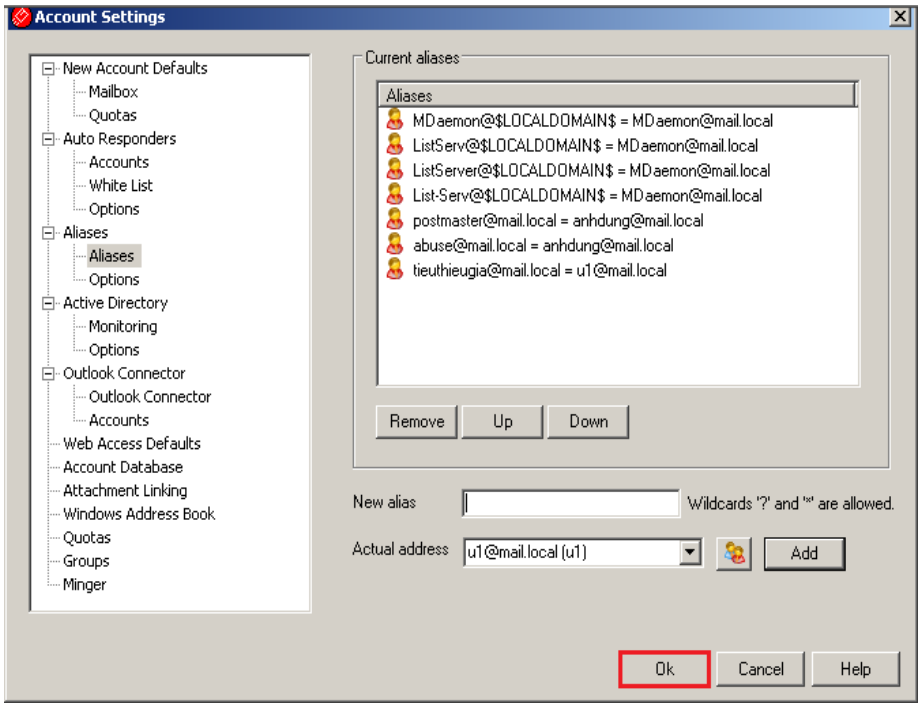
Phần soạn thảo bí danh cho phép bạn tạo nhiều địa chỉ như thực sự chỉ là một user account hoặc là mailing list



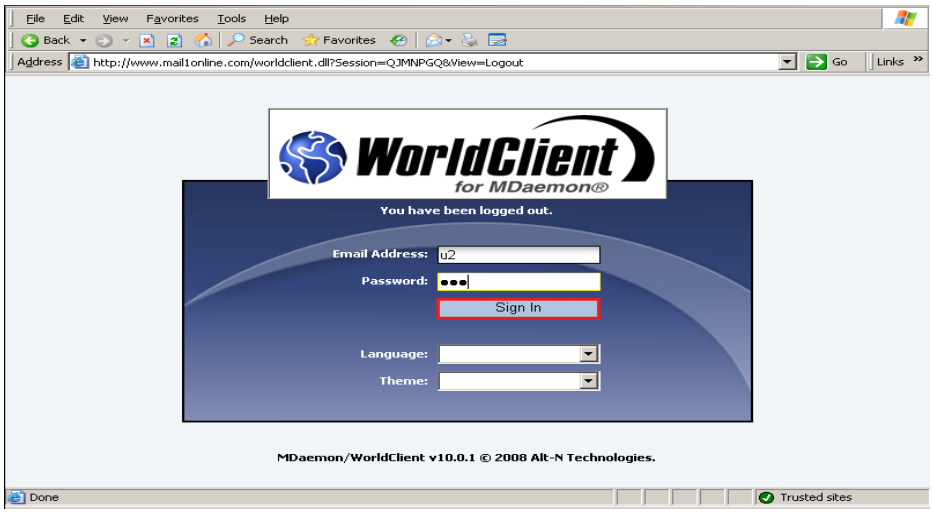
Click Accounts\ Account Settings…



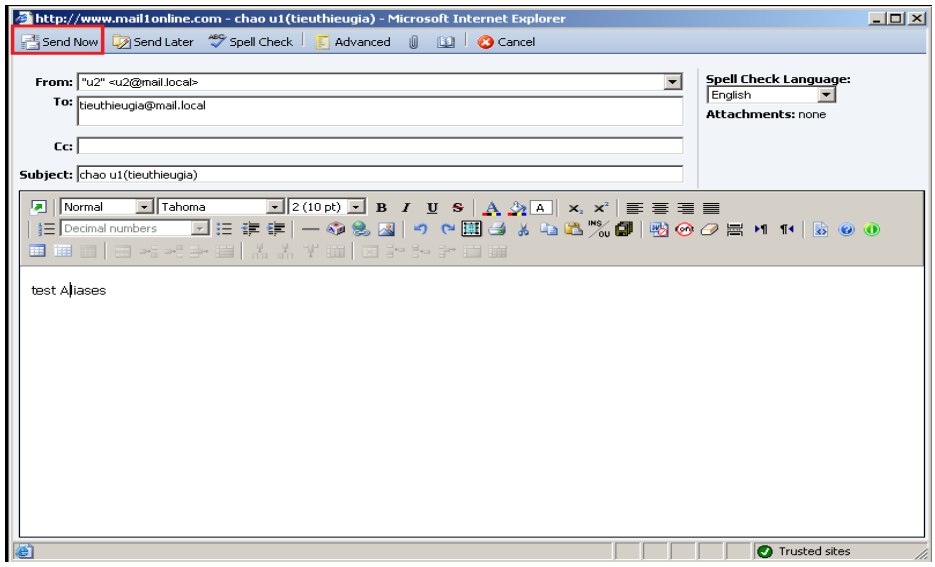
Click Aliases và điền thông tin, sau đó Click Add



Click Ok để chấp nhận

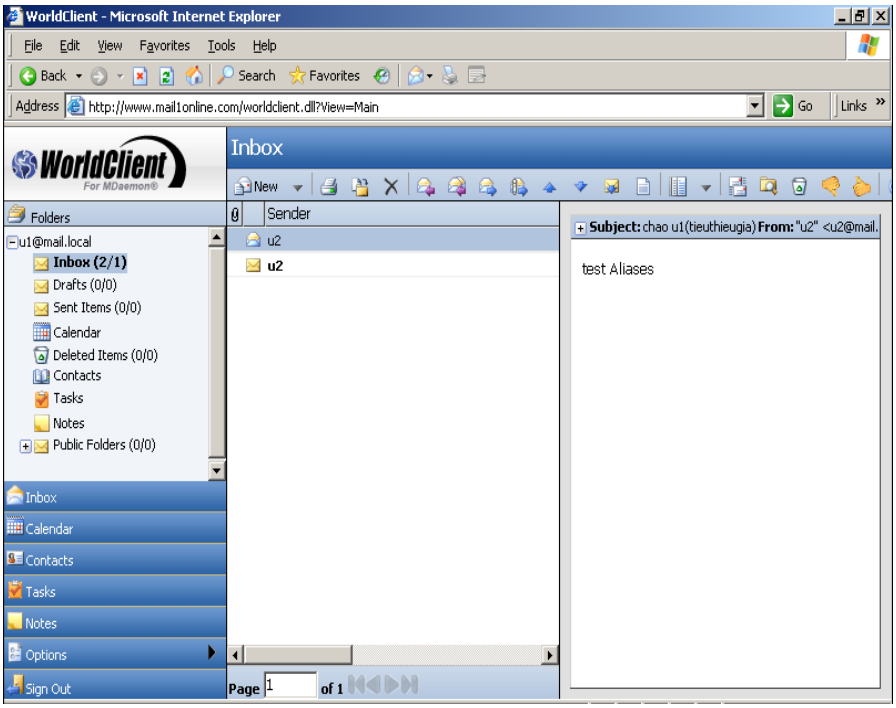


Điền thông tin, sau đó Click Sign In để chấp nhận



Click New và điền thông tin gửi cho tieuthieugia, sau đó Click Send Now để gửi

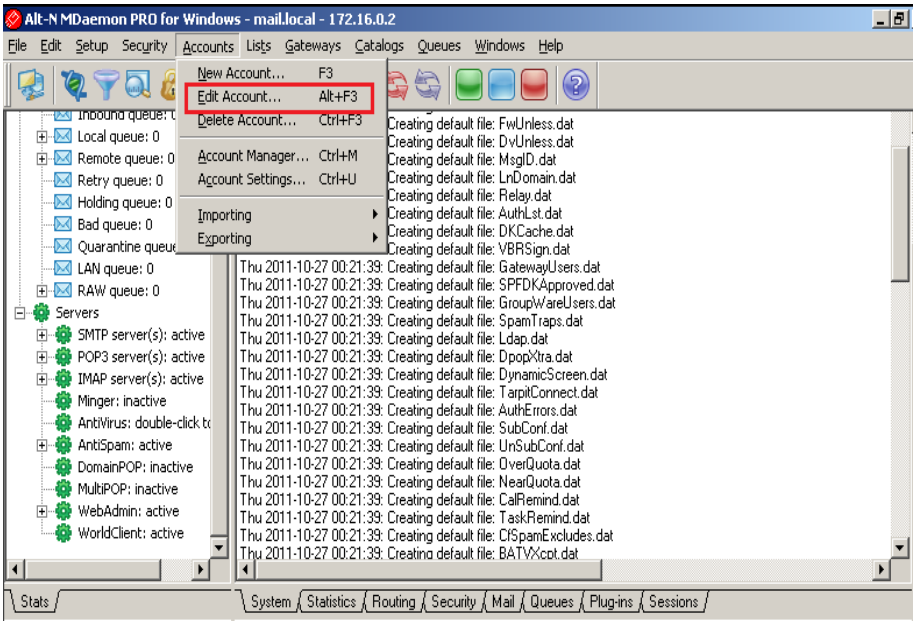
Điền thông tin, sau đó Click Sign In để chấp nhận



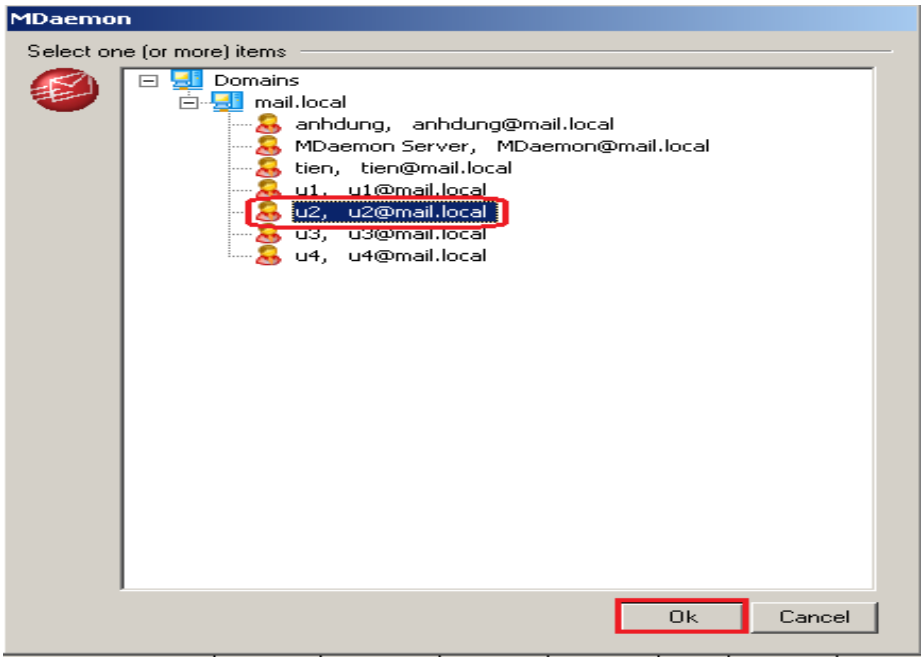
Thông tin u2 gửi u1 thông qua bí danh tieuthieugia@mail.local

- *Forwarding*

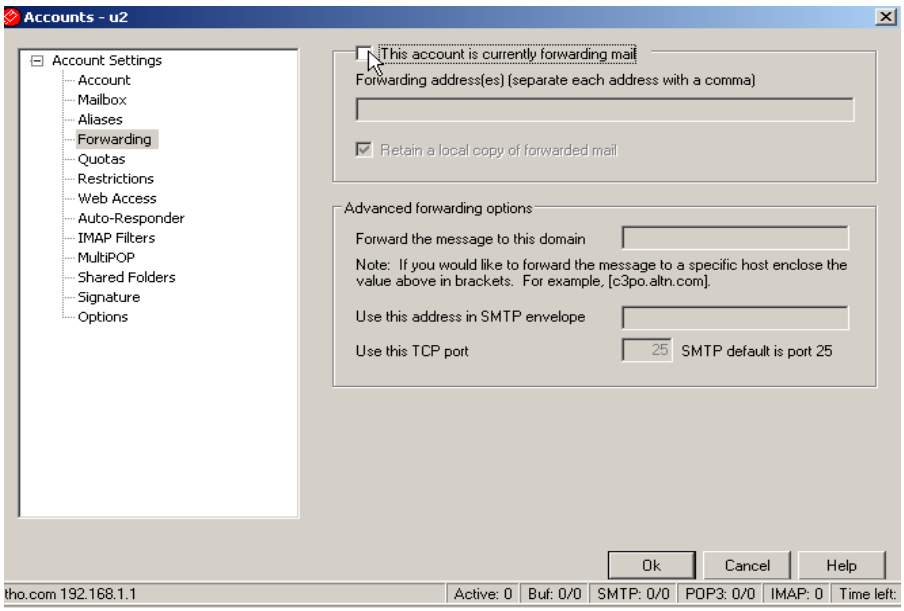
Forwarding là một dạng địa chỉ e-mail không trực tiếp lưu giữ các e-mail khi được người sử dụng Internet gửi tới mà nó chỉ có tác dụng chuyển tiếp các e-mail liên hệ này tới 1 địa chỉ e-mail định trước có khả năng lưu giữ các e-mail liên hệ.



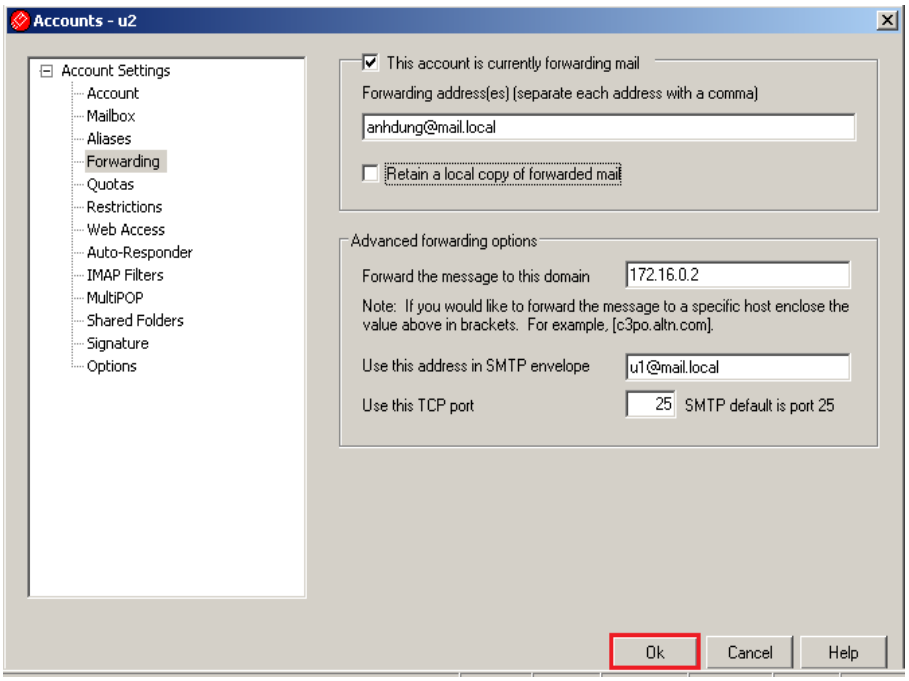
Click Accounts\ Edit Account…



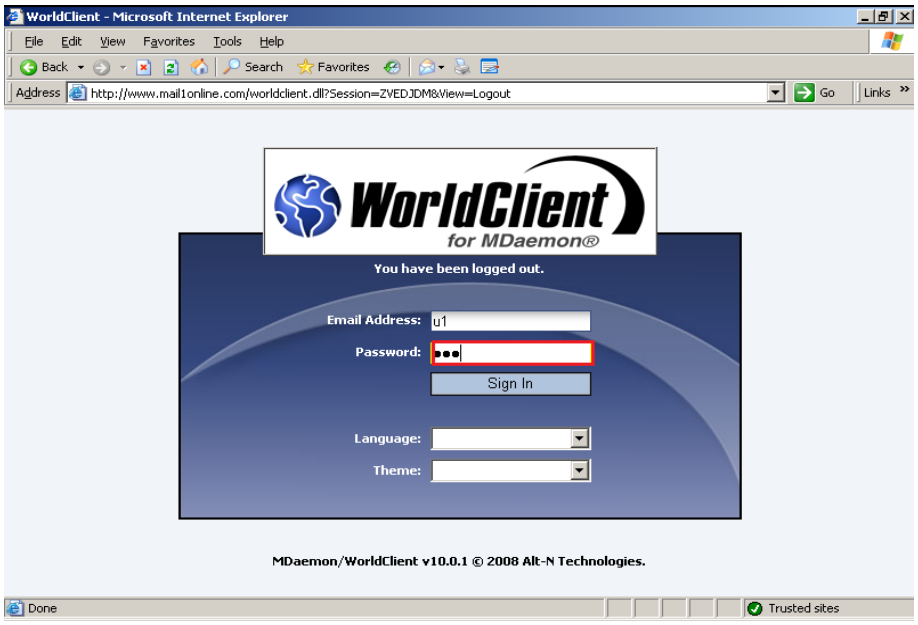
Chọn Account u2, sau đó Click OK



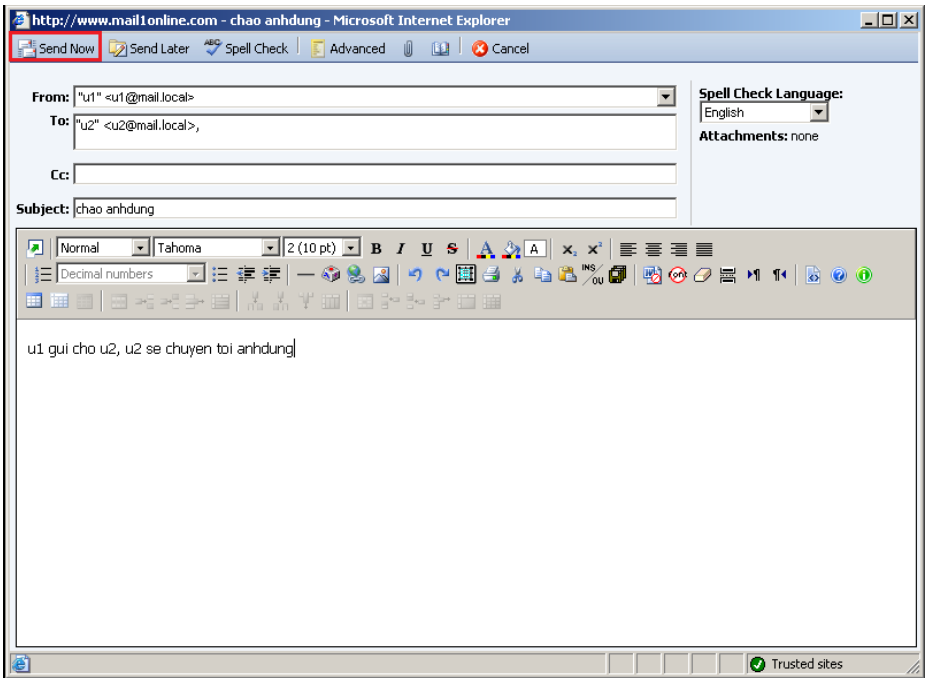
Click Forwarding, sau đó chọn “This account is currently forwarding mail”



Điền thông tin như trên và bỏ chọn "Retain a local copy of forwarded mail", sau đó Click OK

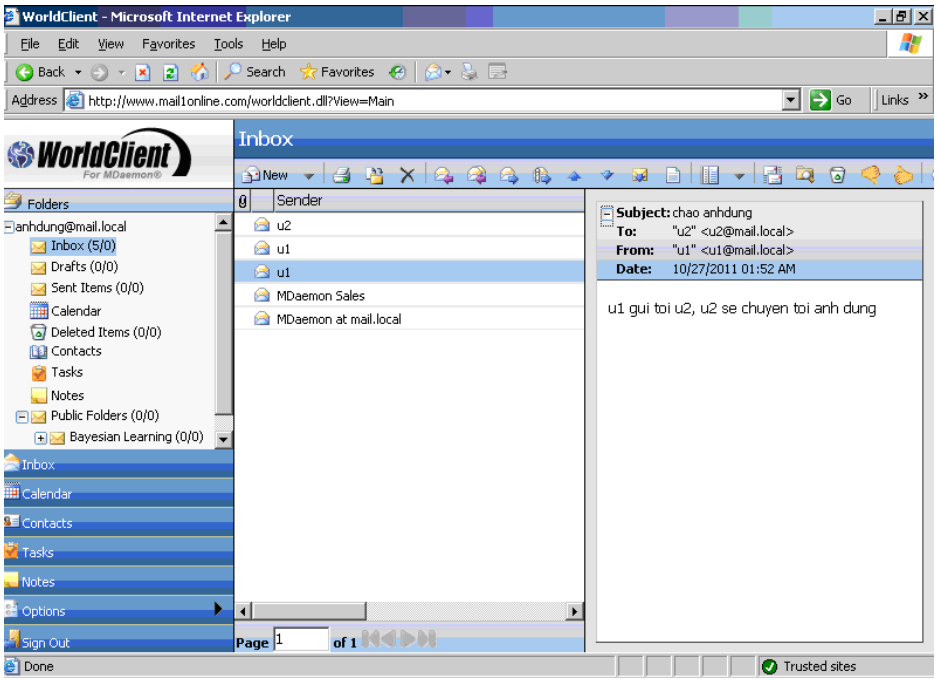


Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account u1 và sau đó Click Sign In để chấp nhận



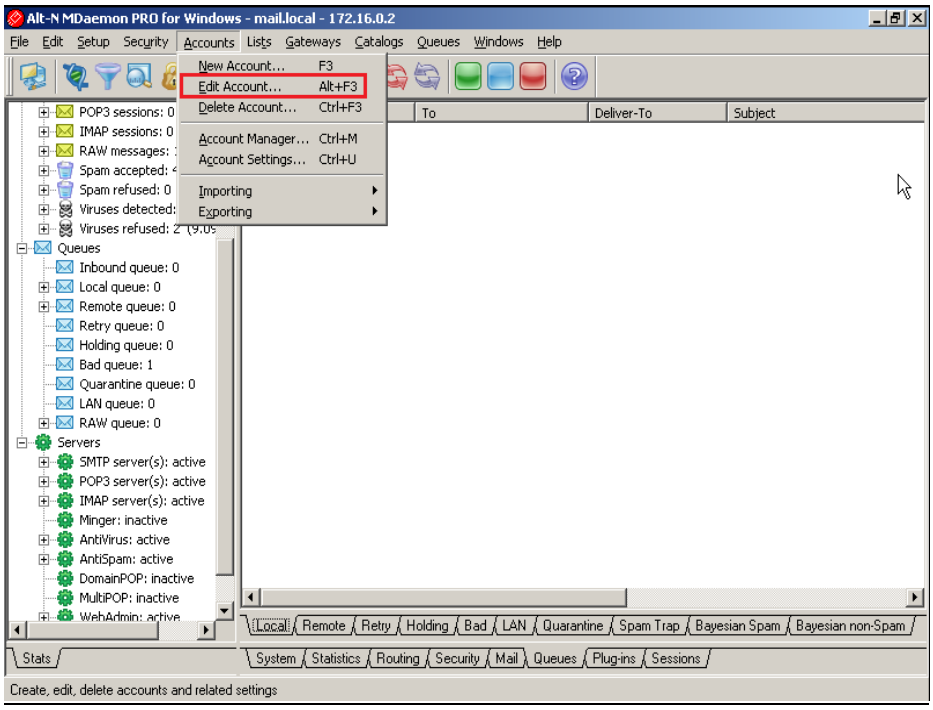
Click New\ điền thông tin như trên\ Click Send Now để gửi

Trên thanh Address gõ địa chỉ: http://www,mail1online.com, điền thông tin account "anhdung" và sau đó Click Sign In để chấp nhận

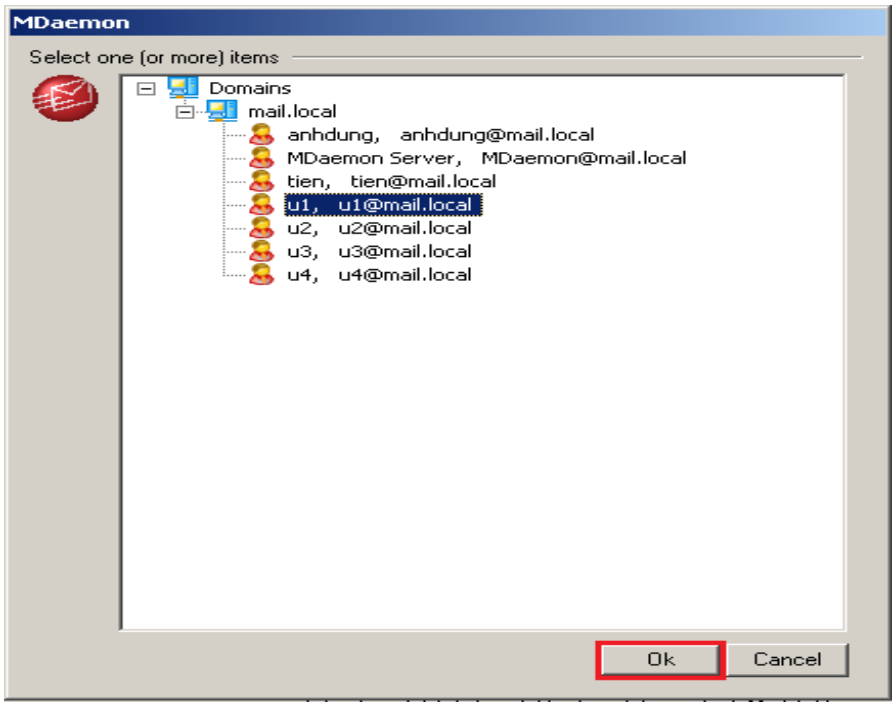


Hình trên là thông tin u1 gửi cho anhdung thông qua u2.(trong u2 sẽ không có thư u1 gửi vì lúc cấu hình Forwarding đã bỏ chọn "Retain a local copy of forwarded mail")

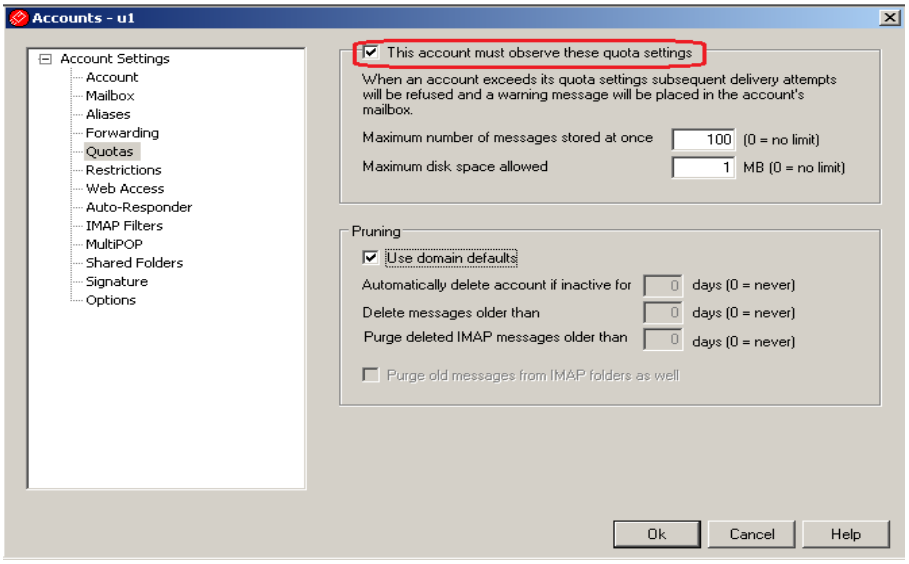
- *Quota*



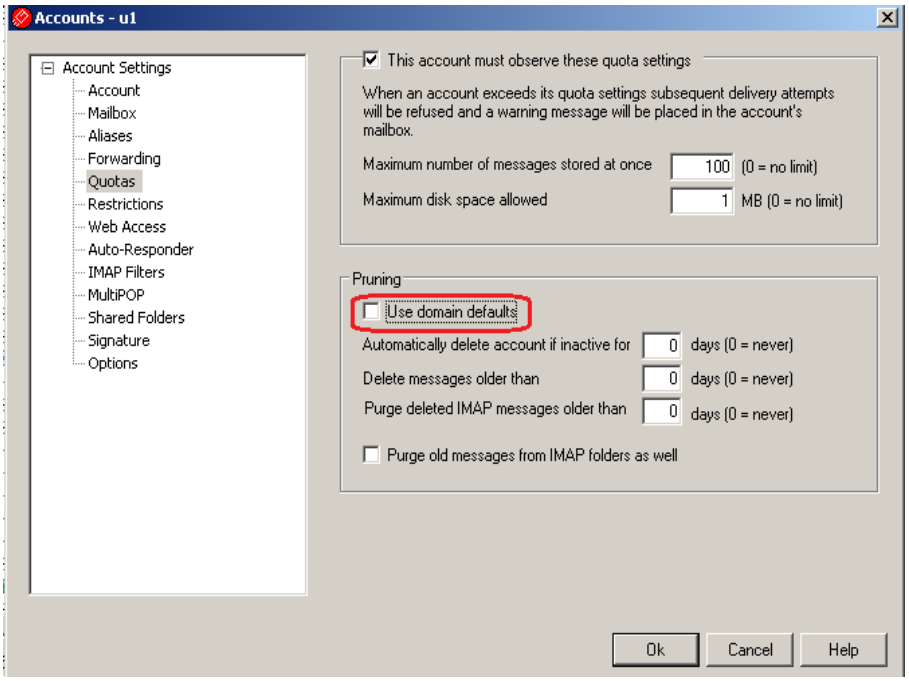
Click Accounts\ Edit Account…



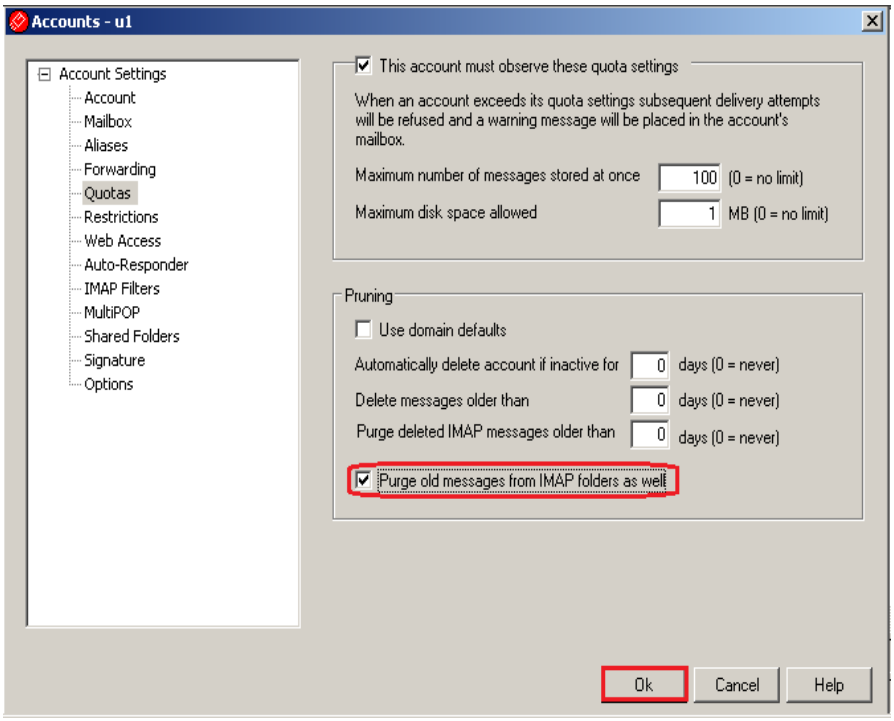
Chọn Account u1, sau đó Click OK để chấp nhận



Click Quotas, sau đó chọn “this account must abserve these quota setting”

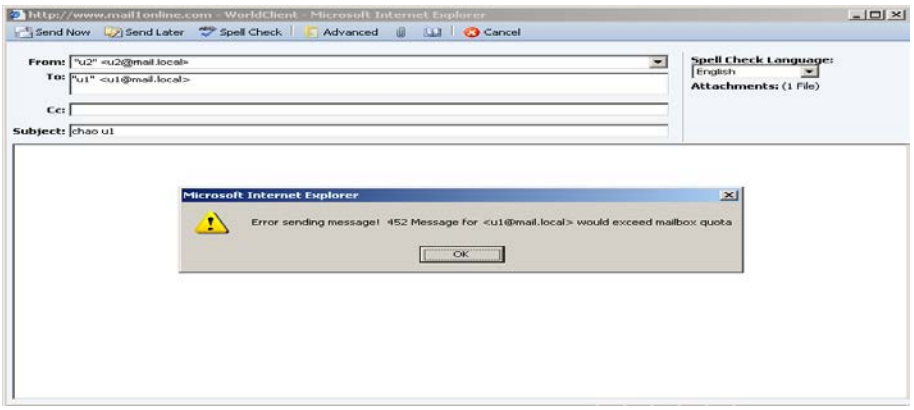


Bỏ chọn “use domain faults, điền thông tin như trên



Chọn “purge old messages form IMAP forder as well”, sau đó Click OK để chấp nhận

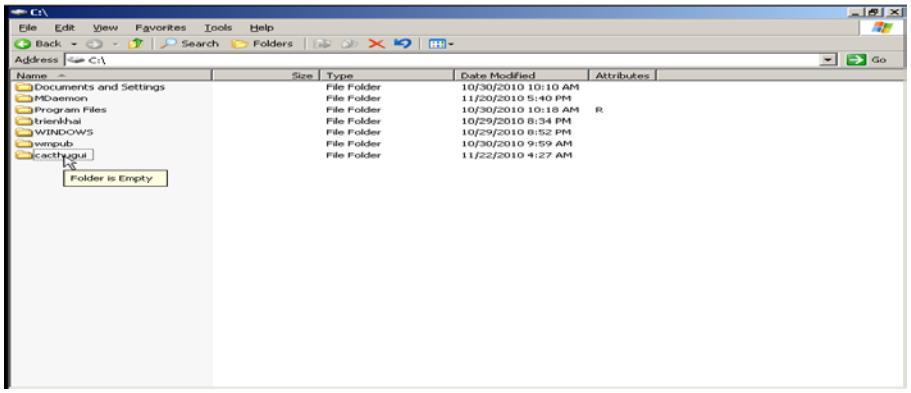
Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account "u2" và sau đó Click Sign In để chấp nhận



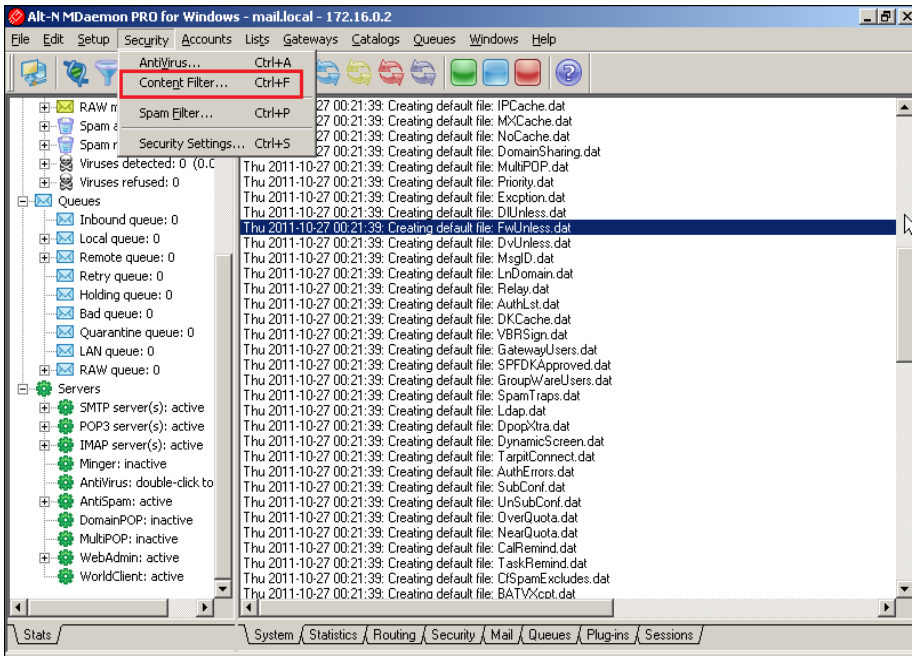
Click New và điền thông tin gửi tới u1, sau đó Click Send Now sẽ nhận được hộp thông báo như trên

4.3. Lọc thư, chống virus thư điện tử

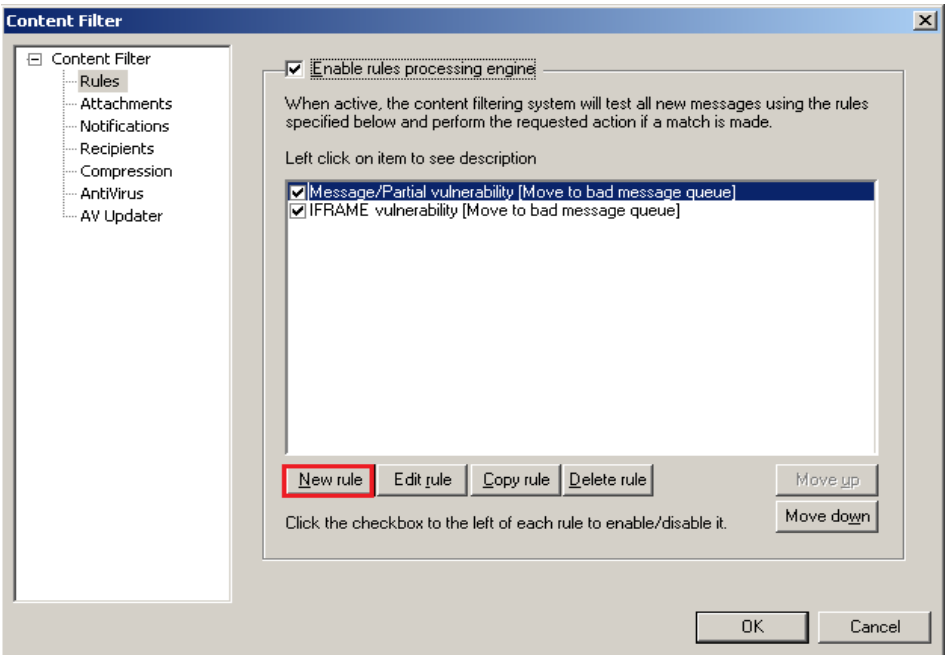
- *Lọc thư*



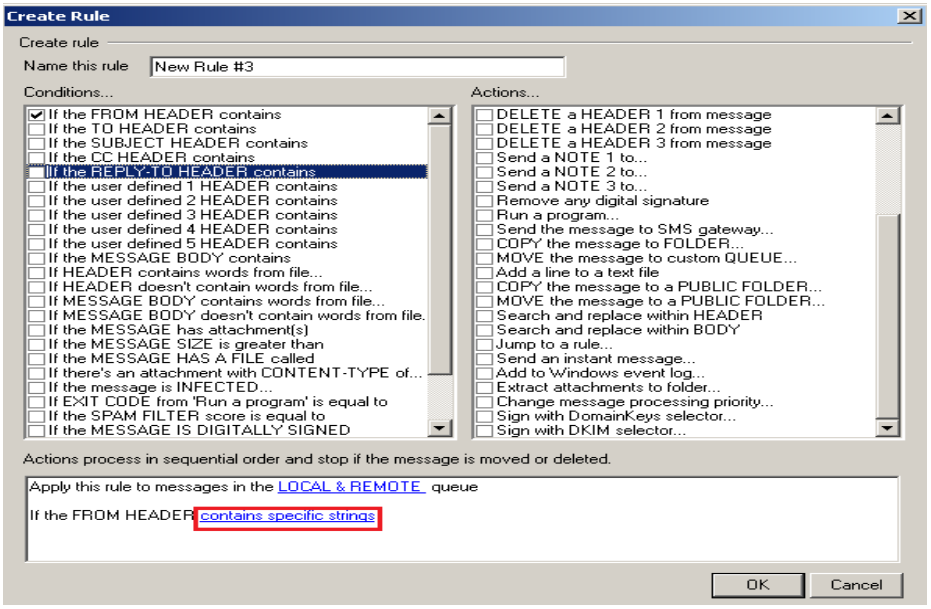
Tạo 1 Folder có tên "cacthugui" nằm trong ổ C



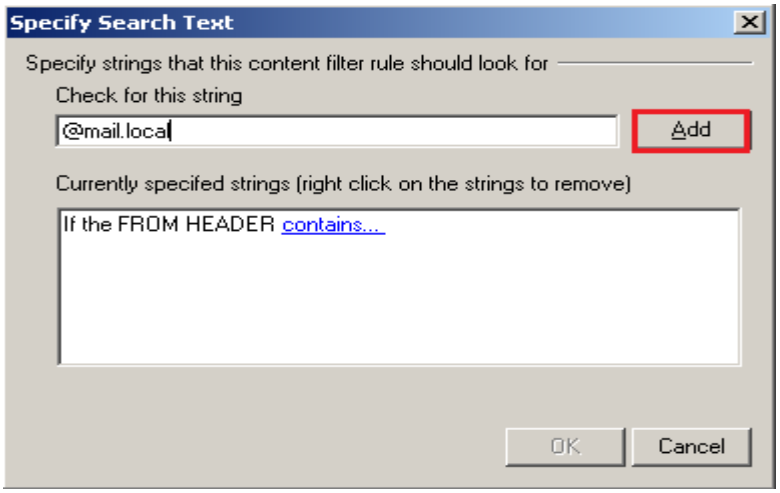
Click Security\ Content Filter…



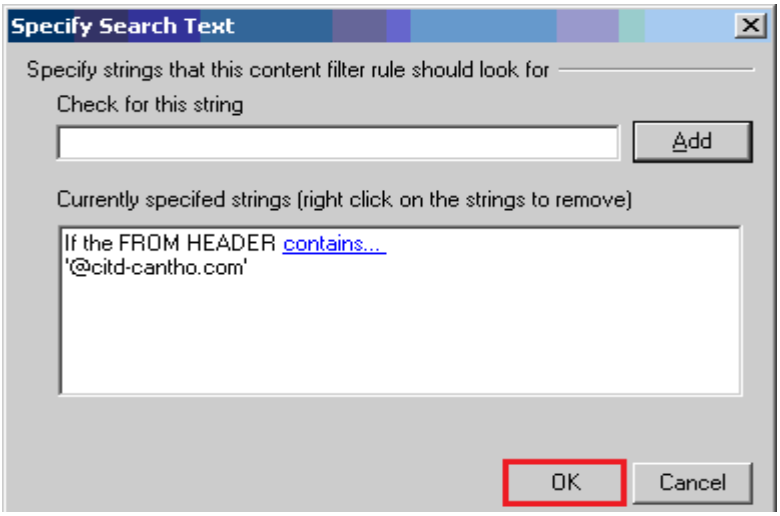
Click Rules và Enable rules processing engine, sau đó Click New rule



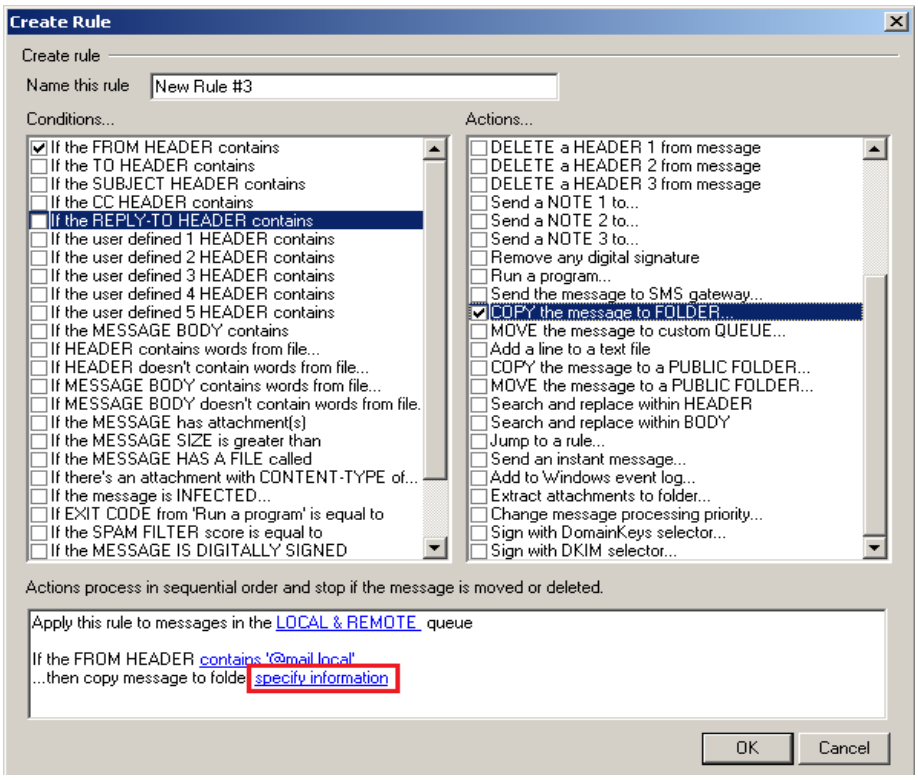
Chọn “If the FROM HEADER contains”\ Click “contains specific strings”



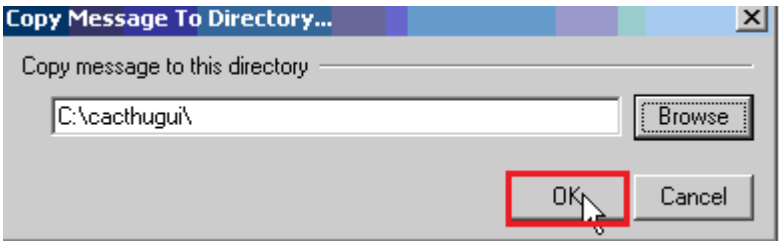
Điền thông tin, sau đó Click Add



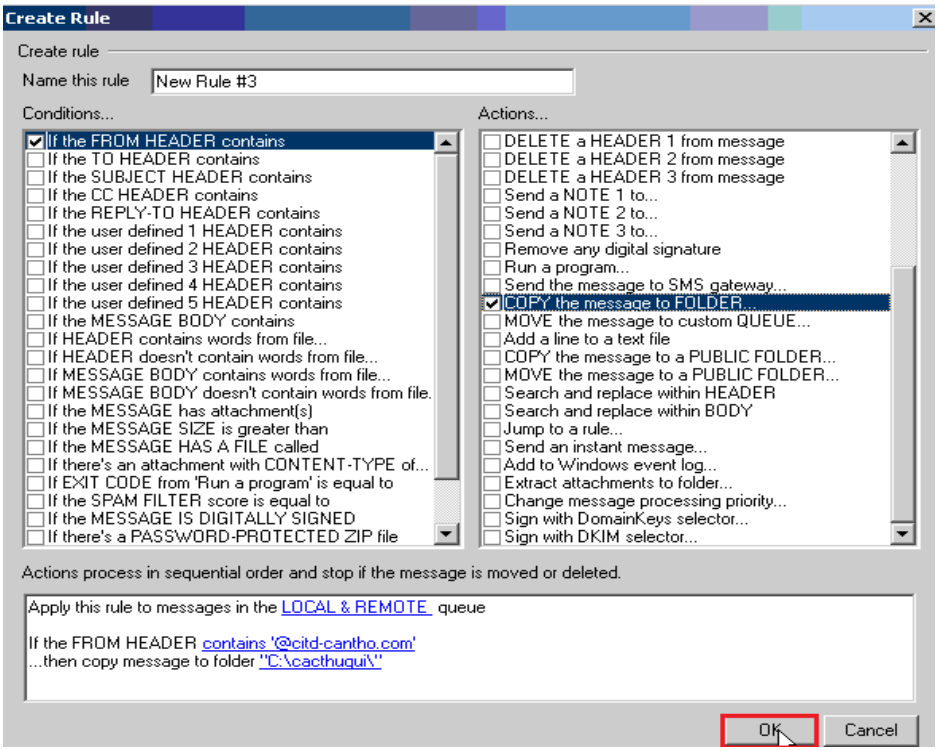
Click OK để chấp nhận



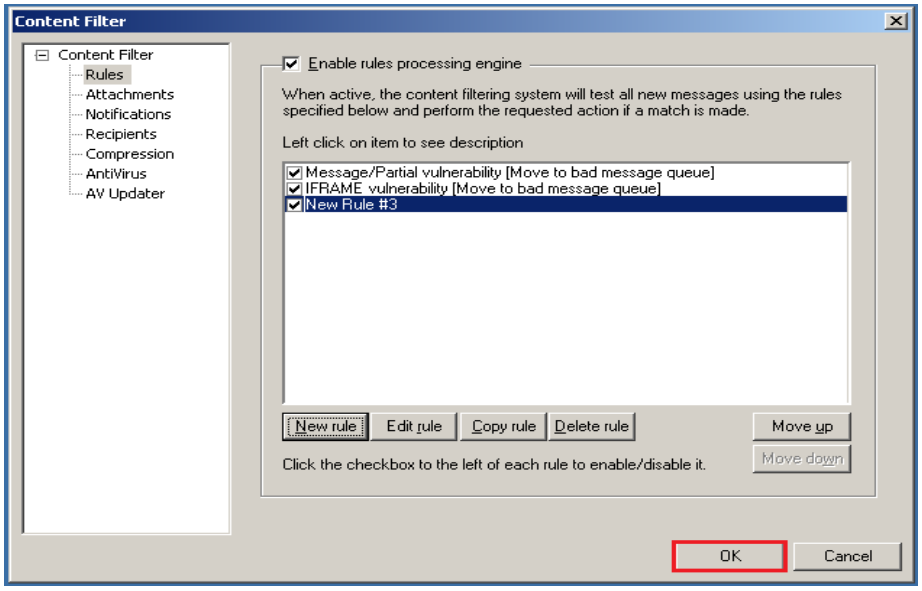
Chọn “COPY the message to FOLDER…”\ Click “specifi information”



Click Browse tìm đường dẫn, sau đóClick OK để chấp nhận

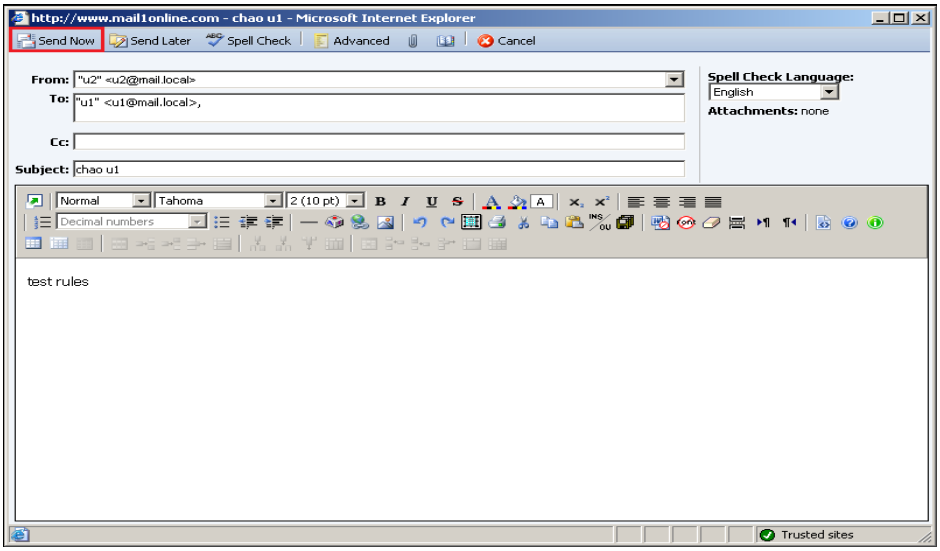


Click OK để chấp nhận

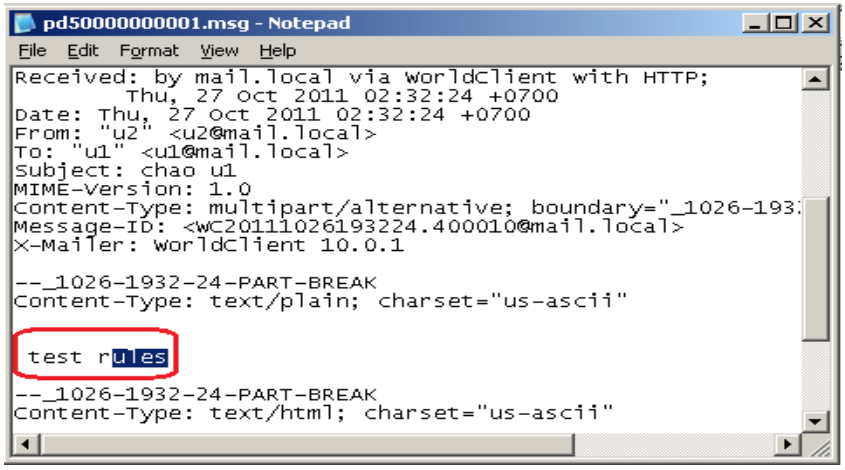


Click OK để chấp nhận

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account u2 và sau đó Click Sign In để chấp nhận



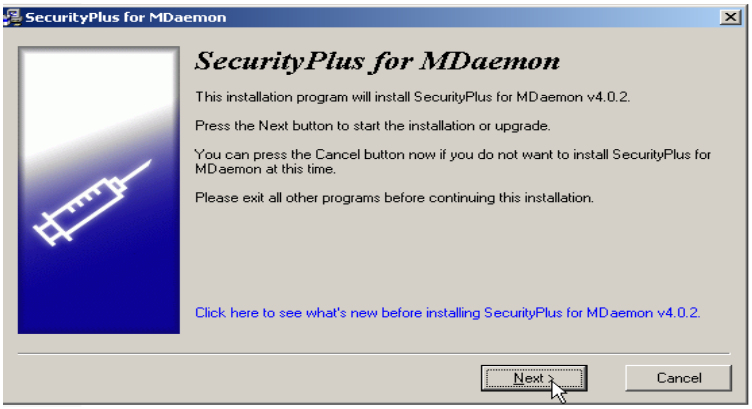
Click New, điền thông tin gửi tới u2, sau đó Click Send Now để Gửi



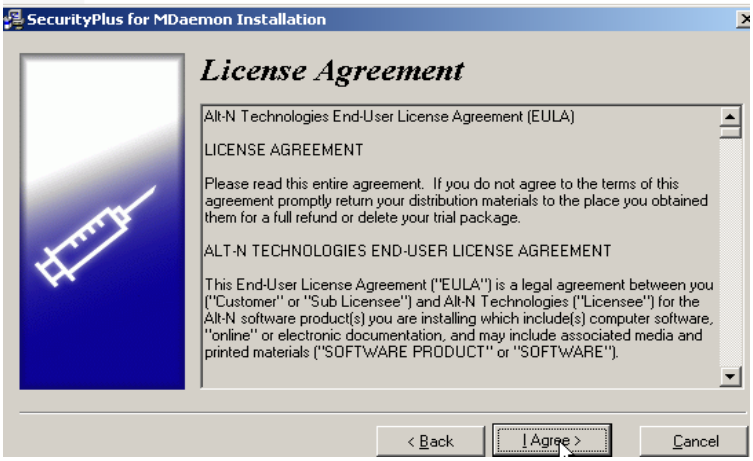
Click ổ C:\cacthugui\ pd50000000001.msg

- *Anti Virus*

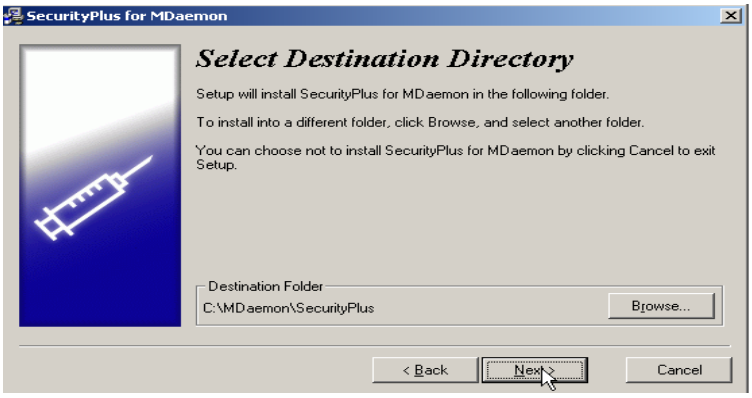
Cài đặt SecurityPlus.4.0.2



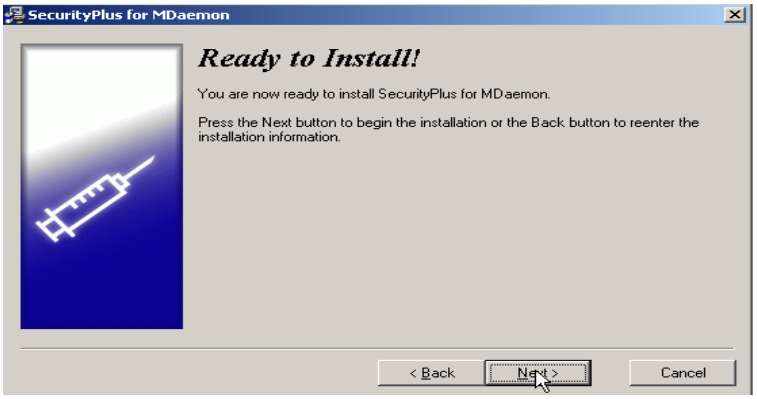
Click Next để tiếp tục



Click Agree

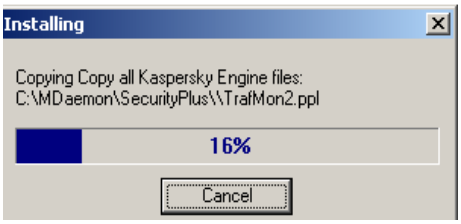


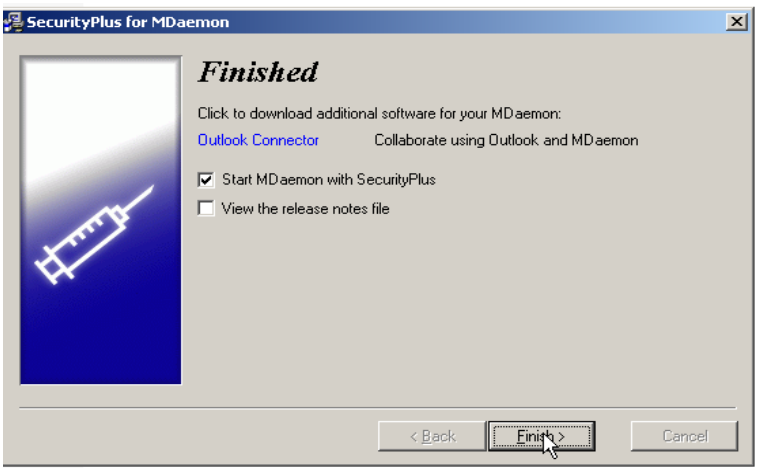
Click Next để tiếp tục



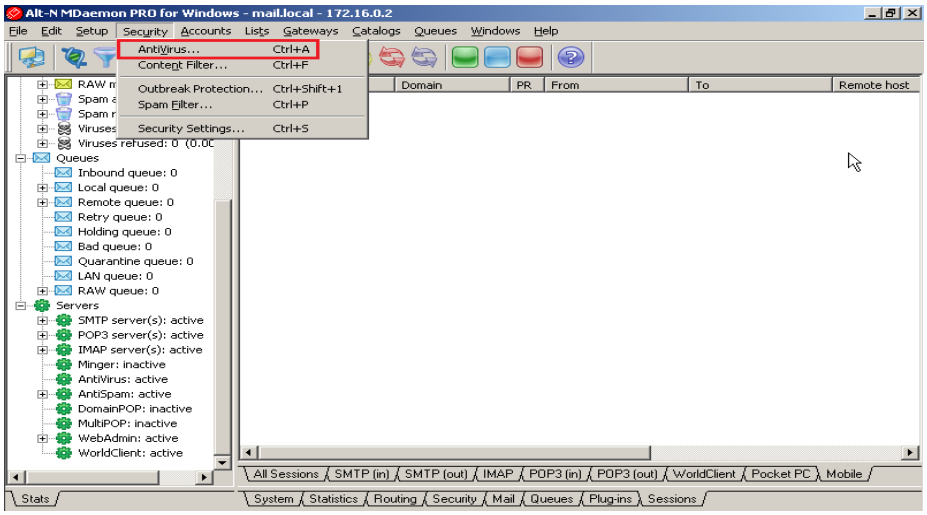
Click Next để tiếp tục

Click continue

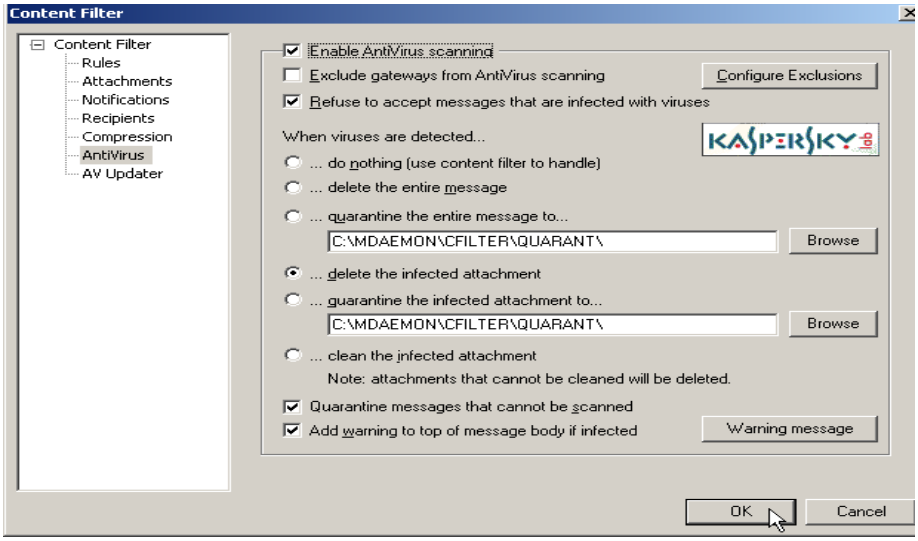




Click Finish để hoàn tất

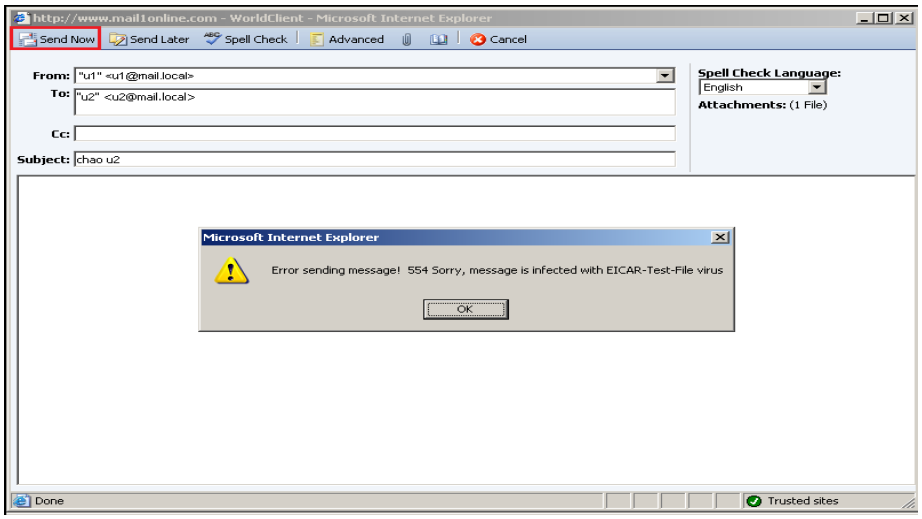


Click Security\ Antivirus…



Click AntiVirus\ Click option " delete the infected attachment to…" , sau đó Click OK để chấp nhận

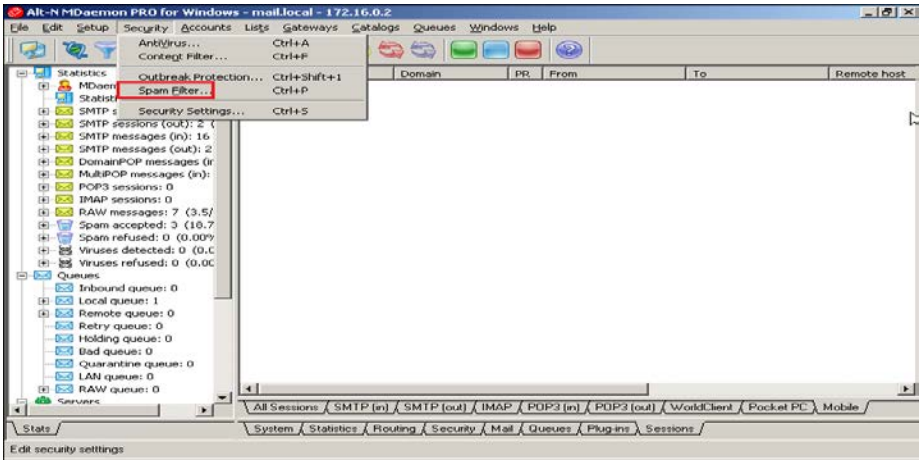
Điền thông tin, sau đó Click SignIn để chấp nhận



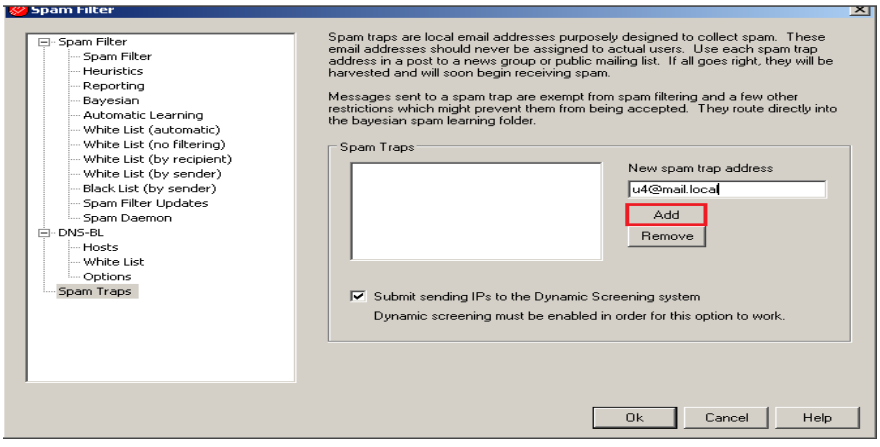
Click New và điền thông tin gửi cho u2 , sau đó Click Send Now sẽ Xuất hiện thông báo tập tin bị nhiễm virus không gửi được

4.4. Anti Spam

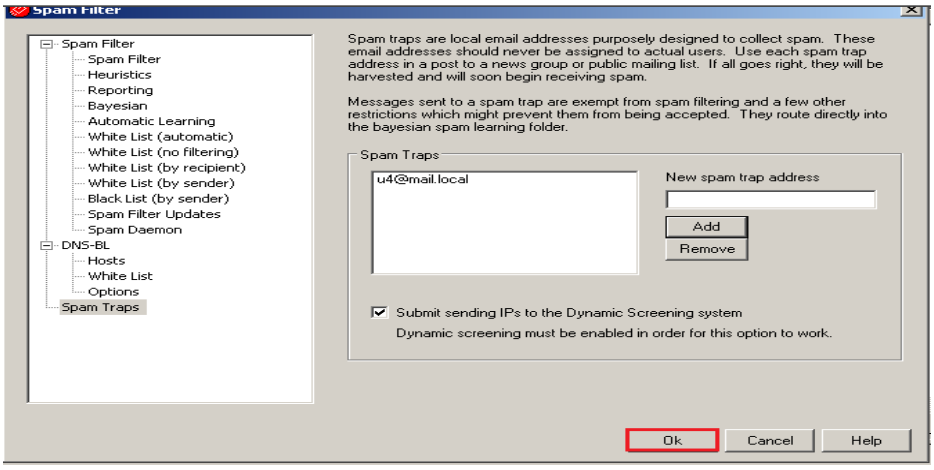
Spam Traps



Click security\ Spam Filter

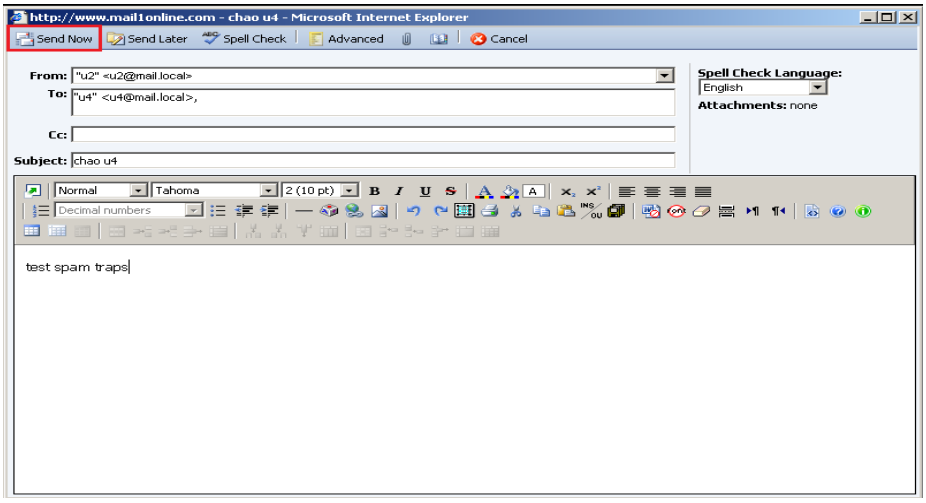


Spam trap\ điền địa chỉ mail , sau đó Click Add



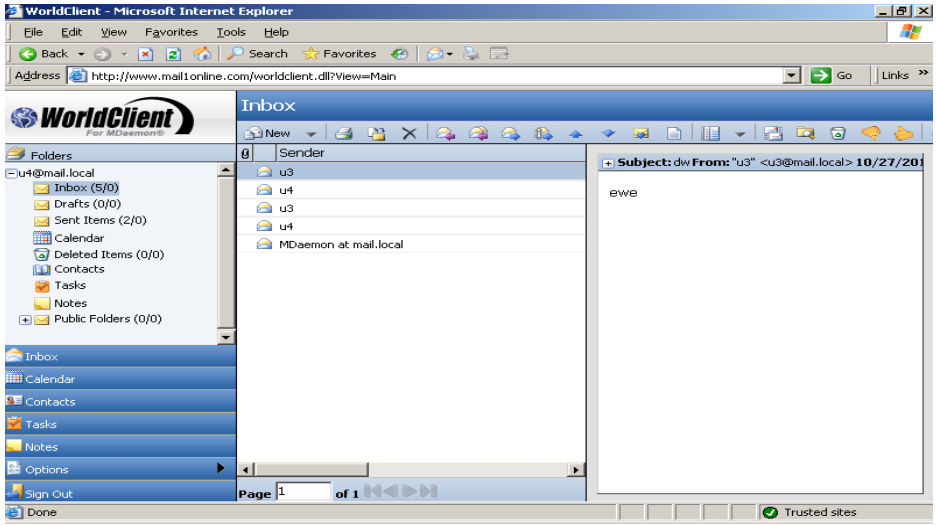
Click Ok để hoàn tất

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account "u2" và sau đó Click Sign In để chấp nhận



Click New\điền thông tin như trên\ Click send Now để gửi

Trên thanh Address gõ địa chỉ: http://www.mail1online.com, điền thông tin account "u4" và sau đó Click Sign In để chấp nhận



U4 sẽ không nhận được thư