Bài 5: IP Sec trong Windows Server 2003.

Mục tiêu bài học

Trong bài học này, chúng ta sẽ:

- Định nghĩa IP Sec.
- Các thao tác bảo mật.
- Các bộ lọc IP Sec.
- Triển khai IP Sec trên Windows Server 2003.

IP Security (IPSec) là một giao thức hỗ trợ thiết lập các kết nối bảo mật dựa trên địa chỉ IP.Giao thức này hoạt động ở lớp **Network** trong mô hình OSI, do đó nó bảo mật và tiện lợi hơn các giao thức bảo mật khác ở lớp **Application** như **SSL**.**IPSec** cũng là một thành phần quan trọng hỗ trợ giao thức **L2TP** trong công nghệ **mạng riêng ảo VPN (Virtual Private Network)**.
Để sử dụng **IPSec** bạn phải tạo ra các quy tắc (rule).Một quy tắc là sự kết hợp giữa hai thành phần: các bộ lọc (filter list) và các thao tác (actions).Chẳng hạn, một quy tắc **IPSec** có nội dung như sau: "Hãy mã hóa tất cả những dữ liệu truyền bằng ứng dụng Telnet từ máy có địa chỉ 203.162.1.1". Quy tắc này gồm hai phần, phần bộ lọc là "quy tắc này chỉ hoạt động khi có dữ liệu được truyền từ máy có địa chỉ 203.162.1.1 thông qua cổng (port) 23", phần thao tác là "mã hóa dữ liệu".

1. Các thao tác bảo mật (security action)

IPSec của Microsoft hỗ trợ bốn loại thao tác (action) bảo mật.Các thao tác bảo mật này giúp hệ thống có thể thiết lập những phiên (session) trao đổi thông tin giữa các máy được an toàn. Danh sách các thao tác bảo mật trong hệ thống Windows Server 2003 gồm:
Block transmissions: Ngăn chặn những gói dữ liệu được truyền.Ví dụ, bạn muốn *IPSec* ngăn chặn dữ liệu truyền từ máy A đến máy B thì giao thức *IPSec* trên máy B loại bỏ mọi dữ liệu truyền đến từ máy A.
Encrypt transmissions: Mã hóa những gói dữ liệu được truyền.Ví dụ, bạn muốn dữ liệu được truyền từ máy A đến máy B.Nhưng bạn sợ rằng có người sẽ nghe trộm *(sniffer)* trên đường truyền kết nối giữa hai máy A và B, vì vậy bạn cần cấu hình cho *IPSec* sử dụng giao thức *ESP* **(Encapsulating Security Payload)** để mã hóa dữ liệu cần truyền trước khi đưa lên mạng. Lúc này, những người xem trộm sẽ thấy những dòng byte ngẫu nhiên và không đọc/hiểu dữ liệu thật.Do *IPSec* hoạt động ở lớp Network nên hầu như việc mã hóa được trong suốt đối với người dùng.Người dùng có thể gửi mail, truyền file hay telnet như bình thường.
Sign transmissions: Ký tên vào các gói dữ liệu truyền nhằm tránh những kẻ tấn công trên mạng giả dạng những gói dữ liệu được truyền từ những máy mà bạn đã thiết lập quan hệ tin cậy (kiểu tấn công còn gọi là *main-in-the-middle*).IPSec cho phép bạn chống lại điều này bằng một giao thức *AH _ Authentication Header*.Giao thức này là phương pháp *ký tên số hóa (digitally signing)* vào các gói dữ liệu trước khi truyền, nó chỉ ngăn ngừa được giả mạo và sai lệch thông tin chứ không ngăn ngừa được sự nghe trộm thông tin.Nguyên lý hoạt động của phương pháp này là hệ thống sẽ thêm một bit vào cuối mỗi gói dữ liệu truyền qua mạng, từ đó chúng ta có thể kiểm tra xem dữ liệu có bị thay đổi khi truyền hay không.
Permit transmissions: Cho phép dữ liệu được truyền qua, chúng dùng để tạo ra các *quy tắc (rule)* hạn chế một số điều này và không hạn chế một số điều khác.Ví dụ, một quy tắc dạng này *"Hãy ngăn chặn tất cả những dữ liệu truyền tới, chỉ trừ dữ liệu truyền trên các cổng 80 và 443"*.
Chú ý: Đối với hai thao tác bảo mật theo phương pháp *ký tên (sign)* và *mã hóa (encrypt)* thì hệ thống còn yêu cầu bạn chỉ ra *IPSec* dùng phương pháp chứng thực nào (có nghĩa là cho *IPSec* biết cách thức mà máy nhận *(receiver)* và máy gửi *(transmitter)* sẽ trao đổi *mật khẩu;* sau đó, chúng sẽ dùng *mật khẩu* này để ký tên hoặc mã hóa các gói dữ liệu truyền đi trên mạng).Microsoft hỗ trợ ba phương pháp chứng thực: *Kerberos,* chứng chỉ *(Certificate)* hoặc một khóa dựa trên sự thỏa thuận *(agree-upon key)*.Phương pháp *Kerberos* chỉ áp dụng được trong các máy trong cùng một *miền (domain) Active Directory* hoặc trong những miền *Active Directory* có ủy quyền cho nhau.Phương pháp dùng các chứng chỉ cho phép bạn sử dụng các chứng chỉ *PKI (Public Key Infrastructure)* để nhận diện một máy.Phương pháp dùng *khóa dùng chung (chia sẻ) trước (preshared key)* thì cho phép bạn dùng một *chuỗi ký tự thông thường (plain text)* làm khóa *(key)*.

2. Các bộ lọc IPSec

Để *IPSec* hoạt động linh hoạt hơn, Microsoft đưa thêm khái niệm *bộ lọc IPSec (IPSec filter)*.Bộ lọc có tác dụng thống kê các điều kiện để quy tắc hoạt động.Đồng thời chúng cũng giới hạn tầm tác dụng

của các thao tác bảo mật trên một phạm vi máy tính nào đó hay một số dịch vụ nào đó.Bộ lọc *IPSec* chủ yếu dựa trên các yếu tố sau:

- Địa chỉ *IP*, *subnet* hoặc tên *DNS* của máy nguồn.
- Địa chỉ *IP*, *subnet* hoặc tên *DNS* của máy đích.
- Theo giao thức *(TCP, UDP, ICMP)* và số hiệu cổng *(port)*.

3. Triển khai IPSec trên Windows Server 2003

Để triển khai *IPSec* bạn dùng các công cụ thiết lập chính sách dành cho *máy cục bộ (local machine)* hoặc dùng cho *miền (domain)*.

- Máy cục bộ: Click *Start > Run*, nhập vào *secpol.msc* hoặc click *Start-> Programs -> Administrative Tools-> Local Security Policy* và trong cửa sổ console *Local Security Settings* chọn mục *IP Security Policies on Local Machine*.
- Miền: Click *Start-> Programs -> Administrative Tools -> Domain Controller Security Policy* và trong cửa sổ console *Default Domain Controller Security Settings* chọn mục *IP Security Policies on Domain Controller*.
  - Tóm lại, khi triển khai *IPSec* bạn cần nhớ:
    - ✓ Nếu triển khai *IPSec* trên Windows Server 2003 thông qua các chính sách (*policy)*, trên một máy tính bất kỳ nào đó vào một thời điểm thì chỉ có một chính sách *IPSec* được hoạt động.
    - ✓ Mỗi chính sách *IPSec* gồm một hoặc nhiều quy tắc *(rule)* và một phương pháp chứng thực nào đó.Mặc dù các quy tắc *Permit* và *Block* không dùng đến chứng thực nhưng Windows Server 2003 vẫn đòi bạn chỉ định phương pháp chứng thực (phương pháp chứng thực nào cũng được).
    - ✓ *IPSec* cho phép bạn chứng thực thông qua *Active Directory,* các chứng chỉ *PKI* hoặc một khóa được dùng chung (chia sẻ) trước *(preshared key)*.
    - ✓ Mỗi quy tắc *(rule)* gồm một hay nhiều bộ lọc *(filter)* và một hay nhiều thao tác bảo mật *(action)*.
    - ✓ Có bốn thao tác bảo mật mà quy tắc có thể dùng là: *Block, Encrypt, Sign* và *Permit*.

4. Các chính sách IPSec tạo sẵn

Bên phải của khung cửa sổ chính của công cụ cấu hình chính sách *IPSec,* bạn sẽ thấy có ba chính sách được tạo sẵn tên là: *Client, Server* và *Secure*.Cả ba chính sách này đều ở trạng thái chưa áp dụng *(unassigned)*. Bạn cần lưu ý, ngay cùng một thời điểm thì chỉ có một chính sách được áp dụng *(assigned)* và hoạt động, có nghĩa là khi bạn <u>áp dụng một chính sách mới thì chính sách đang hoạt động hiện tại sẽ trở về trạng thái không hoạt động</u>.

Chi tiết của ba chính sách tạo sẵn này:

Client (Respond Only): Chính sách này quy định máy tính của bạn không chủ động dùng *IPSec* trừ khi được yêu cầu dùng *IPSec* từ máy đối tác.Chính sách này cho phép bạn có thể kết nối cả với các máy tính dùng *IPSec* hoặc không dùng *IPSec*.Ví dụ: Giả sử bạn đã ấn định chính sách này trên máy *client* và cố gắng truy cập một website trên một máy *server không yêu cầu IPSec*.Trong trường hợp này, máy *server (web server)* sẽ không cố gắng thực hiện *IPSec* với máy *client* nên máy *client* sẽ không yêu cầu áp dụng *IPSec* cho phiên giao dịch với máy *server* đó.Nhưng nếu máy *client* kết nối với một máy *server có thực hiện IPSec* thì *server* này sẽ báo máy *client* áp dụng *IPSec* và lúc này máy *client* bắt buộc phải áp dụng *IPSec*.

Chính sách này có một quy tắc chứa các thiết lập sau:

Rule 1 (default response rule) (có nghĩa là áp dụng cho tất cả chính sách *IPSec*)

+ IP Filter List: *<Dynamic>* (có nghĩa là bộ lọc không được cấu hình.Bộ lọc sẽ tự động tạo ra khi nhận được thỏa thuận bảo mật dữ liệu _ *IKE negotiation packet)*.

+ Filter Action: *Default Response* (có nghĩa là thao tác bảo mật không được cấu hình và bộ lọc *Negotiate Security filter action* được dùng).

+ Authentication: *Kerberos*

+ Tunnel Setting: *None*

+ Connection Type: *All*

=>Mặc định quy tắc này sẽ kích hoạt *(active)* tất cả các chính sách *IPSec*.Bạn có thể cho quy tắc này không hoạt động *(deactivate)*, nhưng không thể gỡ bỏ nó.

Server (Request Security): Chính sách này quy định máy tính của bạn chủ động cố gắng khởi tạo *IPSec* mỗi khi thiết lập kết nối với các máy tính khác, nhưng nếu máy *client* không thể dùng *IPSec* thì *server* vẫn chấp nhận kết nối không dùng *IPSec*.Chính sách này có ba quy tắc chứa các thiết lập sau:

Rule 1

+ IP Filter List: *All IP Traffic* (Tất cả các gói dữ liệu dựa trên giao thức IP)
+ Filter Action: *Request Security (Optional)*
+ Authentication: *Kerberos*
+ Tunnel Setting: *None*
Connection Type: *All*

Rule 2

+ IP Filter List: *All ICMP Traffic* (Tất cả các gói dữ liệu dựa trên giao thức ICMP)
+ Filter Action: *Permit*
+ Authentication: *N/A*
+ Tunnel Setting: *None*
+ Connection Type: *All*

Rule 3 (Default Response Rule)

+ IP Filter List: *<Dynamic>*
+ Filter Action: *Default Response*
+ Authentication: *Kerberos*
+ Tunnel Setting: *None*
+ Connection Type: *All*

Secure Server (Require Security): Chính sách này quy định không cho phép bất kỳ phiên trao đổi dữ liệu nào với *server* hiện tại mà không dùng *IPSec*.Chính sách này có ba quy tắc chứa các thiết lập sau:

Rule 1

+ IP Filter List: *All IP Traffic*
+ Filter Action: *Require Security*
+ Authentication: *N/A*
+ Tunnel Setting: *None*
+ Connection Type: *All*

Rule 2

+ IP Filter List: *All ICMP Traffic*
+ Filter Action: *Permit*
+ Authentication: *Kerberos*
+ Tunnel Setting: *None*
+ Connection Type: *All*

Rule 3 (Default Response Rule)

+ IP Filter List: *<Dynamic>*
+ Filter Action: *Default Response*
+ Authentication: *Kerberos*
+ Tunnel Setting: *None*
+ Connection Type: *All*

5. Ví dụ tạo chính sách IPSec đảm bảo một kết nối được mã hóa

Giả sử bạn có hai máy tính A và B.Máy A là *server* có địa chỉ IP 203.162.1.1 và máy B là *client* có địa chỉ IP 203.162.1.2.Bạn sẽ thiết lập một chính sách *IPSec* trên mỗi máy bằng cách thêm vào hai quy tắc *(rule),* trừ hai quy tắc có sẵn của hệ thống *(All ICMP Traffic* và *All IP Traffic)* gồm:

- ❖ Một quy tắc áp dụng cho dữ liệu truyền vào máy.
- ❖ Một quy tắc áp dụng cho dữ liệu truyền ra khỏi máy.

Quy tắc đầu tiên trên máy A gồm có:

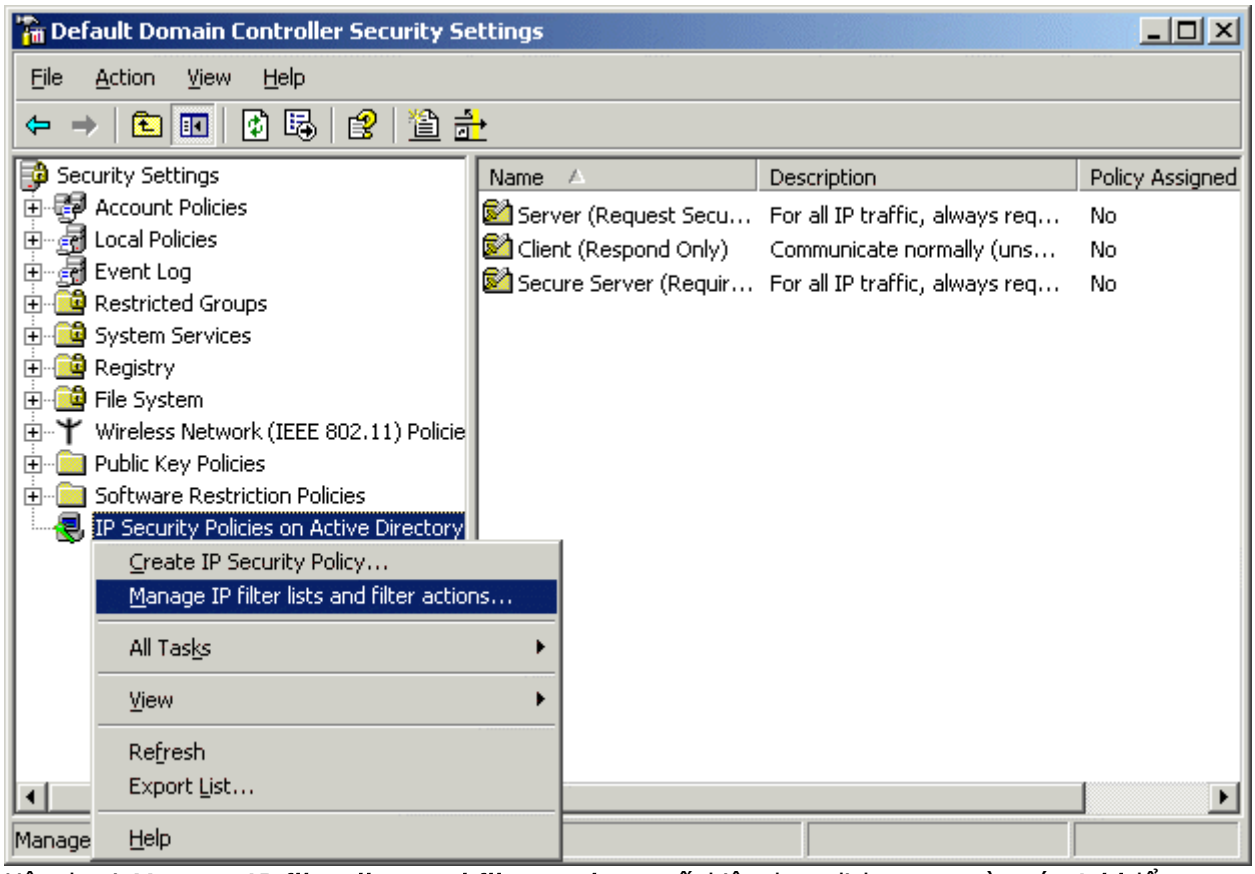
- Bộ lọc *(filter)*: Kích hoạt các quy tắc này khi có dữ liệu truyền đi *(outbound)* đến địa chỉ 203.162.1.2, qua bất kỳ cổng nào.
- Thao tác bảo mật *(action):* Mã hóa dữ liệu đó.
- Phương pháp chứng thực: Khóa dùng chung (chia sẻ) trước là chuỗi "hoasen".

Quy tắc thứ hai áp dụng cho máy A cũng tương tự nhưng bộ lọc có nội dung ngược lại là "dữ liệu truyền vào *(inbound)* từ địa chỉ 203.162.1.2"

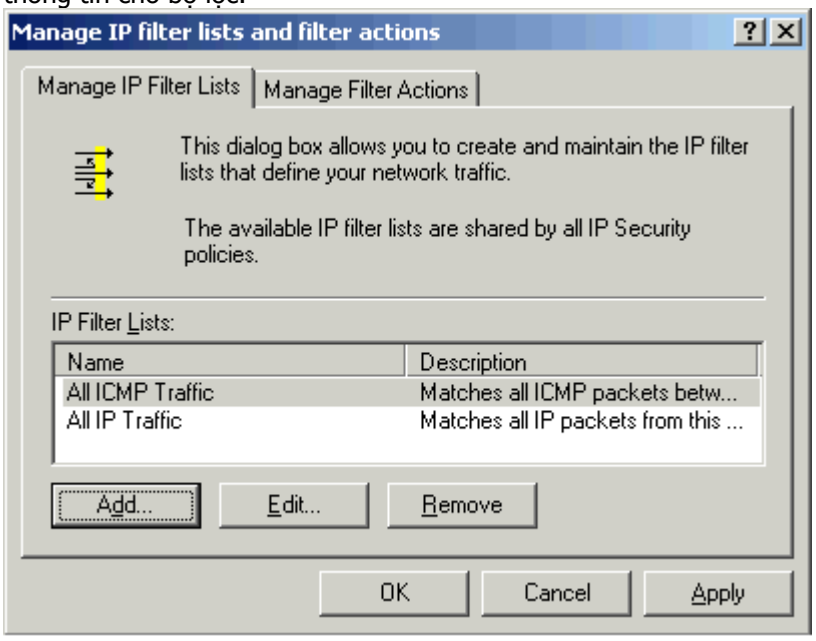
Chú ý: Để tạo ra một quy tắc là đầu tiên bạn phải quy định các bộ lọc và thao tác bảo mật, rồi sau đó mới tạo ra quy tắc từ các bộ lọc và thao tác bảo mật này.

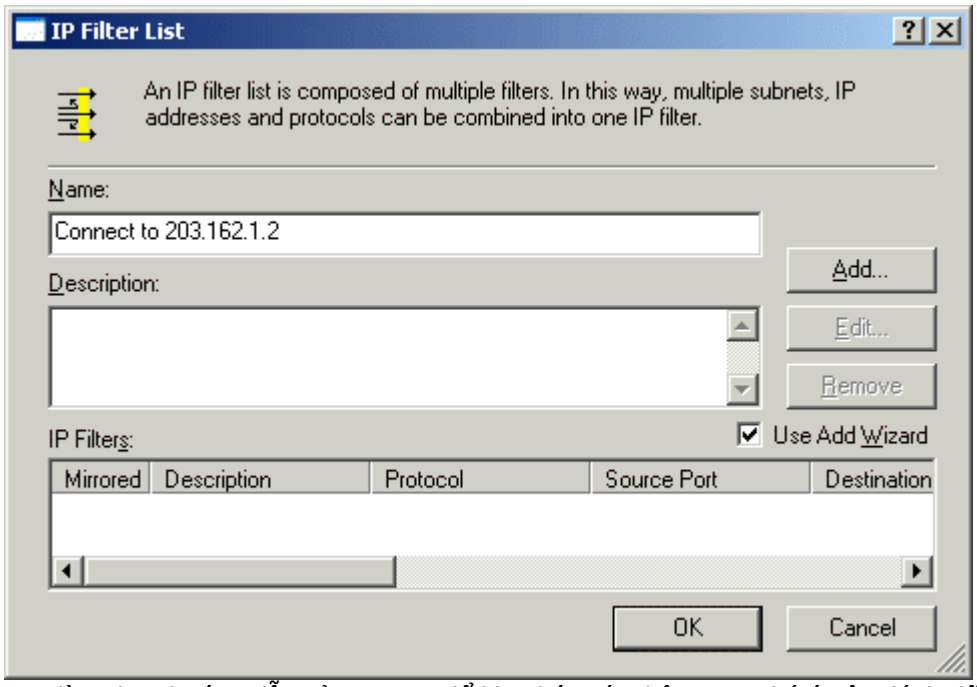
Các bước để thực hiện một chính sách *IPSec* theo yêu cầu trên như sau:

Trong khung bên trái của cửa sổ ***Default Domain Controller Security Settings***, bạn click mouse vào mục ***IP Security Policies on Active Directory*** và chọn ***Manage IP filter lists and filter actions***.

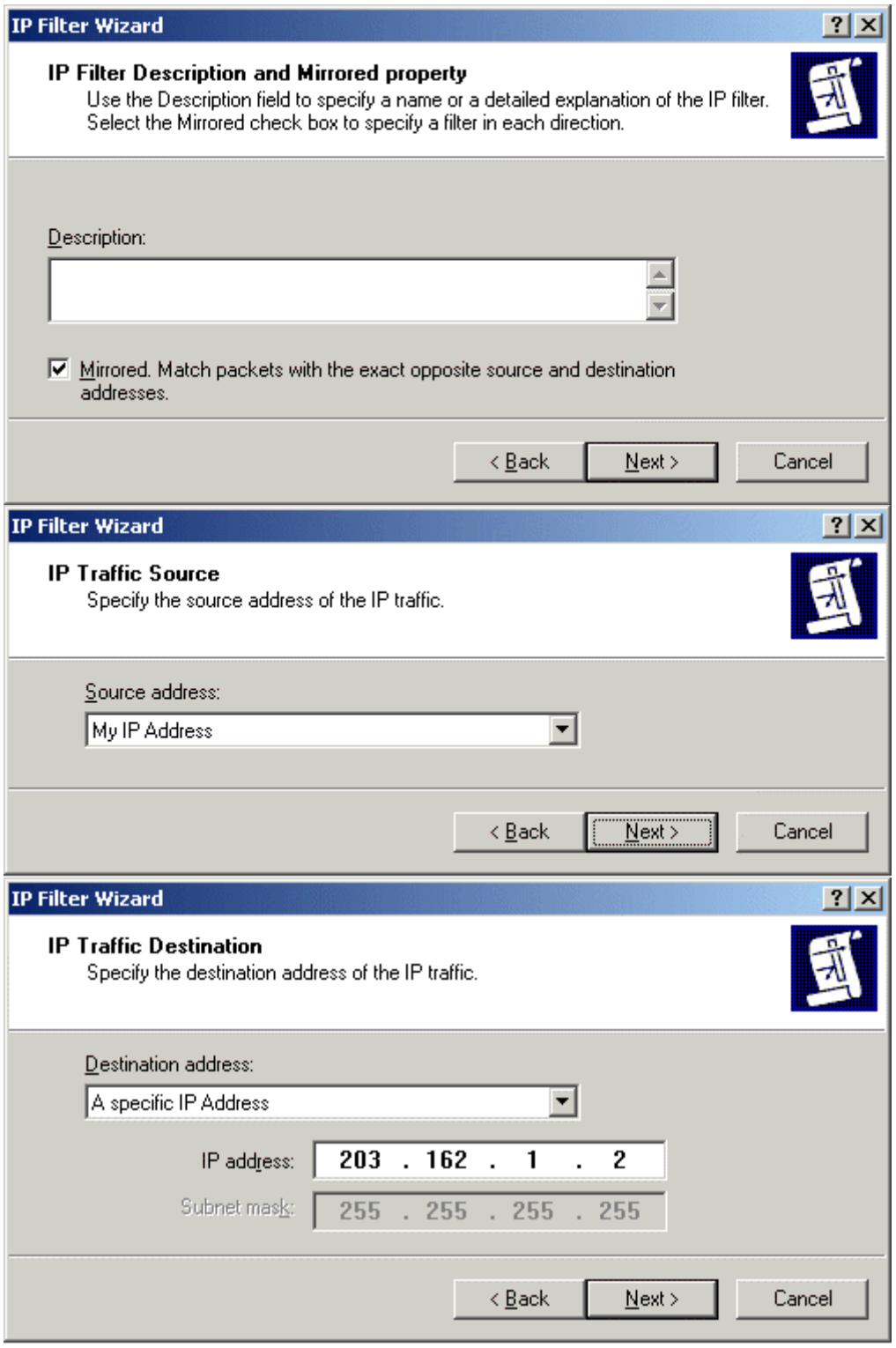


Hộp thoại ***Manage IP filter lists and filter actions*** xuất hiện, bạn click mouse vào nút ***Add*** để thêm một bộ lọc mới.Bạn nhập tên cho bộ lọc này, chẳng hạn *"Connect to 203.162.1.2"*.Bạn click tiếp vào nút ***Add*** để ***Wizard*** **(nhớ đánh dấu chọn *Use Add Wizard*)** hướng dẫn bạn khai báo các thông tin cho bộ lọc.





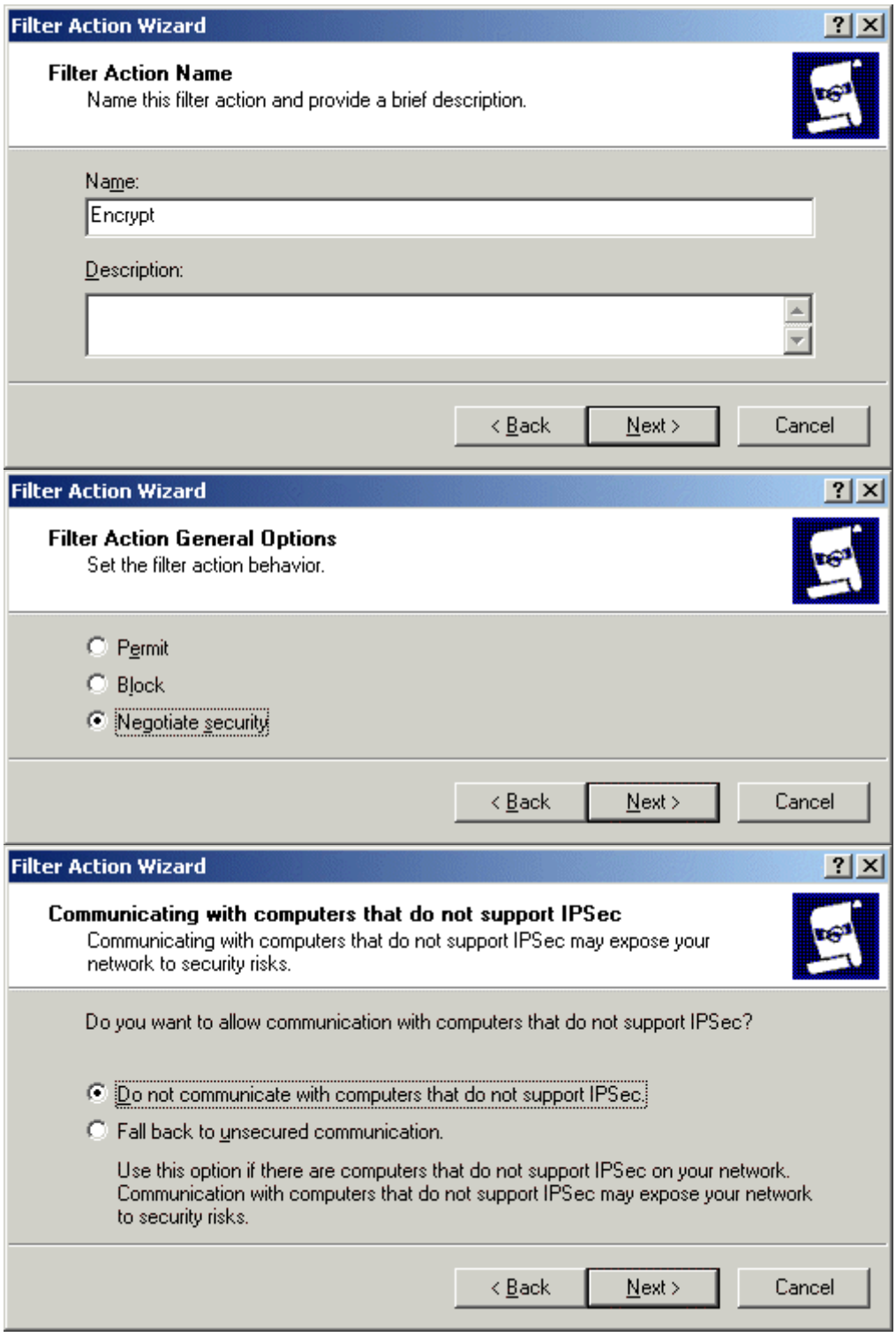
Bạn làm theo hướng dẫn của *Wizard* để khai báo các thông tin, chú ý nên đánh dấu vào mục *Mirrored* để quy tắc này có ý nghĩa hai chiều, bạn không cần phải tốn công để tạo ra hai quy tắc.Mục ***Source address***, chọn ***My IP Address***, mục ***Destination address*** chọn ***A specific IP Address*** và nhập vào địa chỉ "203.162.1.2". Mục ***IP Protocol Type*** bạn để giá trị mặc định và click nút ***Finish*** để hoàn tất việc khai báo và click ***OK*** để quay về hộp thoại ***Manage IP filter lists and filter actions***.


IP Filter Wizard
IP Filter Description and Mirrored property
Use the Description field to specify a name or a detailed explanation of the IP filter.
Select the Mirrored check box to specify a filter in each direction.
Description:
Mirrored. Match packets with the exact opposite source and destination addresses.
< Back
Next >
Cancel
IP Filter Wizard
IP Traffic Source
Specify the source address of the IP traffic.
Source address:
My IP Address
< Back
Next >
Cancel
IP Filter Wizard
IP Traffic Destination
Specify the destination address of the IP traffic.
Destination address:
A specific IP Address
IP address:
203 . 162 . 1 . 2
Subnet mask:
255 . 255 . 255 . 255
< Back
Next >
Cancel

Chọn thẻ ***Manage Filter Actions*** để tạo ra các thao tác bảo mật.Click mouse vào nút ***Add***.Trình ***Wizard*** sẽ hướng dẫn bạn khai báo các thông tin về thao tác.Bạn đặt tên cho thao tác này, chẳng hạn là ***Encrypt***.Trong mục ***Filter Action*** bạn chọn ***Negotiate security***, trong mục ***IP Traffic Security*** bạn chọn ***Integrity and encryption***.


Manage IP filter lists and filter actions
Manage IP Filter Lists
Manage Filter Actions
This dialog box allows you to create and maintain the filter actions that define the security of your network.
The available filter actions are shared by all IP Security policies.
Filter Actions:
Name
Description
Permit
Permit unsecured IP packets to ...
Request Security (Optional)
Accepts unsecured communicati...
Require Security
Accepts unsecured communicati...
Add...
Edit...
Remove
Use Add Wizard
Close
Cancel
Apply

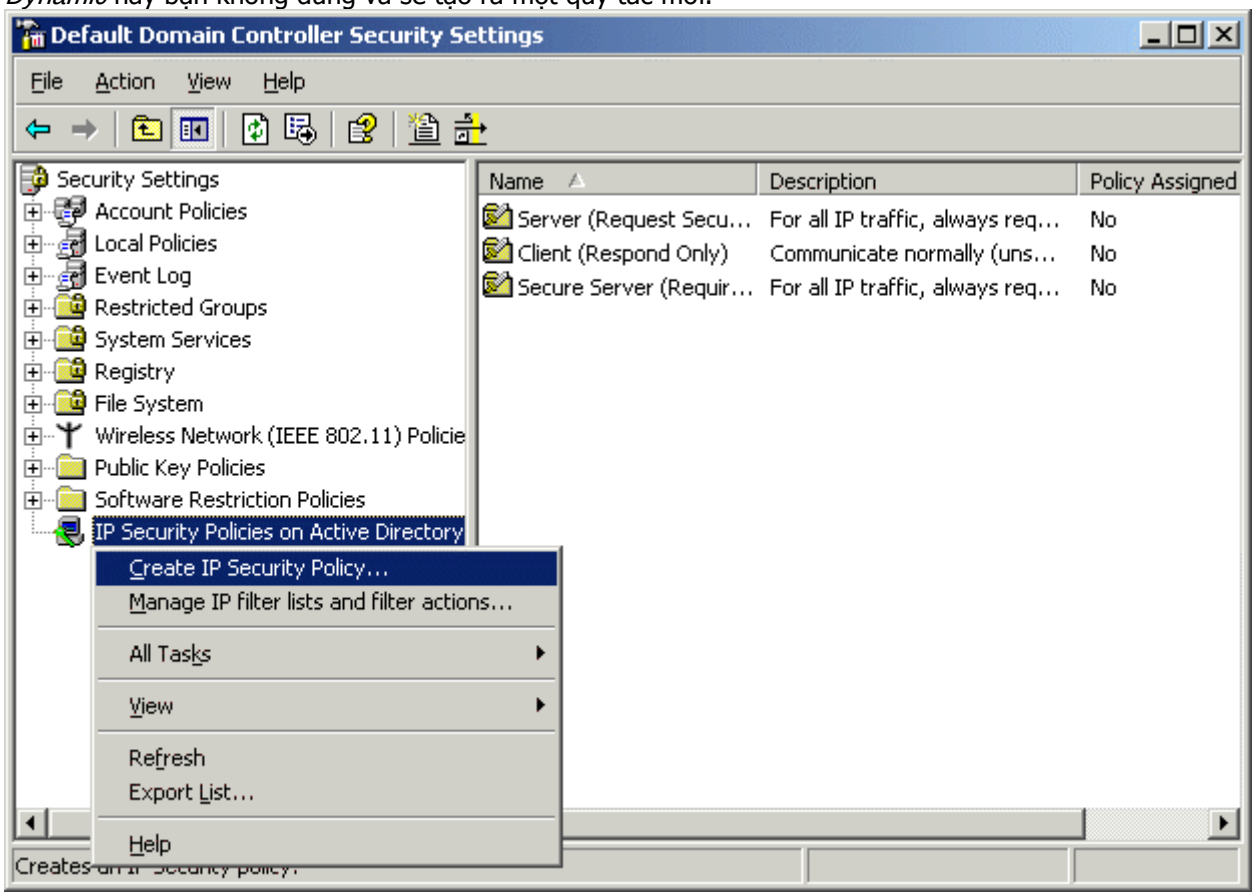

Filter Action Wizard
Welcome to the IP Security Filter Action Wizard
Use this wizard to specify properties for a new filter action.
A filter action sets the security requirements for a data transfer. These requirements are specified in a list of security methods contained in the filter action.
Data transfer is only possible when the computers involved use the same security methods. Multiple security methods increase the chance that two computers will use the same method.
To continue, click Next.
< Back
Next >
Cancel

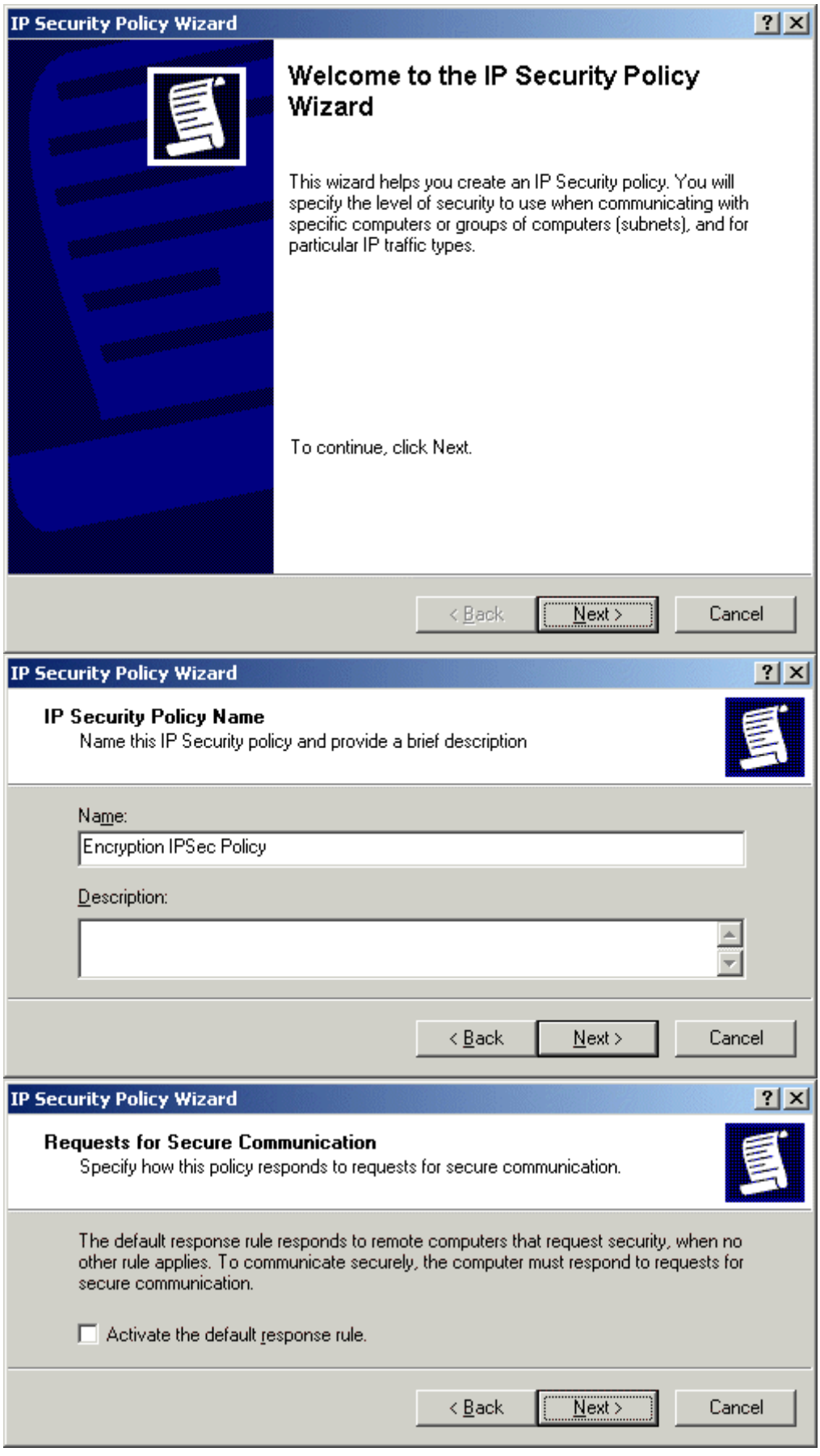

Filter Action Wizard
Filter Action Name
Name this filter action and provide a brief description.
Name:
Encrypt
Description:
< Back
Next >
Cancel
Filter Action Wizard
Filter Action General Options
Set the filter action behavior.
Permit
Block
Negotiate security
< Back
Next >
Cancel
Filter Action Wizard
Communicating with computers that do not support IPSec
Communicating with computers that do not support IPSec may expose your network to security risks.
Do you want to allow communication with computers that do not support IPSec?
Do not communicate with computers that do not support IPSec.
Fall back to unsecured communication.
Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.
< Back
Next >
Cancel


Filter Action Wizard
IP Traffic Security
Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.
This filter action requires at least one security method for IP traffic.
Integrity and encryption
Data will be encrypted, authenticated, and unmodified.
Integrity only
Data will be authenticated and unmodified, but will not be encrypted.
Custom
Settings...
< Back
Next >
Cancel

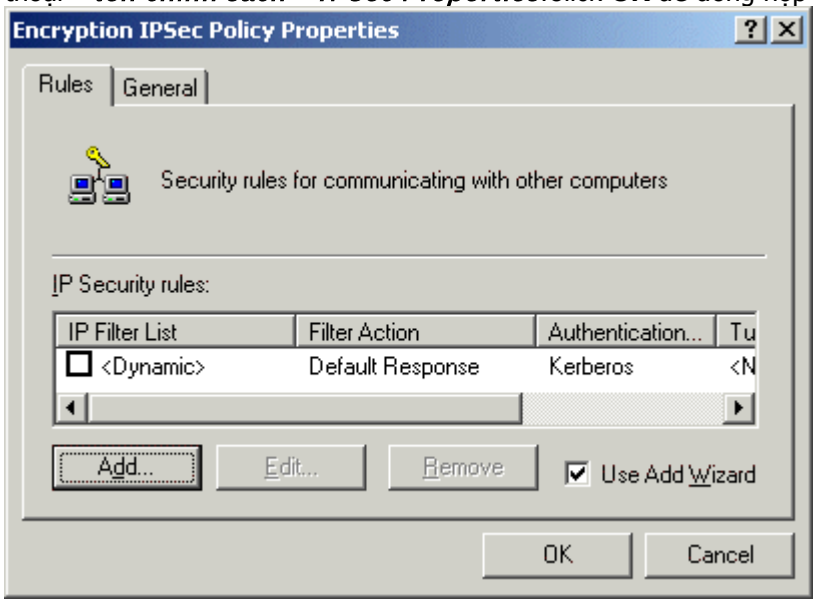

Filter Action Wizard
Completing the IP Security Filter Action Wizard
You have successfully completed the IP Security Filter Action Wizard.
To edit your filter action now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

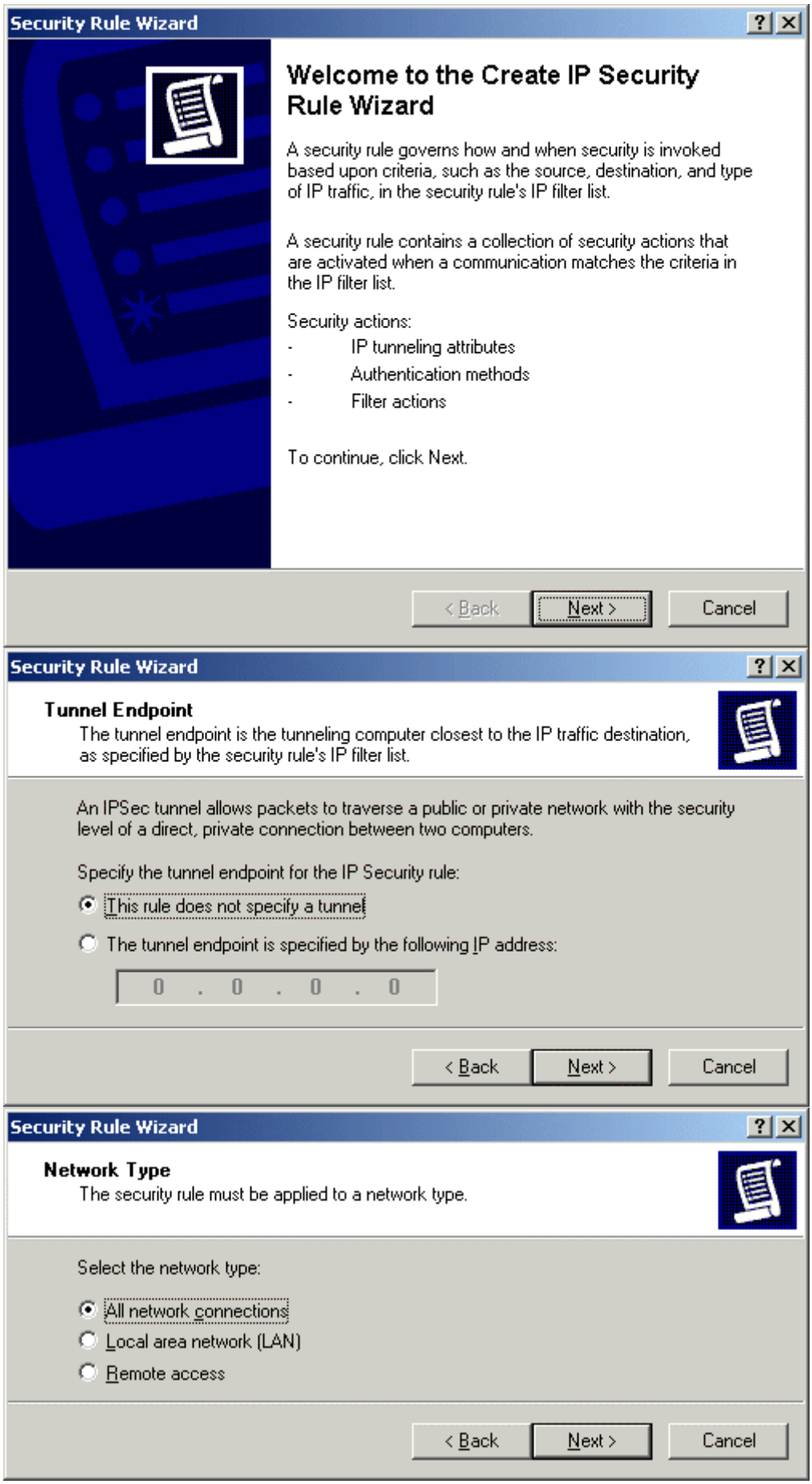
Tiếp theo là bạn tạo một chính sách *IPSec* trong đó chứa một quy tắc kết hợp giữa bộ lọc và thao tác vừa tạo ở bước 4.Trong khung trái của cửa sổ ***Default Domain Controller Security Settings***, click mouse phải vào mục ***IP Security Policies on Active Directory*** rồi chọn ***Create IP Security Policy*** và làm theo hướng dẫn của ***Wizard***. Bạn nhập tên của chính sách vào, chẳng hạn ***Encryption IPSec***, tiếp theo bạn phải bỏ đánh dấu trong mục ***Active the default response rule*** để bỏ qua *quy tắc hỏi đáp mặc định có hiệu lực*.Các giá trị còn lại bạn để mặc định vì quy tắc *Dynamic* này bạn không dùng và sẽ tạo ra một quy tắc mới.

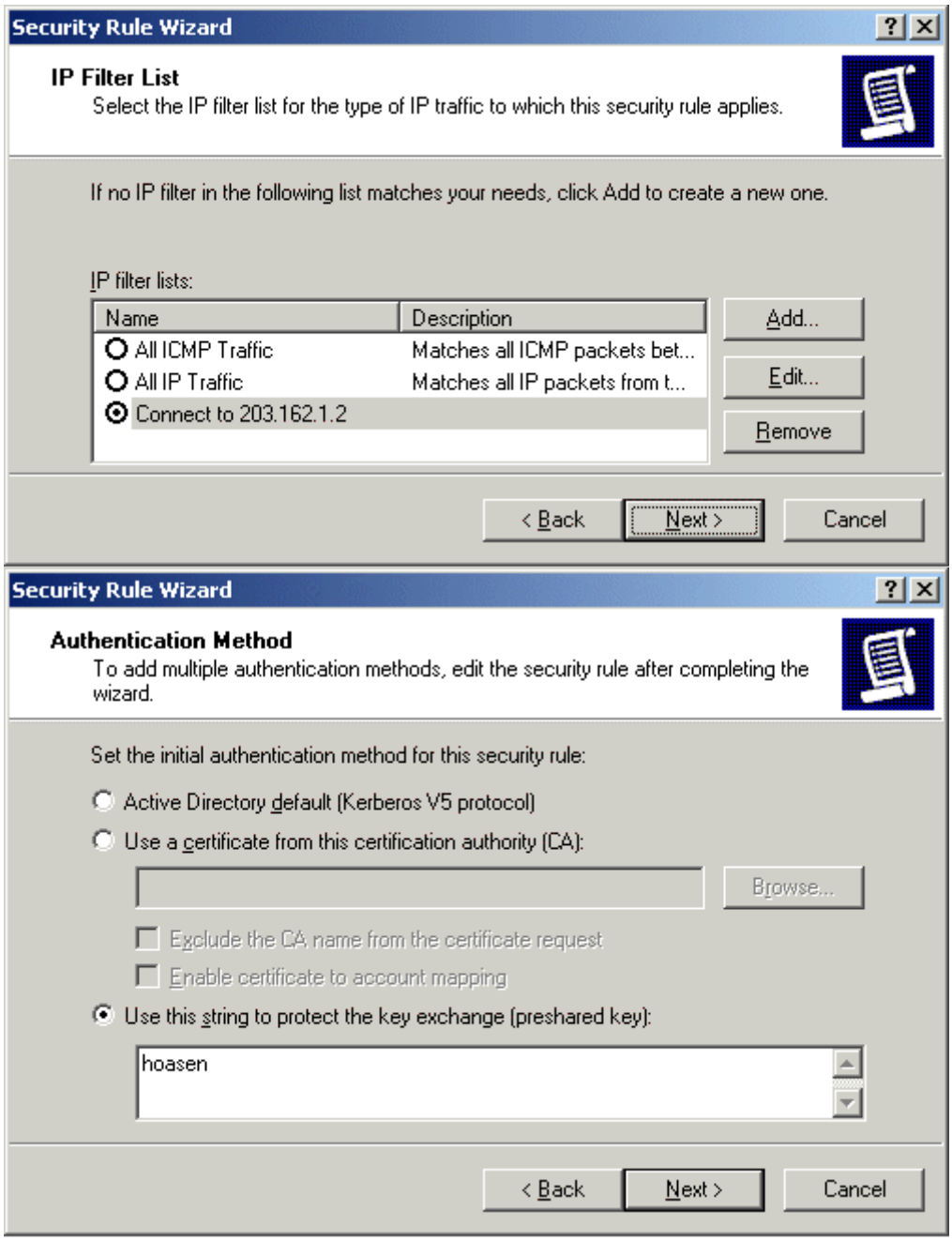


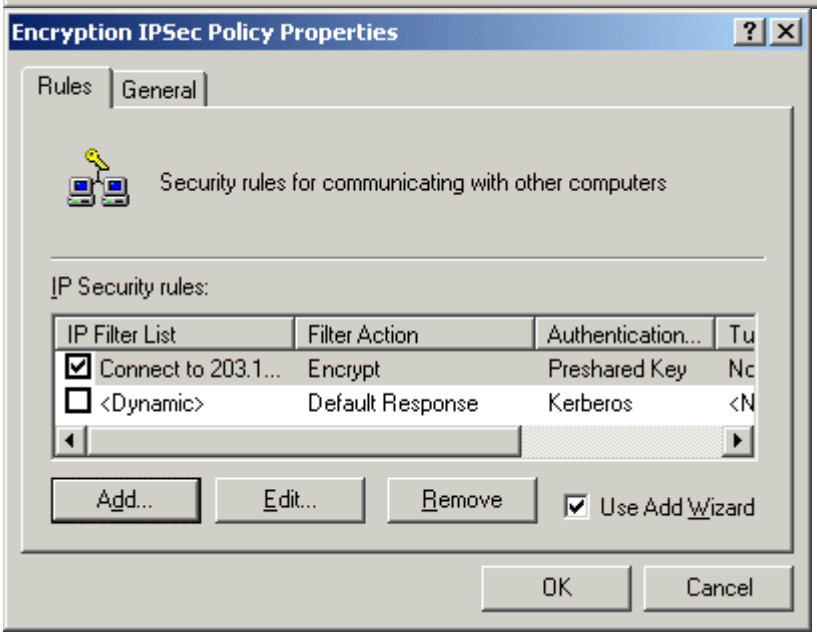

IP Security Policy Wizard
Welcome to the IP Security Policy Wizard
This wizard helps you create an IP Security policy. You will specify the level of security to use when communicating with specific computers or groups of computers (subnets), and for particular IP traffic types.
To continue, click Next.
< Back
Next >
Cancel
IP Security Policy Wizard
IP Security Policy Name
Name this IP Security policy and provide a brief description
Name:
Encryption IPSec Policy
Description:
< Back
Next >
Cancel
IP Security Policy Wizard
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Activate the default response rule.
< Back
Next >
Cancel

Trong hộp thoại ***<tên chính sách> IPSec Properties***, bạn click mouse vào nút ***Add*** để tạo ra quy tắc mới.***Wizard*** sẽ hướng dẫn bạn từng bước thực hiện, đến mục chọn bộ lọc bạn chọn bộ lọc vừa tạo ở bước trên tên là *"Connect to 203.162.1.2"*, mục chọn thao tác, bạn chọn thao tác vừa tạo tên là *"Encrypt"*.Đến mục chọn phương pháp chứng thực bạn chọn mục ***Use this string to protect the key exchange*** và nhập chuỗi làm khóa để mã hóa dữ liệu, chẳng hạn "hoasen".Sau đó, click ***Finish*** để hoàn tất việc tạo một quy tắc. Tên quy tắc sẽ xuất hiện trong khung ***IP Security Rule*** của hộp thoại ***<tên chính sách> IPSec Properties***.Click **OK** để đóng hộp thoại này.

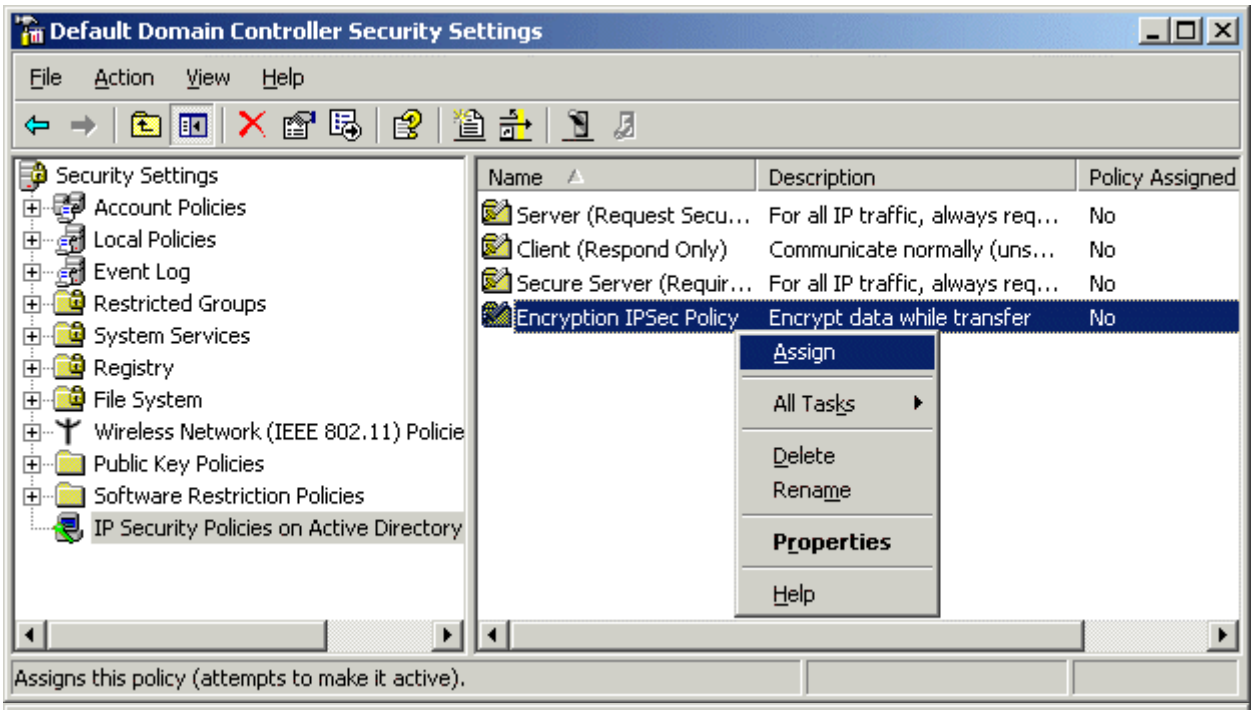


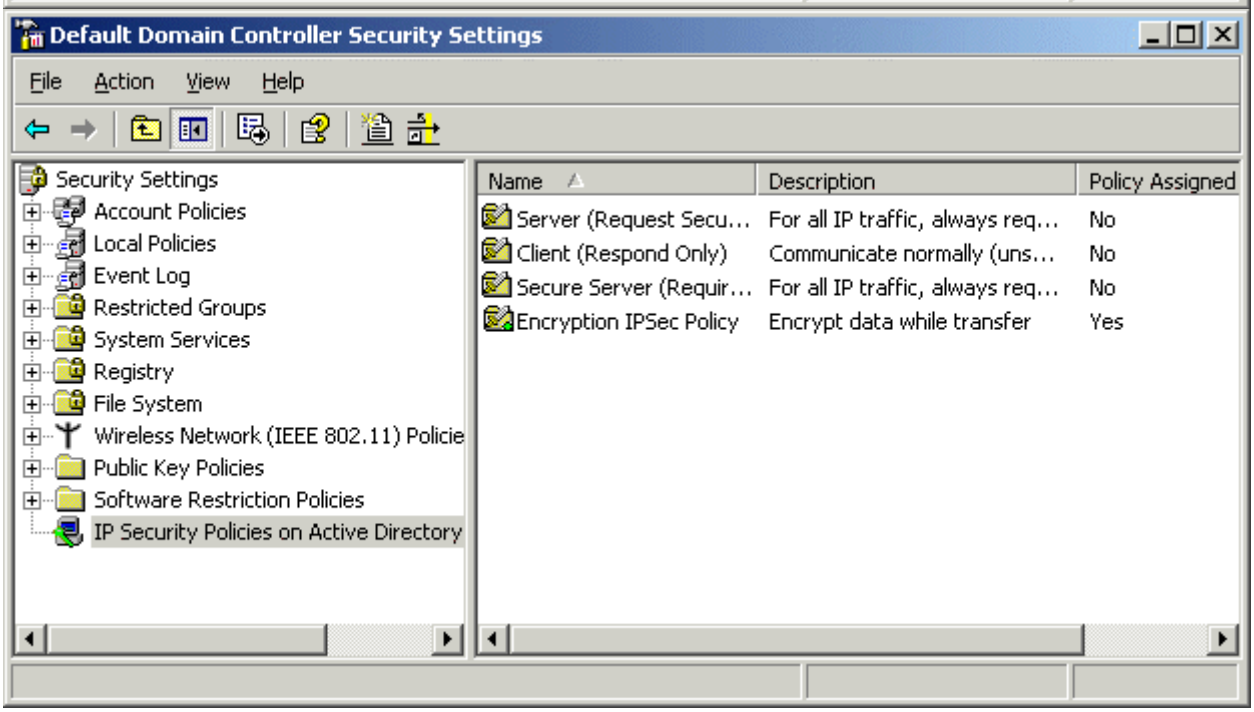

Security Rule Wizard
Welcome to the Create IP Security Rule Wizard
A security rule governs how and when security is invoked based upon criteria, such as the source, destination, and type of IP traffic, in the security rule's IP filter list.
A security rule contains a collection of security actions that are activated when a communication matches the criteria in the IP filter list.
Security actions:
- IP tunneling attributes
- Authentication methods
- Filter actions
To continue, click Next.
< Back
Next >
Cancel
Security Rule Wizard
Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.
An IPSec tunnel allows packets to traverse a public or private network with the security level of a direct, private connection between two computers.
Specify the tunnel endpoint for the IP Security rule:
This rule does not specify a tunnel
The tunnel endpoint is specified by the following IP address:
0 . 0 . 0 . 0
< Back
Next >
Cancel
Security Rule Wizard
Network Type
The security rule must be applied to a network type.
Select the network type:
All network connections
Local area network (LAN)
Remote access
< Back
Next >
Cancel


Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
Connect to 203.162.1.2
Add...
Edit...
Remove
< Back
Next >
Cancel
Security Rule Wizard
Authentication Method
To add multiple authentication methods, edit the security rule after completing the wizard.
Set the initial authentication method for this security rule:
Active Directory default (Kerberos V5 protocol)
Use a certificate from this certification authority (CA):
Browse...
Exclude the CA name from the certificate request
Enable certificate to account mapping
Use this string to protect the key exchange (preshared key):
hoasen
< Back
Next >
Cancel

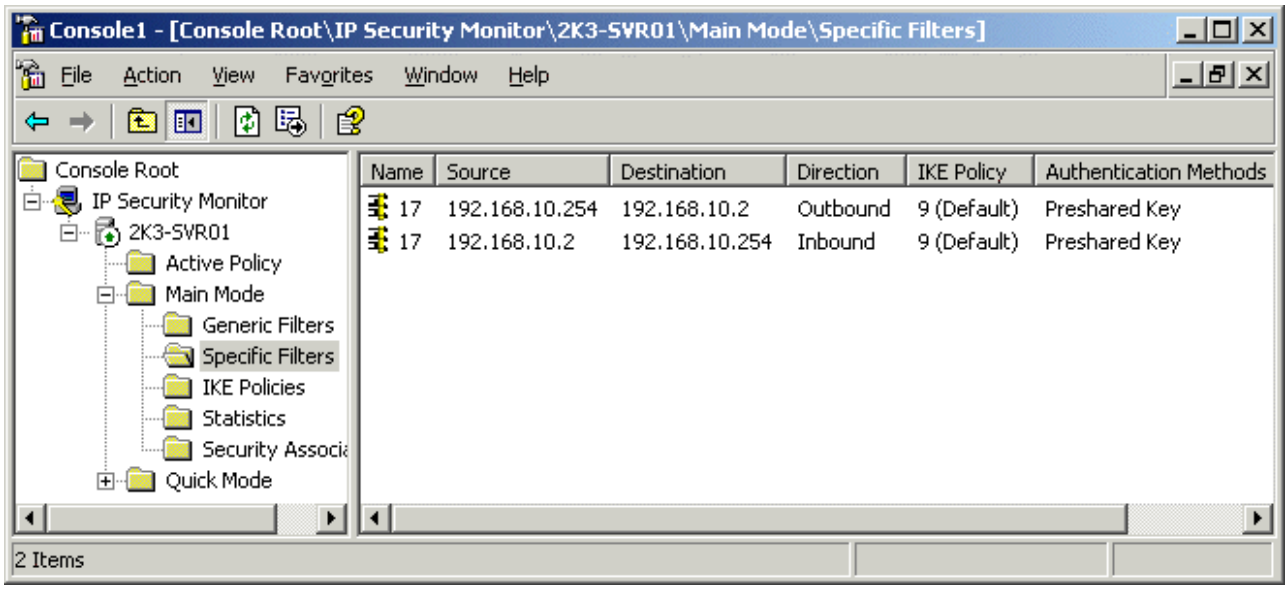


Bạn đã hoàn tất công việc thiết lập chính sách *IPSec* theo yêu cầu.Trong khung phải của cửa sổ ***Default Domain Controller Security Settings***, click mouse phải vào chính sách *Encryption IPSec* và chọn *Assign* để chính sách này được hoạt động trên hệ thống máy *server* (máy A).



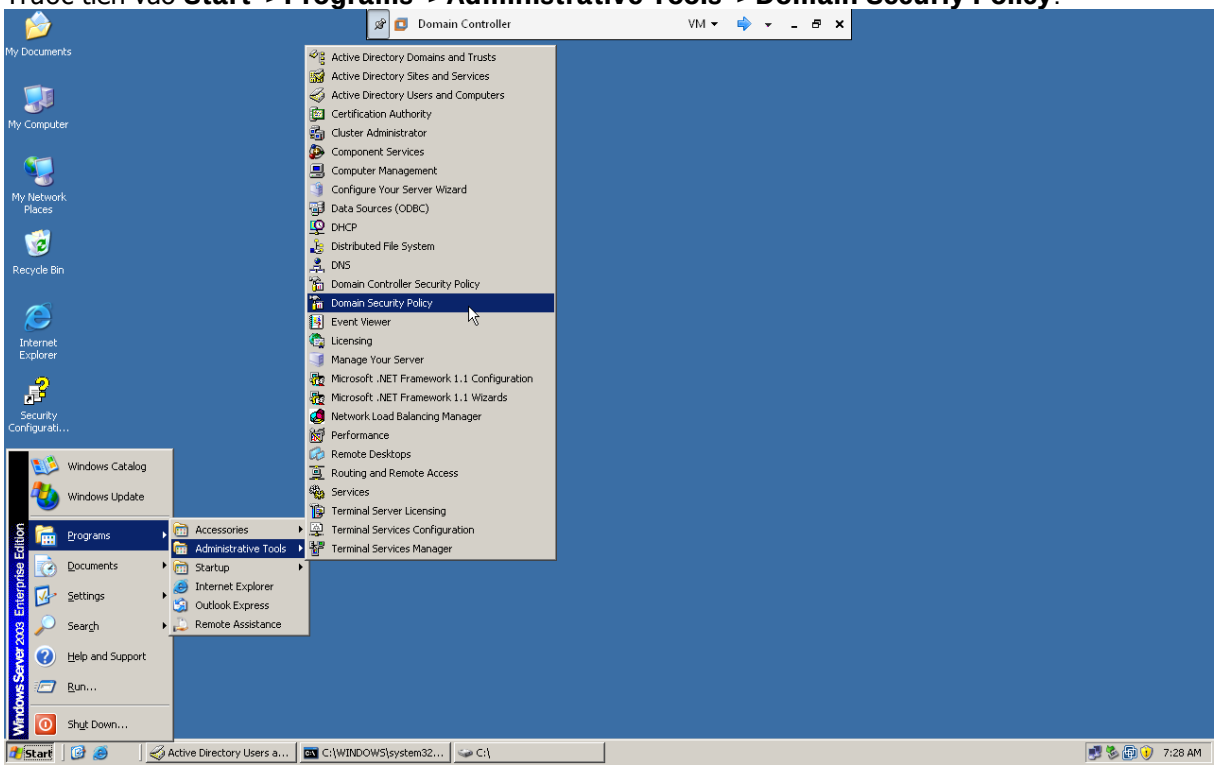


Tiếp theo, bạn sẽ tạo chính sách *IPSec* giống như vậy cho máy B và thay các IP 203.162.1.2 bằng 203.162.1.1.Bạn có thể kiểm tra việc mã hóa dữ liệu đã diễn ra giữa hai máy bằng console ***IP Security Monitor*** như sau: chọn ***Start -> Run*** và nhập vào ***mmc***.Chọn menu ***File -> Add/Remove Snap-in***.Trong hộp thoại ***Add/Remove Snap-in*** click nút ***Add***.Trong hộp thoại ***Add Stanalone Snap-in*** chọn ***IP Security Monitor***, click nút ***Add*** và click nút ***Close*** để đóng hộp thoại này lại.Click nút ***OK*** để đóng hộp thoại ***Add/Remove Snap-in***. Mở rộng mục ***IP Security Monitor -> <Computer_name>*** và chọn một trong hai cách kiểm tra: ***Main Mode*** và ***Quick Mode***.

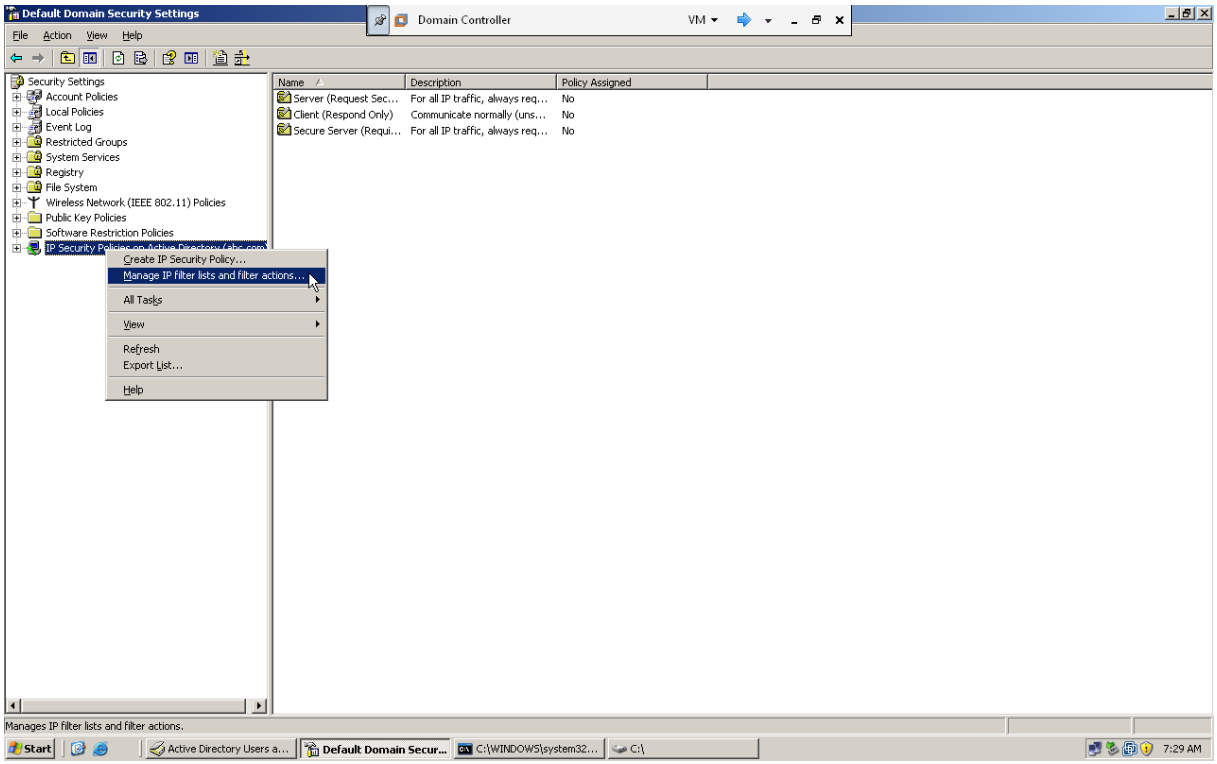


6. Ví dụ tạo chính sách IP Sec chỉ cho phép 1 máy tính trong mạng truy cập tài nguyên hệ thống

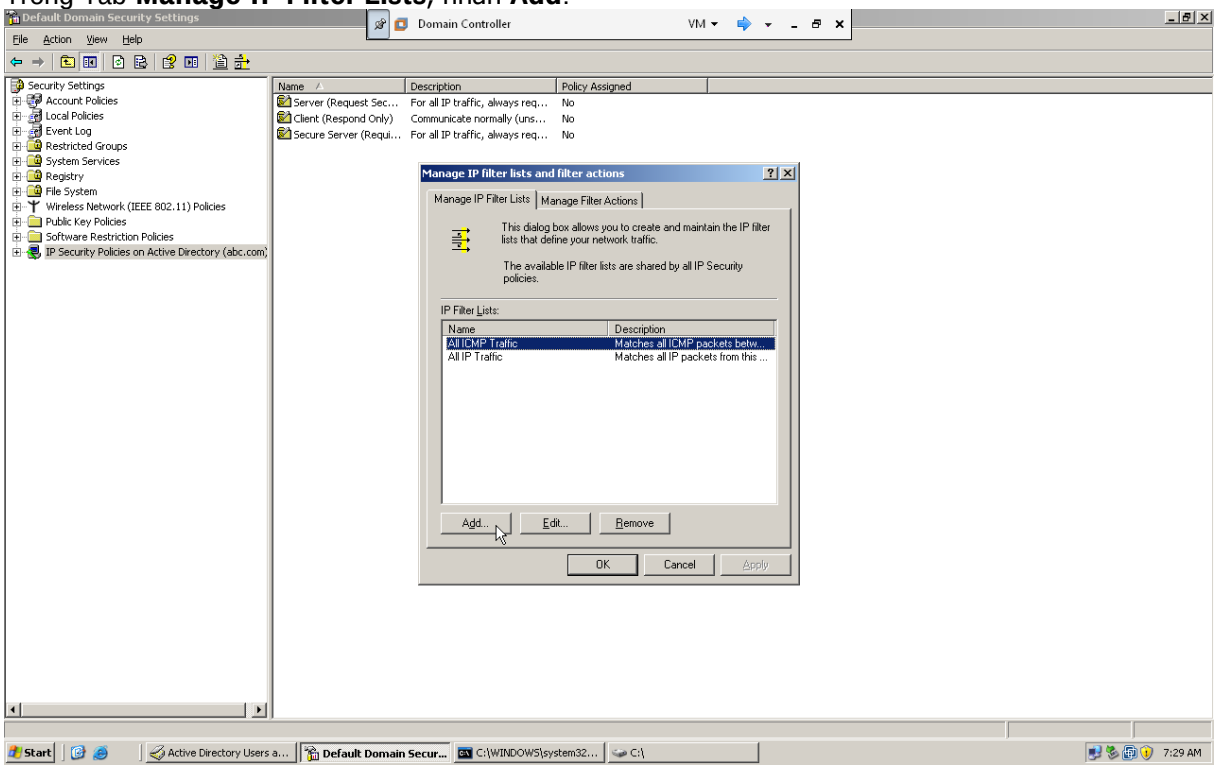
Trước tiên vào **Start->Programs->Administrative Tools->Domain Securiy Policy**:



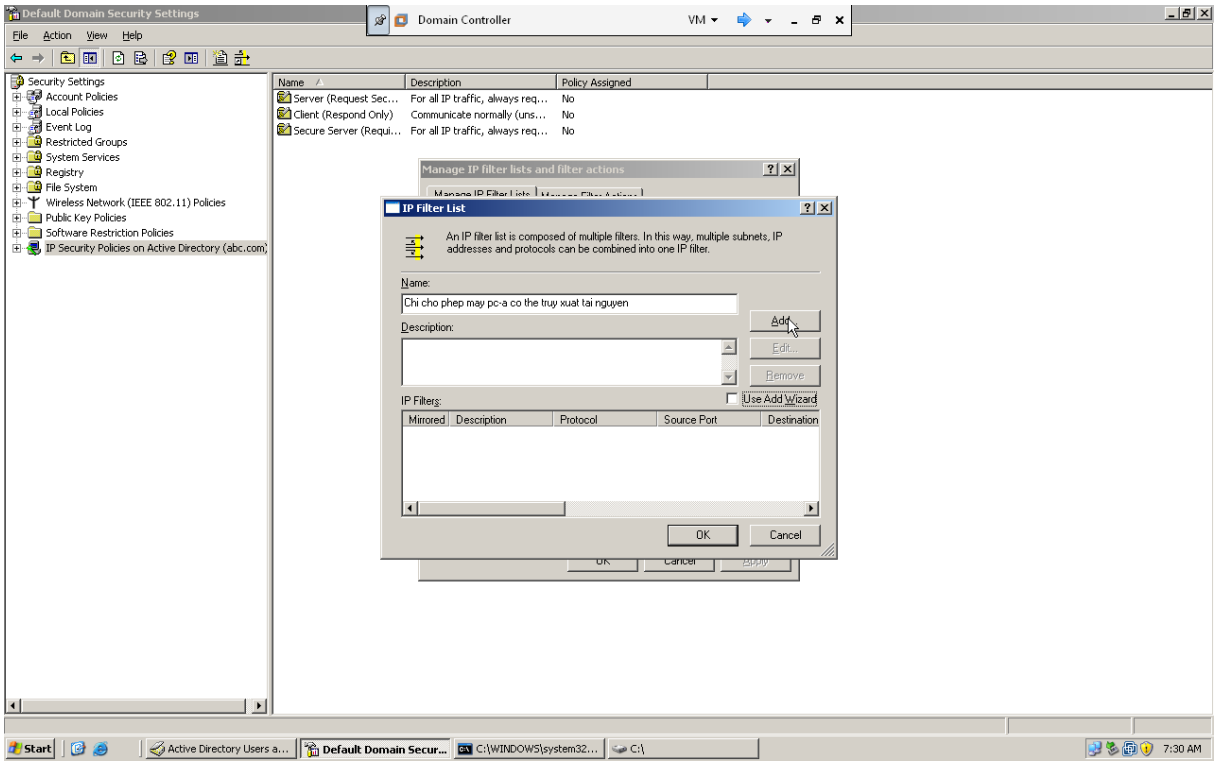
Chọn **IPSec Security Policies on Active Directory (tên domain) ->Manage IP filter lists and filter actions**:



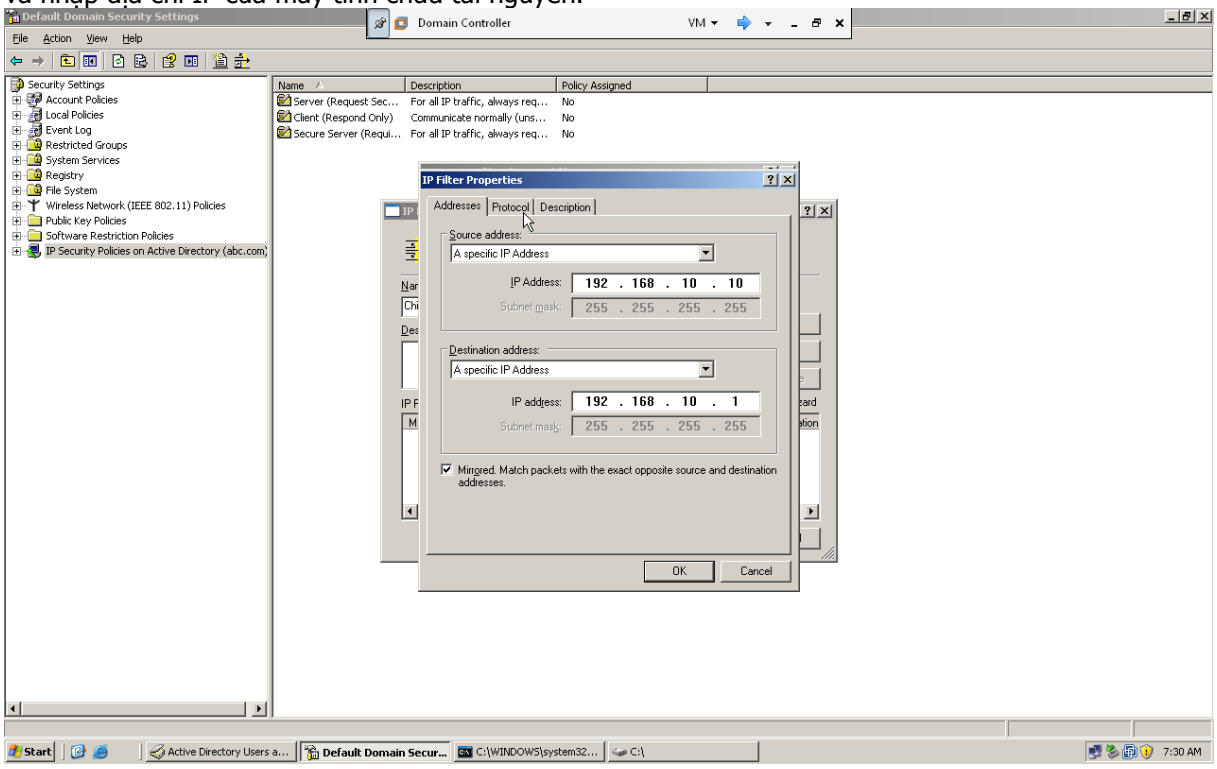
Trong Tab **Manage IP Filter Lists**, nhấn **Add**:



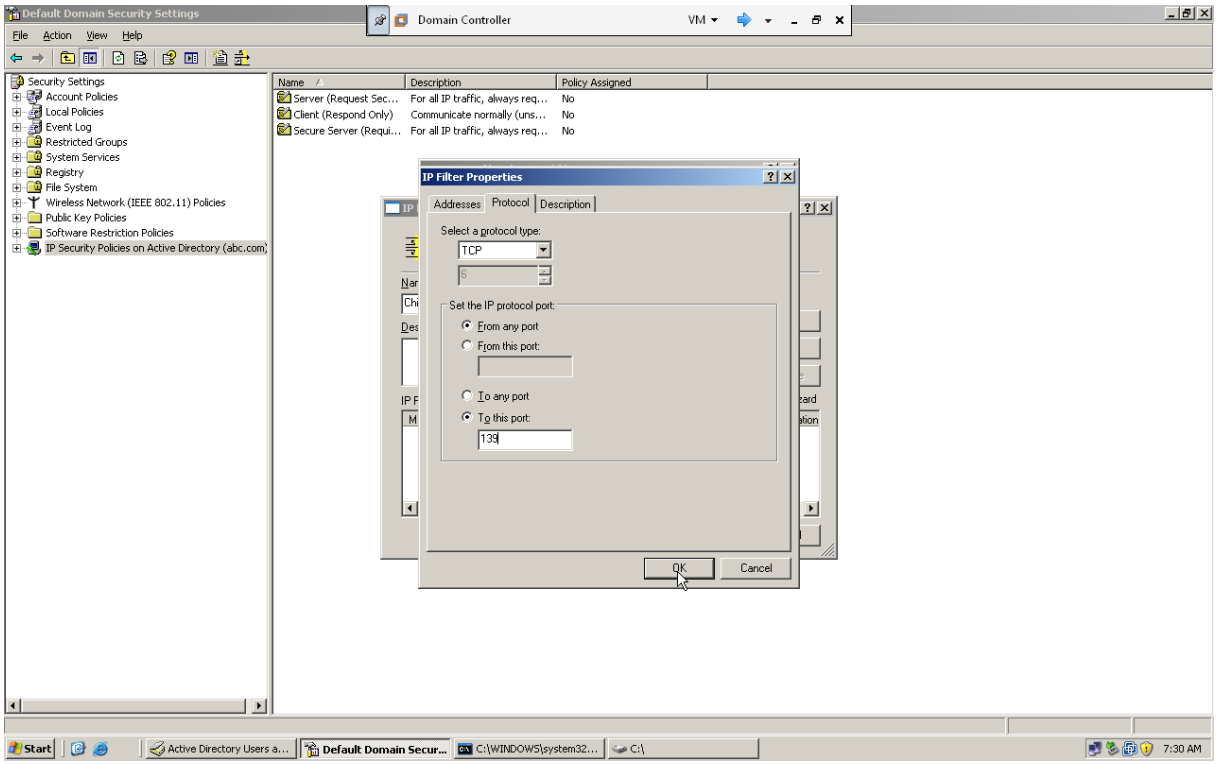
Đặt tên cho **IP Filter List "Chi cho phep may pc-a co the truy xuat tai nguyen"**, bỏ tùy chọn **Use Add Wizard**, nhấn **Add**:



Trong Tab **Addresses**, **Source Address** chọn **A specific IP Address** và nhập địa chỉ IP của máy tính mà chúng ta cho phép truy cập tài nguyên, **Destination Address chọn A specific IP Address** và nhập địa chỉ IP của máy tính chứa tài nguyên.

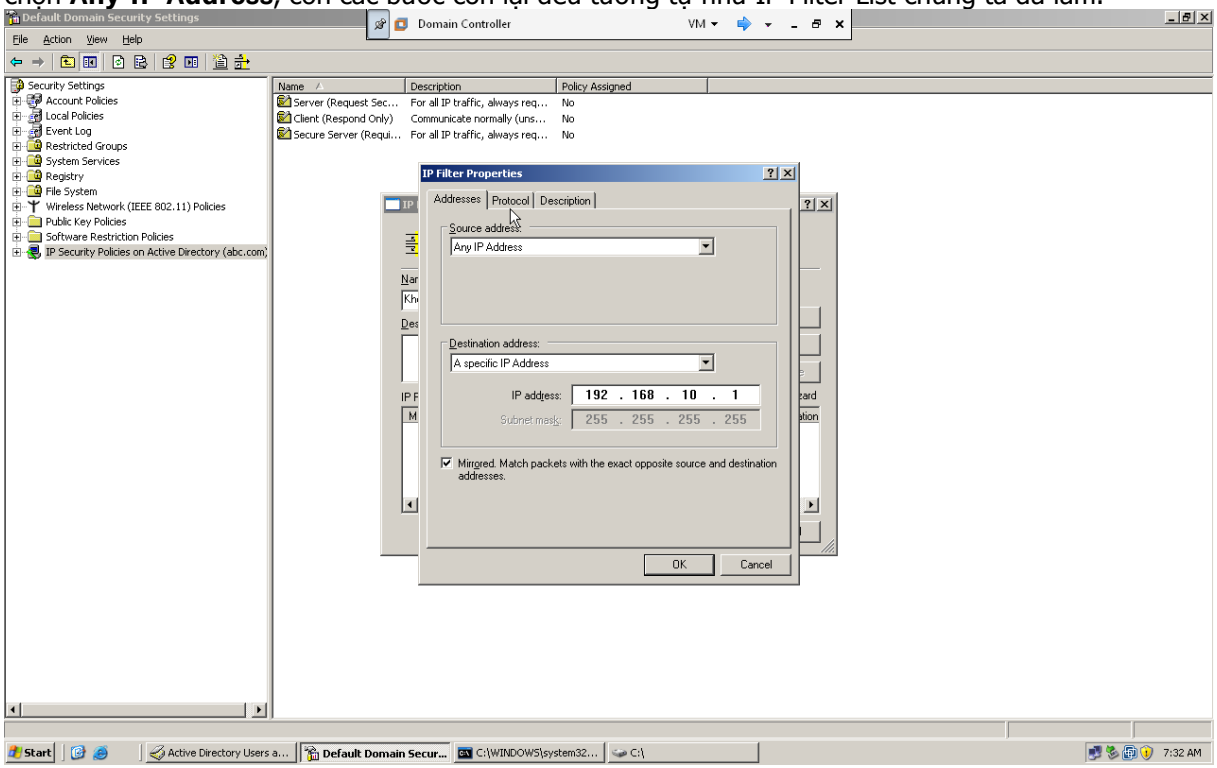


Chọn Tab **Protocol**, **Select a protocol type** chọn **TCP**, **Set the IP protocol port** chọn **From any port** và **To this port** là **139**:

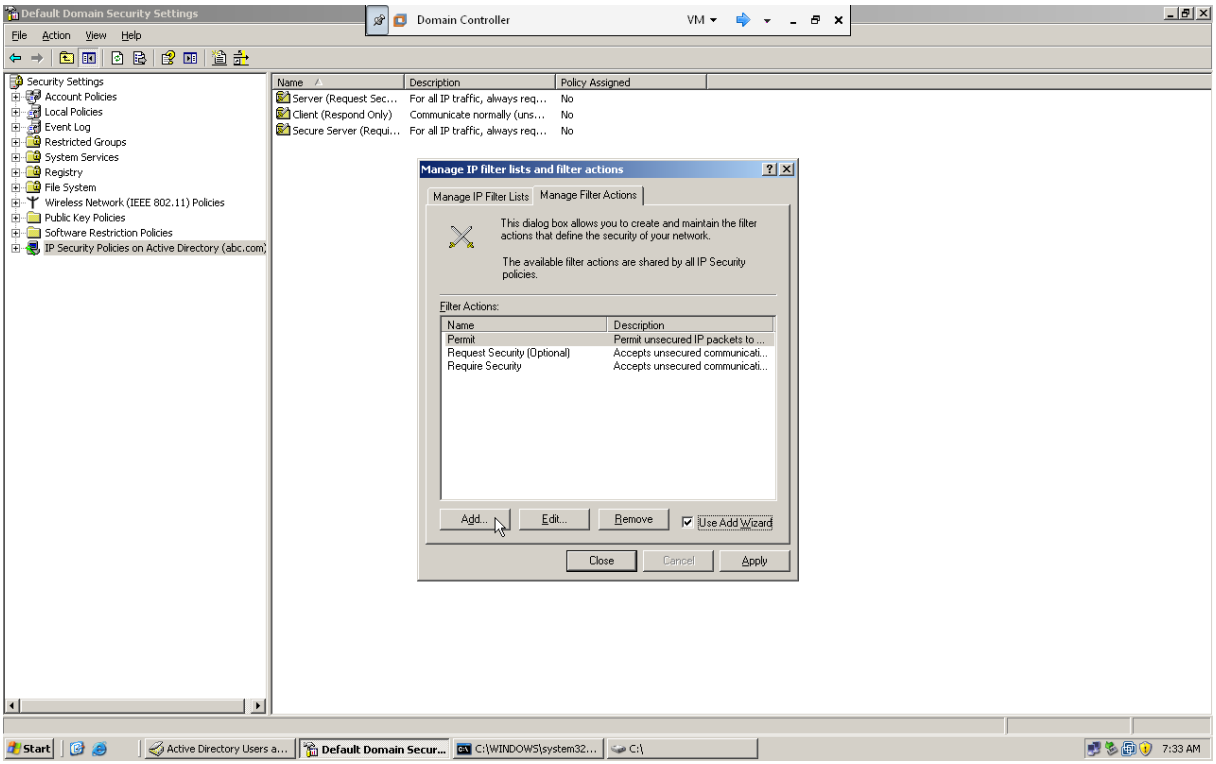


Nhấn **OK**, sau đó chúng ta làm tương tự nhấn **Add**, trong Tab **Addresses**, **Source Address** chọn **A specific IP Address** và nhập địa chỉ IP của máy tính mà chúng ta cho phép truy cập tài nguyên, **Destination Address chọn A specific IP Address** và nhập địa chỉ IP của máy tính chứa tài nguyên, chọn Tab **Protocol**, **Select a protocol type** chọn **TCP**, **Set the IP protocol port** chọn **From any port** và **To this port** là **445.**

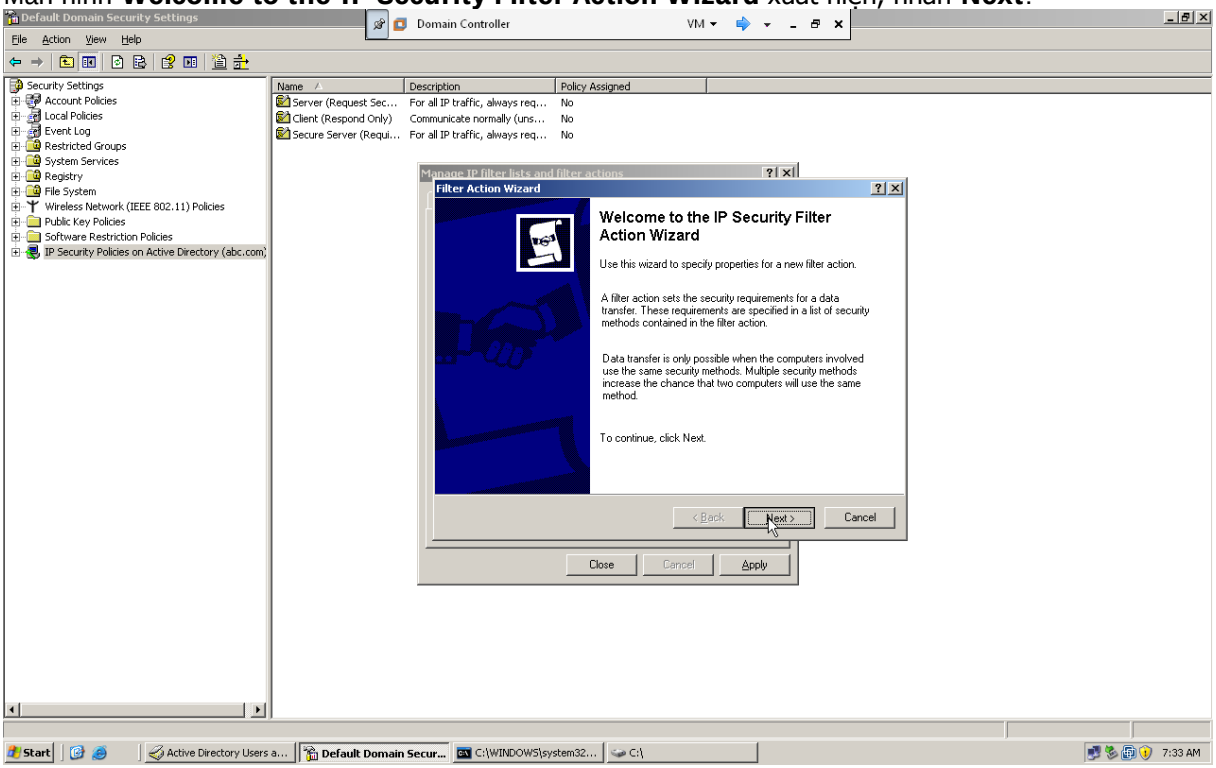
Sau đó nhấn **OK** để đóng cửa sổ IP Filter Lists, chúng ta làm tương tự để tạo một IP Filter List với tên "Khong cho phep con lai truy cap tai nguyen".Ở IP Filter List này, chỉ khác ở chỗ **Source Address** chọn **Any IP Address**, còn các bước còn lại đều tương tự như IP Filter List chúng ta đã làm.



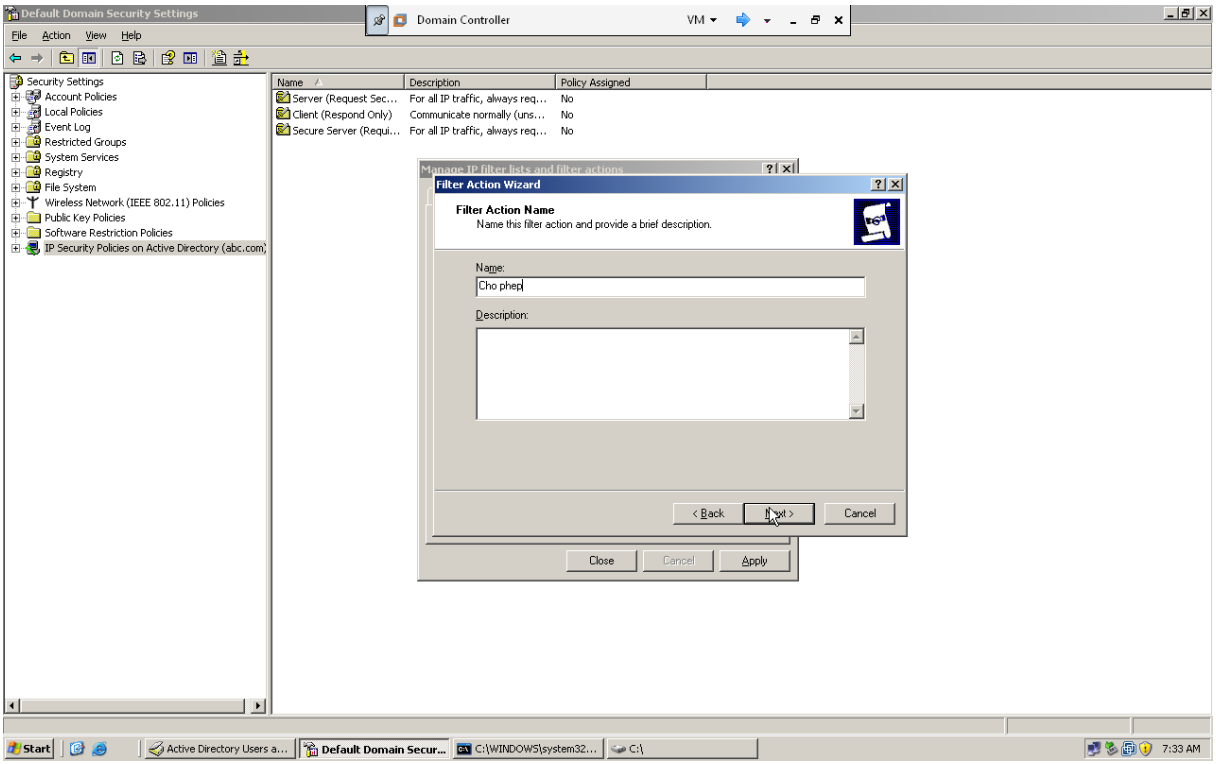
Bây giờ chúng ta sẽ tạo 2 Filter Action tương ứng với 2 Filter List chúng ta đã tạo chọn Tab **Manage Filter Actions**, chọn tùy chọn **Use Add Wizard**, nhấn **Add**:



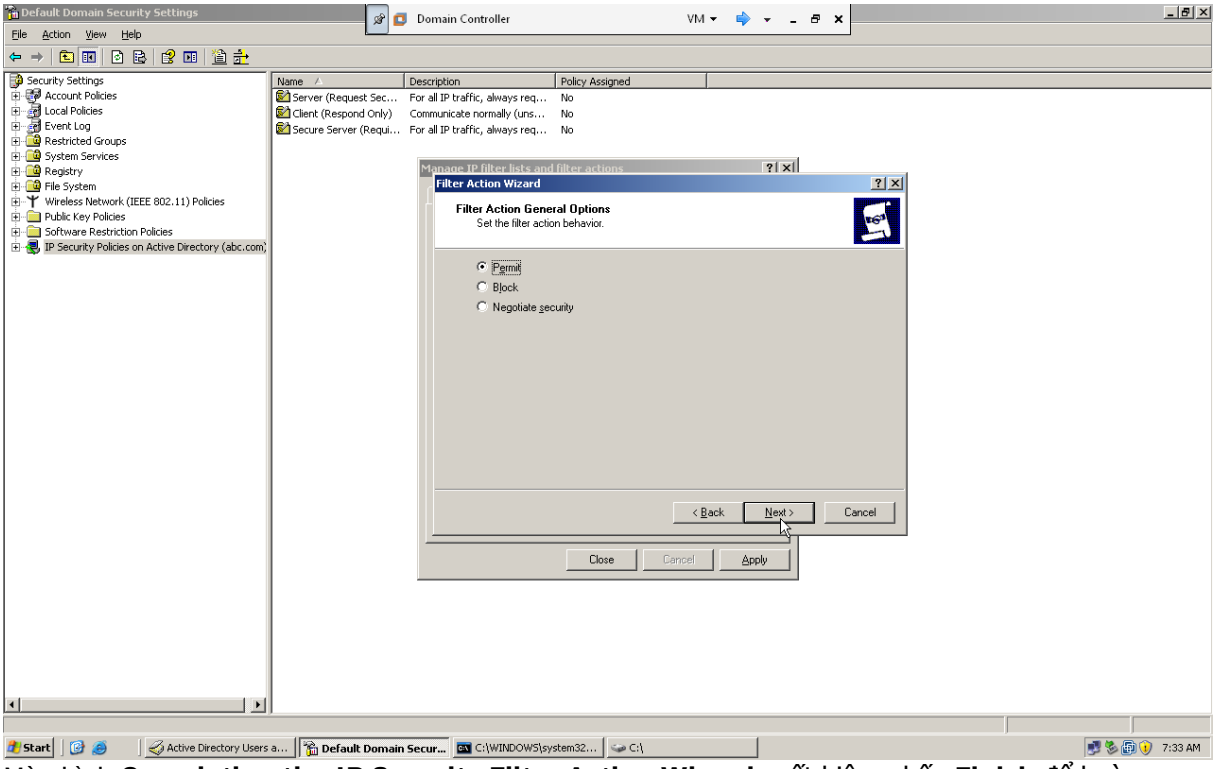
Màn hình **Welcome to the IP Security Filter Action Wizard** xuất hiện, nhấn **Next**:



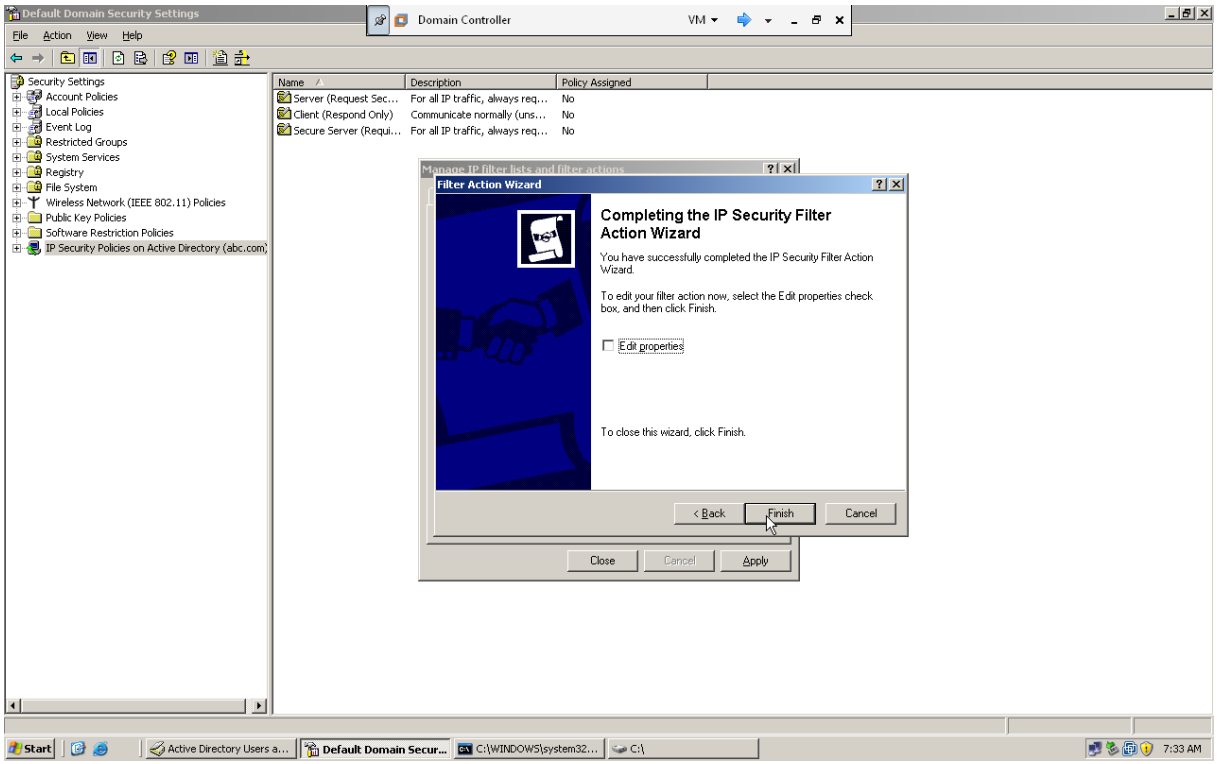
Màn hình **Filter Action Name** xuất hiện, đặt tên cho Filter Action đầu tiên là **"Cho phep"** và nhấn **Next**:



Màn hình **Filter Action General Options** xuất hiện, chọn hành động tương ứng là **Permit**, nhấn **Next**:

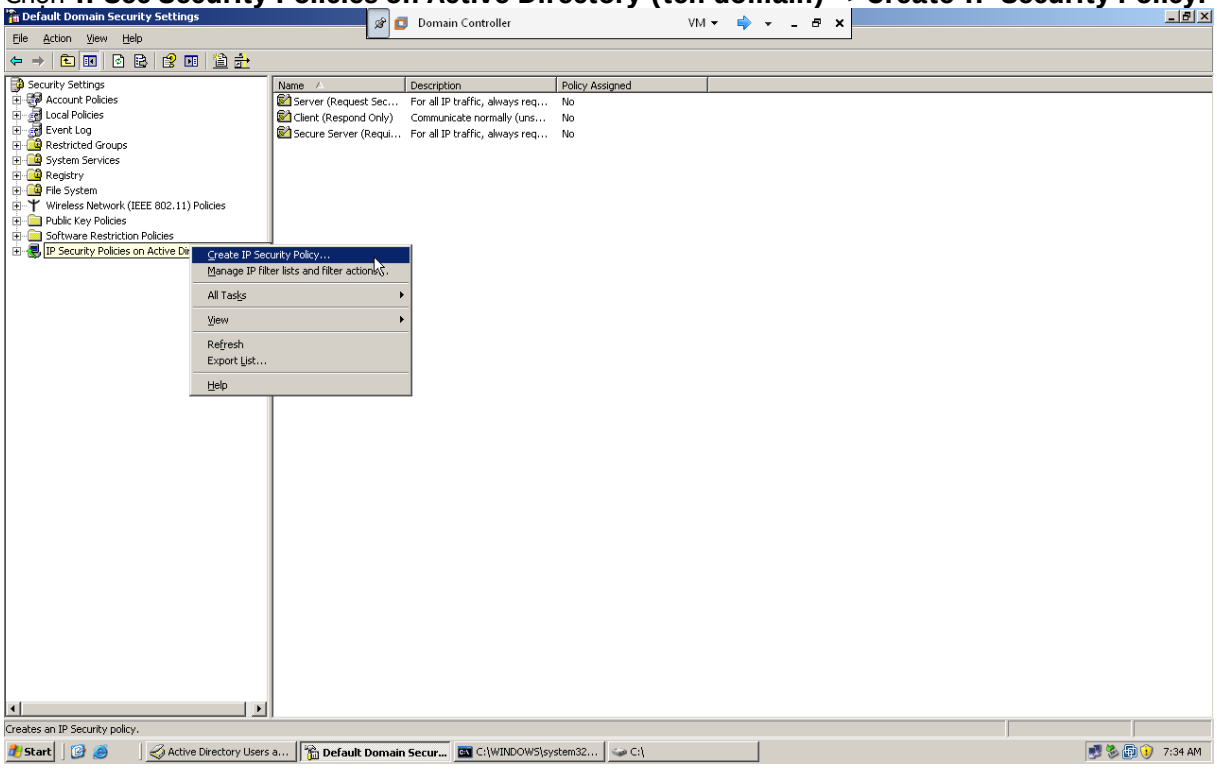


Màn hình **Completing the IP Security Filter Action Wizard** xuất hiện, nhấn **Finish** để hoàn thành việc tạo **Filter Action** đầu tiên:

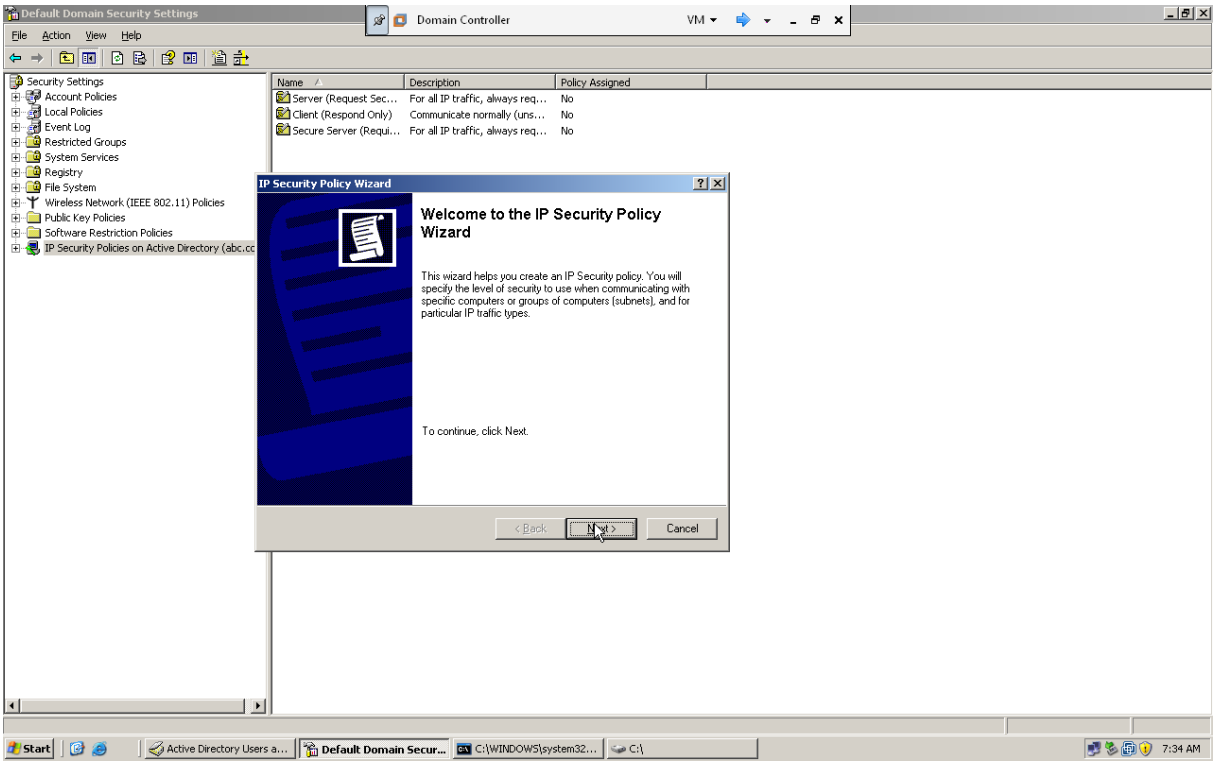


Tương tự chúng ta tạo **Filter Action** thứ 2 có tên là **"Khong cho phep"** tương ứng với hành động **Block**, sau đó nhấn Close để đóng cửa sổ Manage IP filter lists and filter actions.

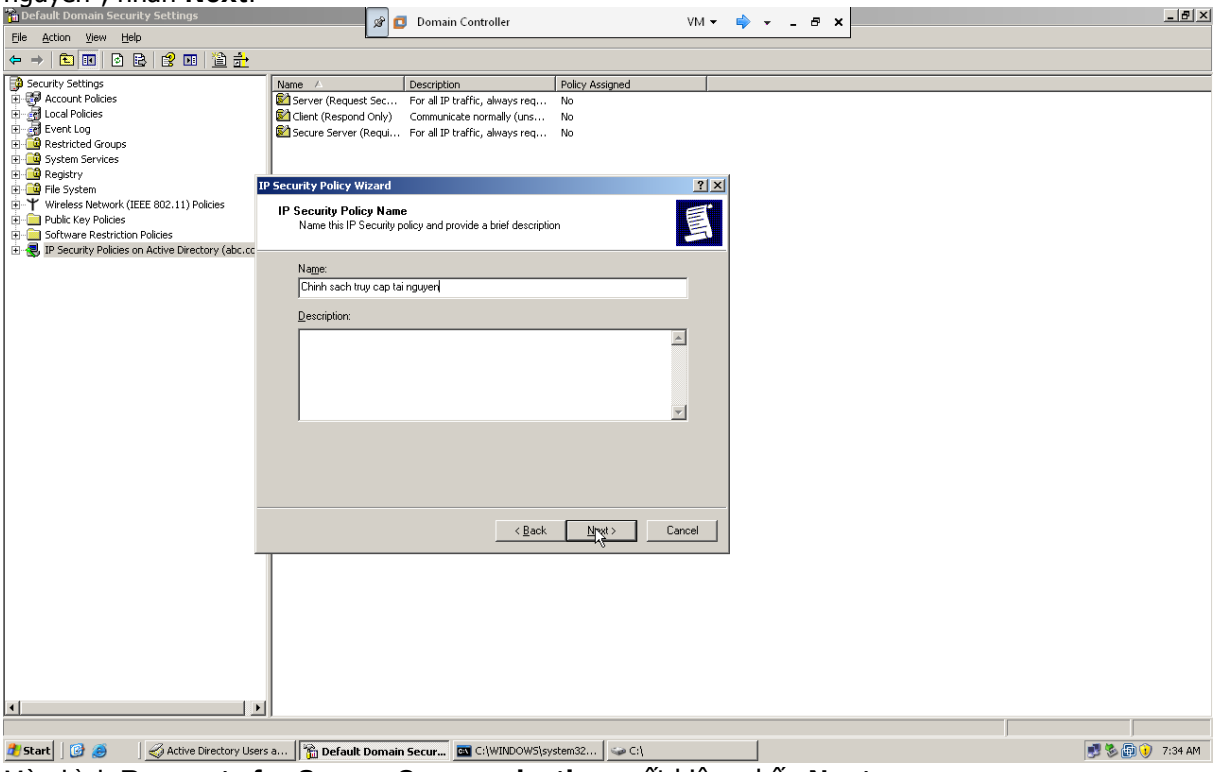
Chọn **IPSec Security Policies on Active Directory (tên domain) ->Create IP Security Policy.**



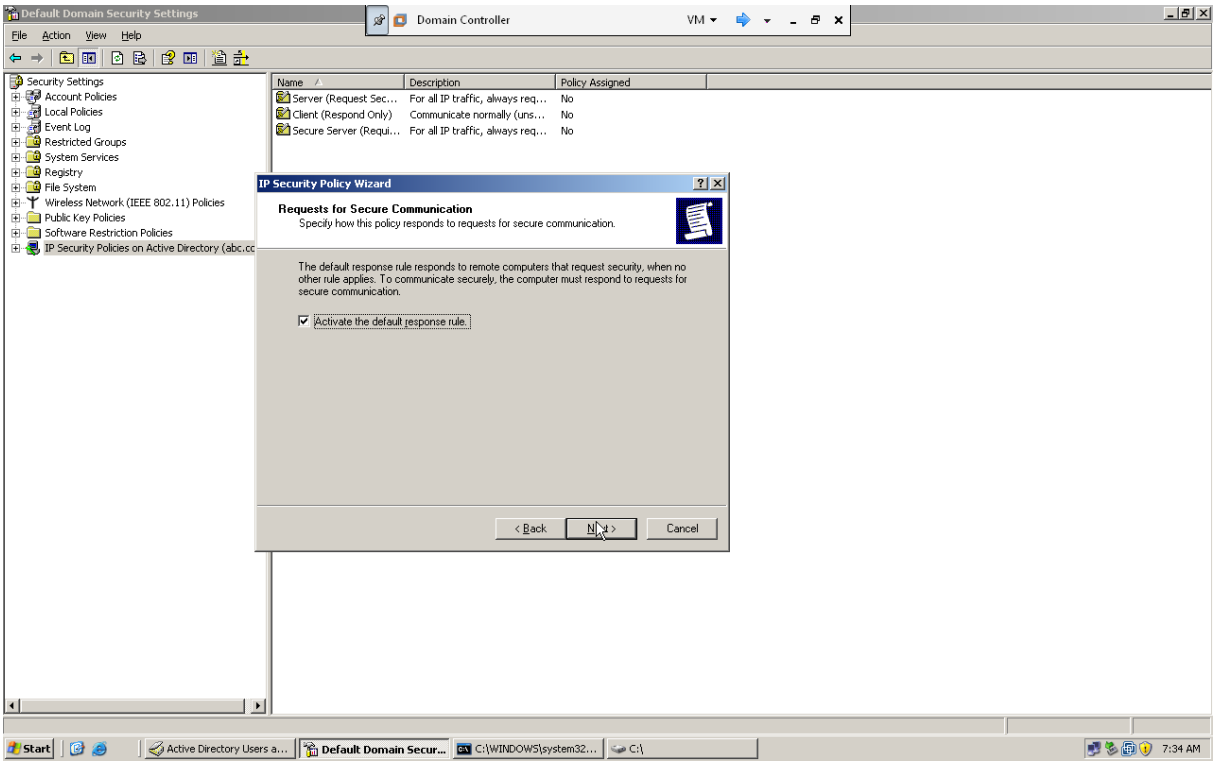
Màn hình **Welcome to the IP Security Policy Wizard** xuất hiện, nhấn **Next**:



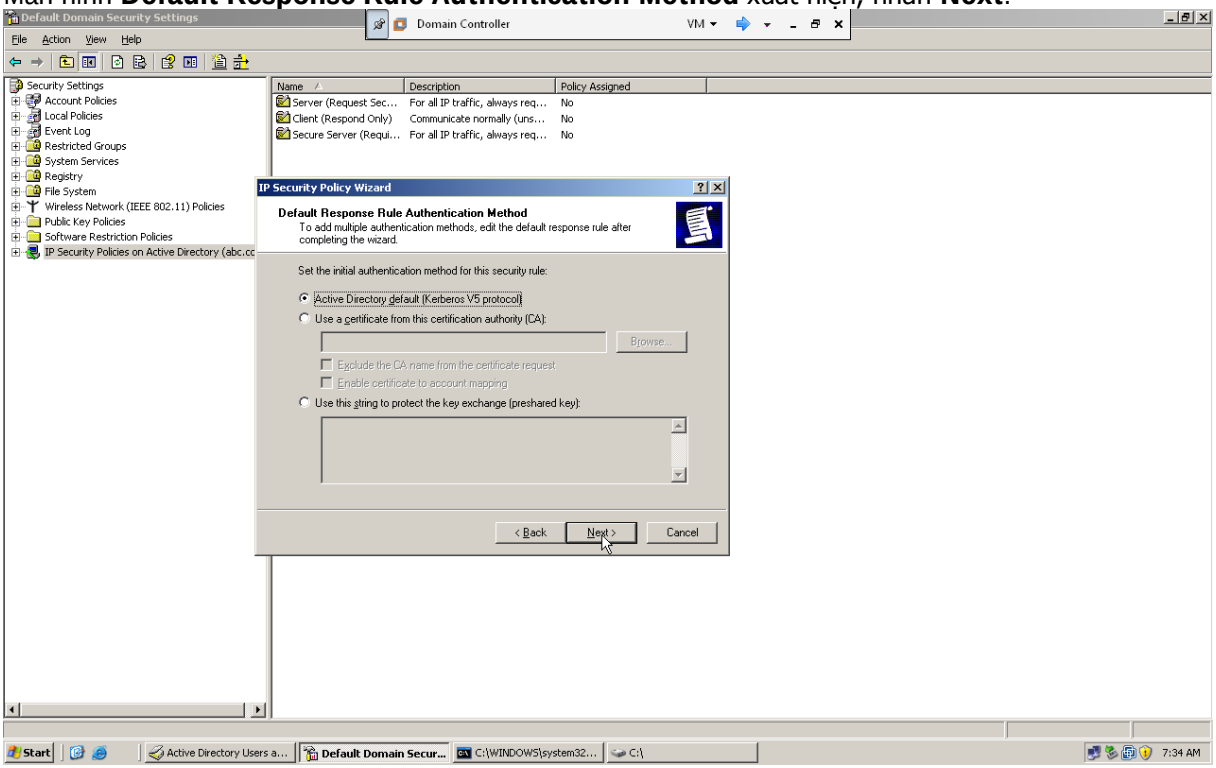
Màn hình **IP Security Policy Name** xuất hiện, đặt tên cho chính sách là "Chinh sach truy cap tai nguyen", nhấn **Next**.



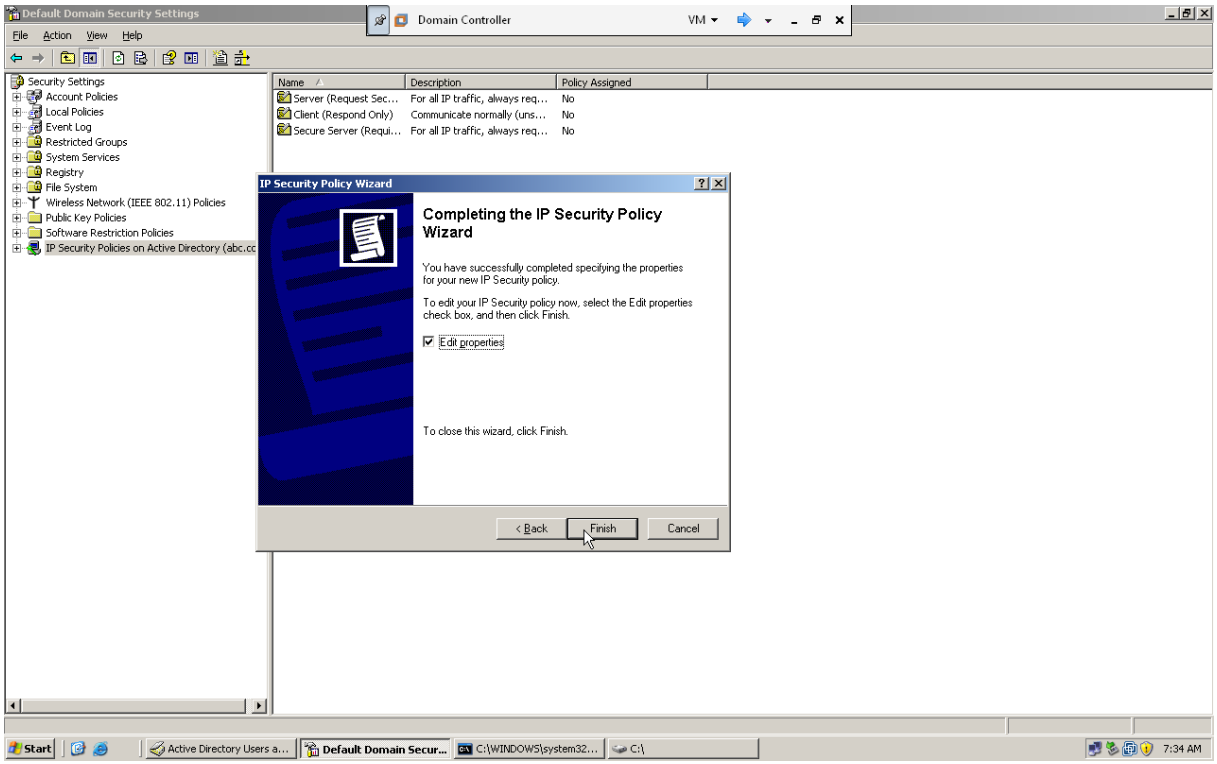
Màn hình **Requests for Secure Communication** xuất hiện, nhấn **Next**.



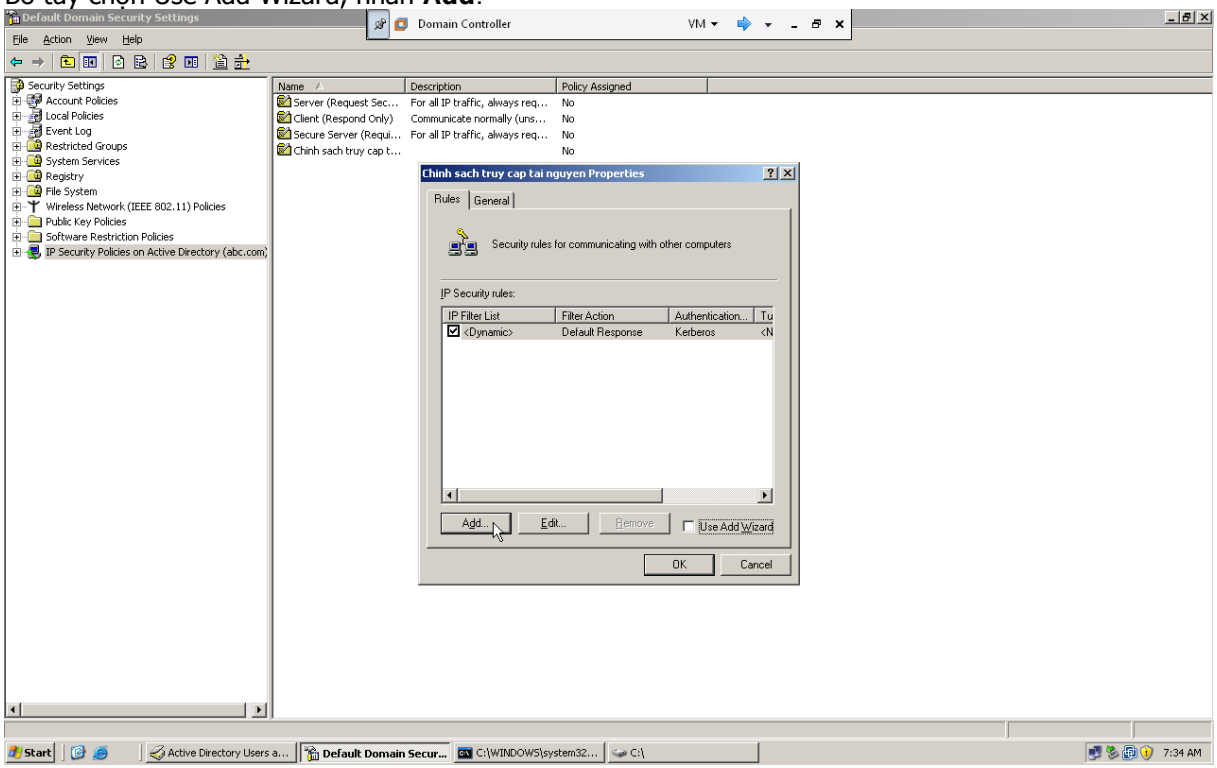
Màn hình **Default Response Rule Authentication Method** xuất hiện, nhấn **Next**.



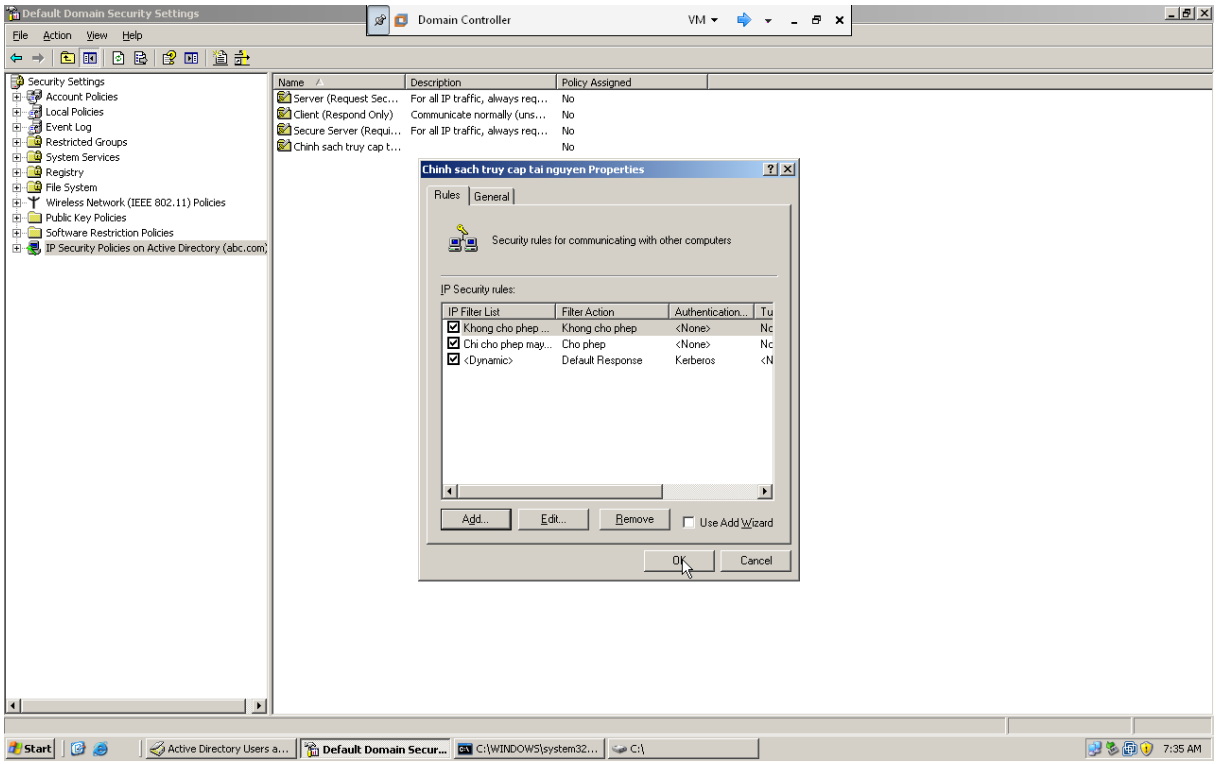
Màn hình **Completing the IP Security Policy Wizard** xuất hiện, chắc chắn rằng tùy chọn **Edit properties** đã được chọn và nhấn **Finish**.



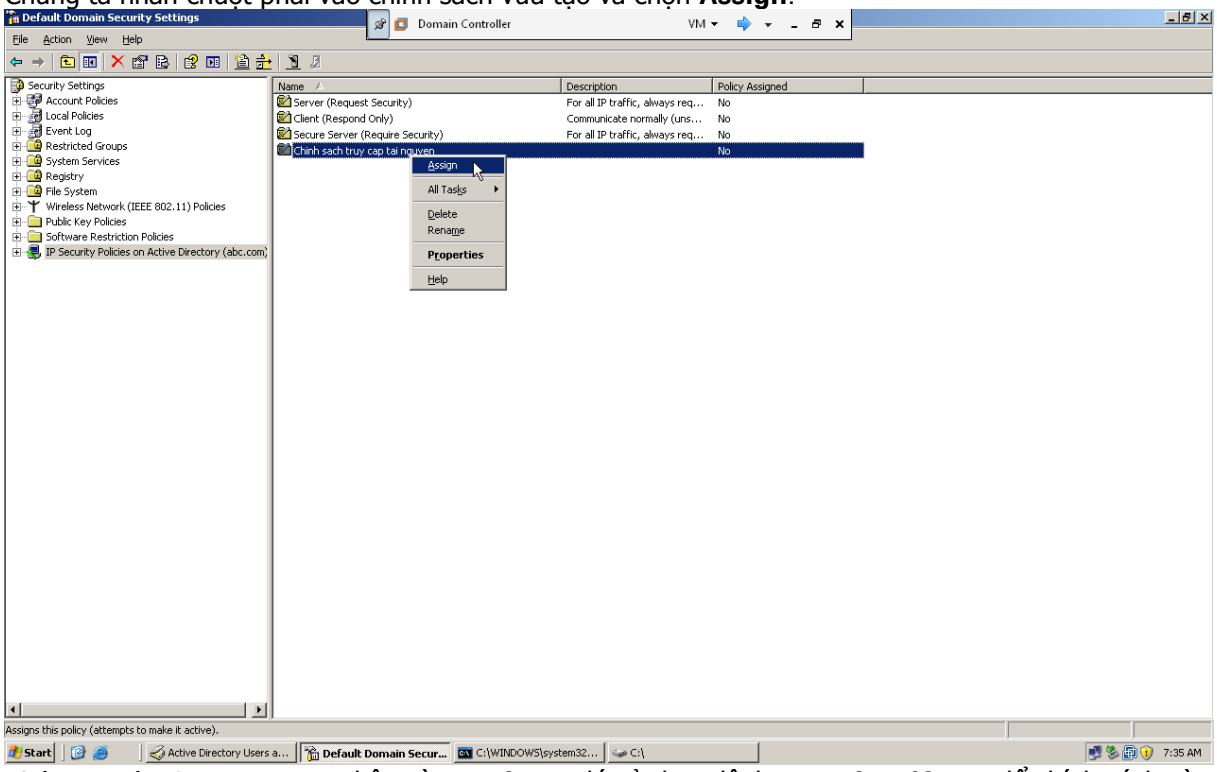
Bỏ tùy chọn Use Add Wizard, nhấn **Add**:



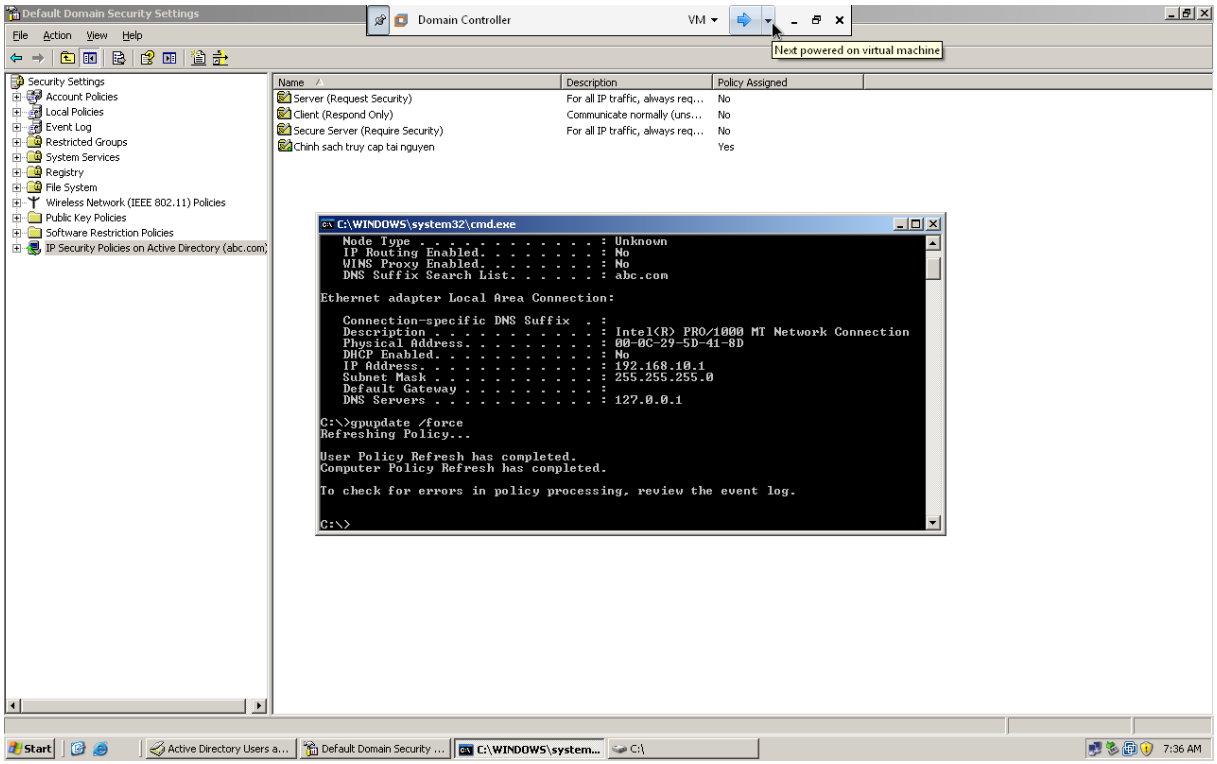
Chúng ta sẽ chọn **Filter List** và **Filter Action** tương ứng sau đó nhấn **Apply** và **OK**,sau đó nhấn **OK** để hoàn thành việc tạo chính sách truy cập tài nguyên.



Chúng ta nhấn chuột phải vào chính sách vừa tạo và chọn **Assign**:



Chúng ta vào **Start->Run**, nhập vào **cmd**, sau đó sử dụng lệnh **gpupdate/force** để chính sách vừa tạo được cập nhật.



Bài 6: VPN trên Windows Server 2003

Mục tiêu bài học

Trong bài học này, chúng ta sẽ:

- Định nghĩa VPN.
- Các thành phần triển khai hệ thống VPN.
- Bảo mật trong VPN.
- Sự phát triển và lợi ích của mạng riêng ảo VPN.
- Các giao thức cài đặt VPN.
- Phân tích nhu cầu thực tiễn để lựa chọn giải pháp VPN.

Khái niệm VPN

VPN có thể được định nghĩa như là một dịch vụ mạng ảo được triển khai trên cơ sở hạ tầng của hệ thống mạng công cộng với mục đích tiết kiệm chi phí cho các kết nối điểm-điểm.**VPN** cho phép các máy tính truyền thông với nhau thông qua một môi trường chia sẻ như mạng Internet nhưng vẫn đảm bảo được tính riêng tư và bảo mật dữ liệu.Để cung cấp kết nối giữa các máy tính, các gói thông tin được bao bọc bằng một header có chứa những thông tin định tuyến, cho phép dữ liệu có thể gửi từ một máy truyền qua môi trường mạng chia sẻ và đến được máy nhận, như truyền trên các đường ống riêng được gọi là tunnel.Để bảo đảm tính riêng tư và bảo mật trên môi trường chia sẻ này, các gói tin được mã hoá và chỉ có thể giải mã với những khóa thích hợp, ngăn ngừa trường hợp "trộm" gói tin trên đường truyền.

Giải pháp **VPN (Virtual Private Network)** được thiết kế cho những tổ chức có xu hướng tăng cường thông tin từ xa vì địa bàn hoạt động rộng (trên toàn quốc hay toàn cầu).Tài nguyên ở trung tâm có thể kết nối đến từ nhiều nguồn nên tiết kiệm được chi phí và thời gian.

- **Các loại VPN**

Có hai loại phổ biến hiện nay là **VPN truy cập từ xa (Remote-Access)** và ***VPN điểm-nối-điểm (site-to-site)*.**

VPN truy cập từ xa còn được gọi là mạng Dial-up riêng ảo (VPDN), là một kết nối người dùng-đến-LAN, thường là nhu cầu của một tổ chức có nhiều nhân viên cần liên hệ với mạng riêng của mình từ rất nhiều địa điểm ở xa.Ví dụ như công ty muốn thiết lập một VPN lớn phải cần đến một nhà cung cấp dịch vụ doanh nghiệp (ESP).ESP này tạo ra một **máy chủ truy cập mạng (NAS)** và cung cấp cho những người sử dụng từ xa một **phần mềm máy khách** cho máy tính của họ.Sau đó, người sử dụng có thể gọi một số miễn phí để liên hệ với NAS và dùng phần mềm VPN máy khách để truy cập vào mạng riêng của công ty.Loại VPN này cho phép các kết nối an toàn, có mật mã.

VPN điểm nối điểm (Site To Site): Áp dụng cho các tổ chức có nhiều văn phòng chi nhánh, giữa các văn phòng cần trao đổi dữ liệu với nhau.Ví dụ một công ty đa quốc gia có nhu cầu chia sẻ thông tin giữa các chi nhánh đặt tại Singapore và Việt Nam, có thể xây dựng một hệ thống VPN Site-to-Site kết nối hai site Việt Nam và Singapore tạo một đường truyền riêng trên mạng Internet phục vụ quá trình truyền thông an toàn, hiệu quả.Loại này có thể dựa trên **Intranet** hoặc **Extranet**.

- Loại dựa trên **Intranet**: Nếu một công ty có vài địa điểm từ xa muốn tham gia vào một mạng riêng duy nhất, họ có thể tạo ra một **VPN intranet (VPN nội bộ)** để nối LAN với LAN.
- Loại dựa trên **Extranet**: Khi một công ty có mối quan hệ mật thiết với một công ty khác (ví dụ như đối tác cung cấp, khách hàng...), họ có thể xây dựng một **VPN extranet (VPN mở rộng)** kết nối LAN với LAN để nhiều tổ chức khác nhau có thể làm việc trên một môi trường chung.

- **Các thành phần triển khai hệ thống VPN**

Để triển khai một hệ thống VPN chúng ta cần có những thành phần cơ bản sau đây:

- **User Authentication**: cung cấp cơ chế chứng thực người dùng, chỉ cho phép người dùng hợp lệ kết nối và truy cập hệ thống VPN.
- **Address Management**: cung cấp địa chỉ IP hợp lệ cho người dùng sau khi gia nhập hệ thống VPN để có thể truy cập tài nguyên trên mạng nội bộ.
- **Data Encryption**: cung cấp giải pháp mã hoá dữ liệu trong quá trình truyền nhằm bảo đảm tính riêng tư và toàn vẹn dữ liệu.
- **Key Management**: cung cấp giải pháp quản lý các khoá dùng cho quá trình mã hoá và giải mã dữ liệu.

- **Bảo mật trong VPN**

Tường lửa (firewall) là rào chắn vững chắc giữa mạng riêng và Internet.Bạn có thể thiết lập các tường lửa để hạn chế số lượng cổng mở, loại gói tin và giao thức được chuyển qua.Một số sản phẩm dùng cho VPN như router 1700 của Cisco có thể nâng cấp để gộp những tính năng của tường lửa bằng cách chạy hệ điều hành Internet Cisco IOS thích hợp.Tốt nhất là hãy cài tường lửa thật tốt trước khi thiết lập VPN.

Mật mã truy cập là khi một máy tính mã hóa dữ liệu và gửi nó tới một máy tính khác thì chỉ có máy đó mới giải mã được.Có hai loại là **mật mã riêng** và **mật mã chung**.

Mật mã riêng (Symmetric-Key Encryption): Mỗi máy tính đều có một mã bí mật để mã hóa gói tin trước khi gửi tới máy tính khác trong mạng.Mã riêng yêu cầu bạn phải biết mình đang liên hệ với những máy tính nào để có thể cài mã lên đó, để máy tính của người nhận có thể giải mã được.

Mật mã chung (Public-Key Encryption) kết hợp mã riêng và một mã công cộng.Mã riêng này chỉ có máy của bạn nhận biết, còn mã chung thì do máy của bạn cấp cho bất kỳ máy nào muốn liên hệ (một cách an toàn) với nó.Để giải mã một message, máy tính phải dùng mã chung được máy tính nguồn cung cấp, đồng thời cần đến mã riêng của nó nữa.Có một ứng dụng loại này được dùng rất phổ biến là Pretty Good Privacy (PGP), cho phép bạn mã hóa hầu như bất cứ thứ gì.

Giao thức bảo mật giao thức Internet (IPSec) cung cấp những tính năng an ninh cao cấp như các thuật toán mã hóa tốt hơn, quá trình thẩm định quyền đăng nhập toàn diện hơn.IPSec có hai cơ chế mã hóa là **Tunnel** và **Transport**.Tunnel mã hóa tiêu đề (header) và kích thước của mỗi gói tin còn Transport chỉ mã hóa kích thước.Chỉ những hệ thống nào hỗ trợ IPSec mới có thể tận dụng được giao thức này.Ngoài ra, tất cả các thiết bị phải sử dụng một mã khóa chung và các tường lửa trên mỗi hệ thống phải có các thiết lập bảo mật giống nhau.IPSec có thể mã hóa dữ liệu giữa nhiều thiết bị khác nhau như router với router, firewall với router, PC với router, PC với máy chủ.

Máy chủ AAA

AAA là viết tắt của ba chữ **Authentication** (thẩm định quyền truy cập), **Authorization** (cho phép) và **Accounting** (kiểm soát).Các server này được dùng để đảm bảo truy cập an toàn hơn.Khi yêu cầu thiết lập một kết nối được gửi tới từ máy khách, nó sẽ phải qua máy chủ AAA để kiểm tra. Các thông tin về những hoạt động của người sử dụng là hết sức cần thiết để theo dõi vì mục đích an toàn.

- **Sự phát triển và lợi ích của mạng riêng ảo VPN**

VPN có thể được phát triển trên nhiều môi trường khác nhau: X.25, Frame Relay, ATM, Internet.Tuy nhiên trên các môi trường khác nhau thì sự phát triển của VPN có các đặc điểm khác nhau về mặt kỹ thuật cũng như về mặt đáp ứng yêu cầu của khách hàng.

Sự phát triển của dịch vụ tạo mạng riêng ảo trên internet (IP VPN) là một xu thế tất yếu trong quá trình hội tụ giữa internet và các mạng dùng riêng.Có bốn lý do dẫn đến quá trình hội tụ này ở việt nam cũng như trên thế giới:

- Sự phát triển về mặt địa lý của thị trường dẫn đến sự gia tăng số lượng nhân viên hoạt động phân tán điều này gây khó khăn trong việc quản lý của các mạng dùng riêng.Nhu cầu liên lạc trong khi đi công tác hay xu hướng làm việc trong khi đi công tác hay xu hướng làm việc tại nhà, xu hướng hội nhập và mở rộng của các công ty diễn ra mạnh mẽ làm cho các hệ thống mạng dùng riêng không đáp ứng được nhanh chóng.VPN chính là một giải pháp trong trường hợp này.
- Nhu cầu sử dụng tác nghiệp trực tuyến.Sự phát triển của nền kinh tế dẫn đến xu hướng làm việc với nhiều nhà cung cấp dịch vụ, sản phẩm cũng như đối với nhiều đối tượng khách hàng khác nhau.Mỗi nhà cung cấp dịch vụ sản phẩm, khách hàng sử dụng cấu trúc mạng khác nhau (thủ tục, ứng dụng, nhà cung cấp dịch vụ, hệ thống quản trị mạng lưới...).Điều này là một thách thức lớn đối với một mạng dùng riêng trong việc kết nối với tất cả các mạng này.
- Chi phí cho việc cài đặt và duy trì một mạng diện rộng(WAN) là lớn.Điều này đặc biệt ảnh hưởng tới các doanh nghiệp có phạm vi hoạt động vượt ra khỏi biên giới quốc gia.
- Nhu cầu tích hợp và đơn giản hoá giao diện cho người sử dụng.

Một VPN được thiết kế tốt sẽ đem đến nhiều lợi ích cho công ty, như:

- Mở rộng kết nối ra nhiều khu vực và cả thế giới.
- Tăng cường an ninh mạng.
- Giảm chi phí so với việc thiết lập mạng WAN truyền thống.
- Giúp nhân viên làm việc từ xa, do đó giảm chi phí giao thông và tăng khả năng tương tác.
- Đơn giản hóa mô hình kiến trúc mạng.
- Cung cấp những cơ hội kết nối toàn cầu (điều này rất khó và đắt nếu kết nối trực tiếp bằng đường truyền riêng.)
- Hỗ trợ làm việc từ xa.
- Cung cấp khả năng tương thích với mạng lưới băng thông rộng.
- Giúp thu hồi vốn nhanh (return on investment) so với mạng WAN truyền thống.
- Quản lý dễ dàng: thường có khả năng quản lý số lượng người sử dụng (khả năng thêm, xoá kênh kết nối liên tục, nhanh chóng).Hiện nay nhu cầu sử dụng tư vấn từ bên ngoài, các nguồn lực từ bên ngoài để phục vụ cho công tác kinh doanh đã trở thành một xu hướng.
- Khả năng lựa chọn tốc độ tối đa từ tốc độ 9,6 Kbit/s tới T1/E1, hoặc sử dụng công nghệ DSL.
- Khả năng cung cấp dịch vụ một cách nhanh chóng: VPN được cung cấp trên mạng IP tích hợp được một số ưu điểm của mạng này đó là khả năng liên kết lớn, mạng lưới sẵn có vì vậy giảm thiểu thời gian cung cấp dịch vụ.

Đối với nhà cung cấp dịch vụ:

- Tăng doanh thu từ lưu lượng sử dụng cũng như xuất phát từ các dịch vụ gia tăng giá trị khác kèm theo.
- Tăng hiệu quả sử dụng mạng internet hiện tại.
- Gia tăng thêm khả năng tư vấn thiết kế mạng cho khách hàng đây là một yếu tố quan trọng tạo ra mối quan hệ gắn bó giữa nhà cung cấp dịch vụ với khách hàng đặc biệt là các khách hàng lớn.
- Đầu tư không lớn nhưng hiệu quả đem lại cao.
- Mở ra lĩnh vực kinh doanh mới đối với nhà cung cấp dịch vụ.Thiết bị sử dụng cho mạng VPN.

Một mạng riêng ảo hiệu quả bao gồm các đặc điểm sau:

- Bảo mật (Security).
- Tin cậy (reliablitity).
- Khả năng quản trị hệ thống mạng (network management).
- Khả năng quản trị chính sách (policy management).

- **Các giao thức cài đặt VPN**

✓ **IPSec**

IP Sercurity hay còn gọi là IPSec dựa trên nền tảng chuẩn cung cấp một khoá cho phép bảo mật giữa hai thiết bị mạng ngang hàng:
- Dữ liệu được tin cậy (Data confidentiality).
- Thông qua việc mã hoá dữ liệu nhằm bảo vệ dữ liệu khỏi sự tấn công của các hacker. Các thuật toán hỗ trợ mã hoá bao gồm: DES, 3DES, and AES.
- Tính xác thực và toàn vẹn của dữ liệu (Data authentication and Data integrity).
việc làm này thông qua chức năng HMAC nó kiểm tra các gói dữ liệu để không làm xáo trộn cho việc nhận dữ liệu.Các chức năng hỗ trợ HMAC bao gồm: MD5 and SHA-1.
- Phát hiện lỗi (Anti-replay detection).
- Là việc làm thông qua việc mã hoá số thứ tự các gói dữ liệu.
- Tính xác thực của mạng (Peer authentication) việc làm này đảm bảo chắc chắn dữ liệu trước khi được truyền trên mạng

- **Giao thức IPSec**

IPSec có 3 tầng giao thức chính:
- **Internet Key Exchange (IKE):** Giúp cho các thiết bị tham gia VPN trao đổi với nhau về thông tin an ninh như mã hóa thế nào? Mã hóa bằng thuật toán gì? Bao lâu mã hóa 1 lần? IKE có tác dụng tự động thỏa thuận các chính sách an ninh giữa các thiết bị tham gia VPN.Do đó IKE giúp cho IPSec có thể áp dụng cho các hệ thống mạng mô hình lớn.
Trong quá trình trao đổi key,IKE dùng thuật toán mã hóa đối xứng (symmetric encrytion) để bảo vệ việc trao đổi key giữa các thiết bị tham gia VPN.
- **Encapsulation Security Payload (ESP):** Có tác dụng xác thực (authentication) mã hóa (encrytion) và đảm bảo tính trọn vẹn dữ liệu (securing of data).Đây là giao thức được dùng phổ biến trong việc thiết lập IPSec .
- **Authentication Header (AH):** Có tác dụng xác thực, AH thì thường ít được sử dụng vì nó đã có trong giao thức ESP.

❖ **Internet Key Exchange (IKE)**

a. Cơ chế hoạt động của Internet Key Exchange (IKE)

Như đã nói ở trên giao thức IKE sẽ có chức năng trao đổi key giữa các thiết bị tham gia VPN và trao đổi chính sách an ninh giữa các thiết bị.Và nếu không có giao thức này thì người quản trị phải cấu hình thủ công.
Những chính sách an ninh trên những thiết bị này được gọi là **SA (Security Associate)**
Do đó các thiết bị trong quá trình IKE sẽ trao đổi với nhau tất cả những SA mà nó có và giữa các thiết bị này sẽ tự tìm ra cho mình những SA phù hợp với đối tác nhất.
Những key được trao đổi trong quá trình IKE cũng được mã hóa và những key này sẽ thay đổi theo thời gian (generate key) để tránh tình trạng bruteforce của Attacker.Và dưới đây là các giao thức xác thực cũng như mã hóa key trong quá trình IKE
Oakley(Tham khao thêm trên RFC 2412), ISAKMP (RFC 2408), Skeme.
Giao thức IKE sử dụng **UDP** port **500**.

b.Các giai đoạn hoạt động của IKE (IKE Phases)

- **IKE Phases 1** (Bắt buộc xảy ra trong quá trình IKE):
  - **Bước 1** : Xác thực giữa các thiết bị tham gia VPN (Authentication the peers).
  - **Bước 2** : Trao đổi các SA.

Và Phases 1 này có 2 chế độ hoạt động là **Main mode** (Cần **6 message** để hoàn thành các bước 1&2) và **Aggressive mode** (Cần **3 message** để hoàn thành các bước 1&2).
- **IKE Phases 1.5** (không bắt buộc).
Giao đoạn này có tác dụng cấp phát địa chỉ IP LAN, DNS thông qua DHCP và xác thực User (Authentication User).Giao thức được gọi trong quá trình này là Xauth (Extended Authentication).
- **IKE Phases 2** (bắt buộc phải xảy ra).
Sau khi trải qua **Phase 1 & 1.5** lúc này giữa các thiết bị đã có đầy đủ các thông tin về nhau như chính sách mã hóa, xác thực (SA) và key.
Và nhờ IKE thì giữa các thiết bị đã xây dựng được 1 kênh truyền ảo an ninh .
Đến đây giữa các thiết bị lại tiếp tục trao đổi cho nhau 1 SA khác.Cái SA được trao đổi lúc này là **chính sách của giao thức IPsec** (chính sách an ninh đóng gói dữ liệu) nó khác với SA của giao thức IKE (làm thế nào để xây dựng 1 kênh an toàn).Cái SA của IPsec này nó sẽ trao đổi với nhau việc mã hóa đóng gói dữ liệu theo ESP hay AH, nó hoạt động theo dạng **tunel mode** hay **transports mode**, thời gian mã hóa là bao lâu?

Đây là mã hóa dữ liệu chứ không còn là mã hóa trao đổi khóa (key) như diễn ra trong quá trình IKE. Đến lúc này nếu muốn trao đổi với ai thì nó sẽ trao đổi SA IPSec với người đó và dữ liệu được gửi trên đường truyền được mã hóa dựa vào SA IPsec này.

c. Các chức năng khác của IKE giúp cho IKE hoạt động tối ưu hơn bao gồm:

- **Dead peer detection (DPD)** and **Cisco IOS keepalives** là những chức năng bộ đếm thời gian.Nghĩa là sau khi 2 thiết bị đã tạo được VPN IPsec với nhau rồi thì nó sẽ thường xuyên gửi cho nhau gói keepalives để kiểm tra tình trạng của đối tác.Mục đích chính để phát hiện hỏng hóc của các thiết bị.Thông thường các gói keepalives sẽ gửi mỗi **10s**
- Hỗ trợ chức năng **NAT-Traversal**: Chức năng này có ý nghĩa là nếu trên đường truyền từ A tới B nếu có những thiết bị NAT or PAT đứng giữa thì lúc này IPSec nếu hoạt động ở chế độ **tunel mode** và **enable** chức năng **NAT- Trasersal** sẽ vẫn chuyển gói tin đi được bình thường.
- Chức năng **Mode Configuration** :

Chức năng này có tác dụng **pushing** các chính sách bảo mật cũng như thông tin về IP , DNS , Gateway cho người dùng di động khi họ quay VPN vào hệ thống .

Ngoài ra Cisco có cung cấp giải pháp cho việc này đó là Easy VPN.

- Chức năng cuối cùng IKE hỗ trợ là **Xauth**.**Xauth** sẽ cho phép phương thức **AAA (Authentication, Authorization, Accounting)** hoạt động đối với việc xác thực user.Ta cũng nên lưu ý phần này,Xauth không đè lên IKE mà việc xác thực của giao thức Xauth này là xác thực người dùng chứ không phải quá trình xác thực diễn ra trong Phares 1.

❖ **Encapsulation Security Payload (ESP)**

ESP sử dụng IP protocol number là **50** (ESP được đóng gói bởi giao thức IP và trường protocol trong IP là **50**).

Giao thức ESP sẽ làm công việc là mã hóa (encryption), xác thực(authentication), bảo đảm tính trọn vẹn của dữ liệu (Securing of data).Sau khi đóng gói xong bằng ESP mọi thông tin về mã hóa và giải mã sẽ nằm trong ESP Header. .

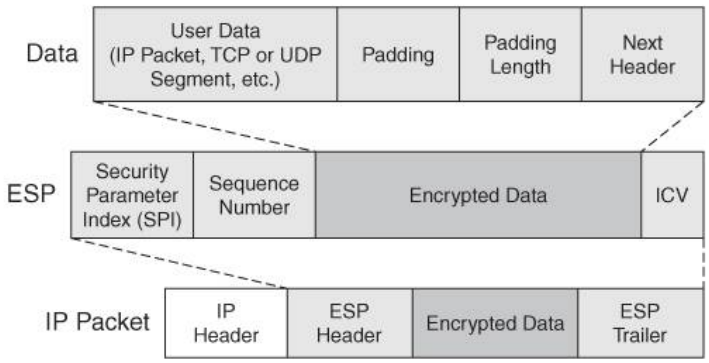
Các thuật toán mã hóa bao gồm **DES, 3DES, AES**.

Các thuật toán để xác thực bao gồm **MD5** hoặc **SHA-1**

ESP còn cung cấp tính năng anti-relay để bảo vệ các gói tin bị ghi đè lên nó.

Dưới đây là một mô hình của quá trình thực thi ESP trên user data để bảo vệ giữa 2 IPsec peers

Figure 3-7. ESP Packetization Process



❖ **Authentication Header (AH)**

Giao thức AH chỉ làm công việc xác thực (authentication) và bảo đảm tính trọn vẹn dữ liệu.Giao thức AH không có chức năng mã hóa dữ liệu.Do đó AH ít được dùng trong IPSec vì nó không đảm bảo tính an ninh .

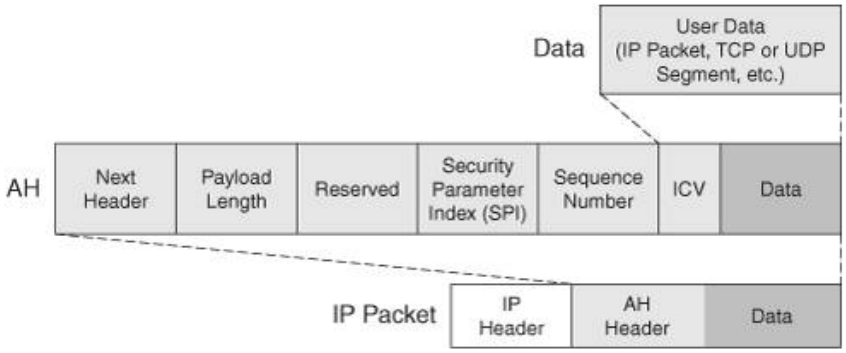
Bước thứ 1: Giao thức AH sẽ đem gói dữ liệu (packet) bao gồm payload + IP header + Key cho chạy qua 1 giải thuật gọi là giải thuật Hash và cho ra 1 chuỗi số.Các bạn nhớ đây là giải thuật 1 chiều, nghĩa là từ gói dữ liệu + key = chuỗi số.Nhưng từ chuỗi số không thể hash ra = dữ liệu + key.Và chuỗi số này sẽ được gán vào AH header.

Bước thứ 2: AH Header này sẽ được chèn vào giữa Payload và IP Header và chuyển sang phía bên kia.Đương nhiên ta cũng nhớ cho rằng việc truyền tải gói dữ liệu này đang chạy trên 1 tunel mà trước đó quá trình IKE sau khi trao đổi khóa đã tạo ra .

Bước thứ 3: Router đích sau khi nhận được gói tin này bao gồm IP header + AH header + Payload sẽ được chạy qua giải thuật Hash 1 lần nữa để cho ra 1 chuỗi số .

Bước thứ 4: So sánh chuỗi số nó vừa tạo ra và chuỗi số của nó nếu giống nhau thì nó sẽ chấp nhận gói tin. Nếu trong quá trình truyền gói dữ liệu 1 attacker sniff nói tin và chỉnh sửa nó dẫn đến việc gói tin bị thay đổi về kích cỡ, nội dung thì khi đi qua quá trình hash sẽ cho ra 1 chuỗi số khác chuỗi số ban đầu mà router đích đang có.Do đó gói tin sẽ bị drop.
Thuật toán hash bao gồm **MD5** và **SHA-1**.Và trong trường hợp này IPSec đang chạy ở chế độ **transports mode** .
Dưới đây là một ví dụ về AH:

Figure 3-6. AH Packetization Process



Bảng so sánh giữa 2 giao thức ESP và AH:

Security Feature	AH	ESP
Layer-3 IP protocol number	51	50
Provides for data intergrity	Yes	Yes
Provides for data authentication	Yes	Yes
Provides for data encryption	No	Yes
Protects against data replay attacks	Yes	Yes
Works with NAT	No	Yes
Works with PAT	No	No
Protects the IP packet	Yes	No
Protects only the data	No	Yes

- ✓ **PPTP**

Point – To – Point Tunneling Protocol(PPTP) được phát triển bởi Microsoft nó cung cấp một giải pháp bảo mật cho remote access.Tất cả những dữ liệu cần thiết sẽ được vận chuyển từ client qua mạng công cộng tới một server (VPN gateway).
Một vài đặc điểm chính của PPTP:

- **Compression (nén)**: nén dữ liệu được thực thi thông qua giao thức Microsoft's Point-to-Point Compression (MPPC) với PPP payload.Nó hỗ trợ bởi cả PPTP và L2TP.
- **Encryption(mã hoá)**: dữ liệu được mã hoá dựa trên giao thức Microsoft's Point-to-Point Encryption (MPPE).Mã hoá dữ liệu sử dụng thuật toán RSA's RC4 .
- **User authentication**: User authentication sẽ được hoàn thành bởi phương thức xác thực:PPP ví dụ: PAP or CHAP.
- **Data delivery**: sử dụng giao thức PPP, nó được đóng gói ở trong một gói tin PPTP/ L2TP.
- **Client addressing**: PPTP and L2TP hỗ trợ cơ chế gán địa chỉ tự động sử dụng Network Control Protocol (NCP) của PPP.

- **Thành phần của PPTP.**

Ở đây ta sẽ nói đến PPTP dựa trên một kiến trúc client-server với kết nối remote access bao gồm 2 phần:
* Client được quy định như là một **PPTP Access Concentrator** (PAC).Giới hạn của nó chính là sự sai lệch,vấn đề bởi vì các thiết bị của CISCO hay sử dụng thường đã giới hạn phiên truyền remote access.Tuy nhiên với PPTP thì chức năng này đã được phân chia ra một PC, và một server.
* Server là một **PPTP Network Server** (PNS).Server sẽ chịu trách nhiệm xác đinh đường hầm từ PAC nó sẽ có nhiệm vụ bảo vệ gói dữ liệu PPP trong đường hầm, kiểm tra nhằm bảo vệ, giải mã các gói tin và đóng gói các gói tin PPP và gói tin IP để tới đích.

- **Cách thức hoạt động của PPTP**

PPTP là giao thức hướng kết nối mà PAC và PNS duy trì một trạng thái kết nối.Phiên truyền được tạo ra khi PAC khởi tạo một kết noi PPP tới PNS.Hai kết nối này sẽ xây dựng nên một phiên truyền: một điều khiển kết nối (control connection) và một dữ liệu kết nối (data connection).Một phiên truyền được thiết lập PAC và PNS có thể sử dụng GRE thông qua dữ liệu kết nối để truyền tín hiệu tới người dùng. Nói một cách tổng quát kết nối dữ liệu được gọi là: một đường hầm (Tunnel).

Control Connection

Điều khiển kết nối sẽ chịu trách nhiệm thiết lập, duy trì và đẩy nhanh dữ liệu đường hầm (data tunnel) nó sử dụng giao thức TCP nhằm vận chuyển,mang các thông tin tới đích với cổng là :1.723 .Kết nối này có thể được thiết lập từ PAC hoặc PNS.

Có 2 PPTP messages có thể được sử dụng cho control connection:

- Control
- Management (this is currently not defined in the RFC)

a.1.Setting Up the Control Connection

Cài đặt một Control Connection bao gồm sự trao đổi giữa 2 đầu của gói tin:

Start-Control-Connection-Request.

Start-Control-Connection-Reply.

Ban đầu sẽ gửi một bản tin đầu tiên khi mà phản hồi lại cho người dùng với khoảng thời gian là 1s.Bảng dưới đây sẽ mô tả kết quả có thể bao gồm một gói tin phản hồi.Hơn nữa việc khởi tạo kết nối, những message cho phép PAC có khả năng chia sẻ thông tin với PNS.Mỗi PNS/PAC yêu cầu một control connection riêng biệt.

Code	Description
1	Control connection successfully established.
2	General error.
3	Control connection already exists.
4	The requestor is not authorized to establish a control connection to the receiver.
5	The requestor's protocol version is not supported.

Vì cả PNS and PAC đều có thể khởi tạo một control connection.Do đó một miền xung đột có khả năng xảy ra nếu cả 2 cùng cố gắng tạo một control connection trong cùng một thời điểm.Chỉ một control connection được tồn tại giữa PNS and PAC .

Một miền xung đột xảy đến khi tại cùng một thời điểm cả PNS and PAC đều gửi một Start-Control-Connection-Request messages.Trong tình trạng đó việc khởi tạo với một IP address cao (32 bit) được sử dụng và một control connection ngay lập tức được kết thúc.

a.2 duy trì một Control Connection(Maintaining the Control Connection)

Keepalives được sử dụng trên **Control Connection** để đảm bảo chắc chắn được kết nối giữa PAC and PNS, bất cứ thiết bị nào trong số chúng không hoạt động có thể phát hiện ra nhanh nhất.Có 2 loại keepalive messages cho Control Connection :

- **Echo-Request**
- **Echo-Reply**

Cả PAC and PNS đều có thể khởi tạo một keepalives.**Keepalive messages** được sinh ra nếu không có control message được nhận trong khoảng thời gian là **60s**.Nếu một PAC/PNS không nhận một **Echo-Reply** phản hồi từ yêu cầu, control connection sẽ bị kết thúc.

a.3 Terminating the Control Connection

Control connection cũng chịu trách nhiệm xác định bất kỳ một data connections và quá trình control connection, việc xác định control connection sử dụng bởi 2 thành phần sau:

- **Stop-Control-Connection-Request.**
- **Stop-Control-Connection-Reply.**

Hình dưới đây là một vài lý do mà tại sao control connection có thể bị chấm dứt:

Code	Description
1	General teardown request.
2	The peer's version of the protocol can't be supported.
3	The sender of the request message is being shut down.

❖ **Tunnel Connection**

Tunnel chứa tất cả những PPP Packet.GRE được sử dụng như là một giao thức vận chuyển cho PPP packets.Một control connection xác định tốc độ thực tế và thông số của vùng đệm nhằm sử dụng để đảm bảo chắc chắn PAC/PNS không tạo ra những vấn đề điều khiển luồng.Những thông số khác cần được xem xét là việc gán địa chỉ PAC.Các thuật toán mã hoá và nén cũng sẽ được sử dụng nếu có.Vấn đề tiếp theo được xem xét là dữ liệu người dùng sẽ được đóng gói và vận chuyển qua đường ống như thế nào.

b.1 Thiết lập Kết nối Đường hầm (Setting Up the Tunnel Connection)

Khi một trạng thái bắt đầu-điều khiển kết nối-yêu cầu **(Start-Control-Connection-Request)** và bắt đầu-điều khiển kết nối-trả lời yêu cầu **(Start-Connection-Reply)** của các gói tin đã được trao đổi thông qua điều khiển kết nối (control connection) thì việc kế tiếp là cài đặt một kết nối đường hầm (dữ liệu).Nó sẽ bao gồm các quá trình sau:

- **Outgoing-Call-Request**
- **Outgoing-Call-Reply**
- **Incoming-Call-Request**
- **Incoming-Call-Reply**
- **Incoming-Call-Connected**

PPP được sử dụng ở đây là một giải pháp cho dialup.Vì vậy hầu hết các PPP được thực thi và danh mục được tìm thấy ở đây khi PPP và PPTP được phân chia.

Outgoing được gọi là những gói tin được sinh ra khi có một trạng thái kết nối từ PNS tới PAC, PAC được nói đến nhằm để thiết lập một đường hầm tới PNS.Kết nối này cũng cung cấp thông tin nhằm điều chỉnh dữ liệu được truyền thông qua đường hầm từ PAC Tới PNS, như là những thông tin trong một cửa sổ windows.

Outgoing reply sẽ gửi một loạt các kết quả trả lời từ PAC tới PNS(như hình dưới):

Code	Brief Description	Detailed Description
1	Connected	The tunel is established with no errors.
2	General error	The tunel could not be established based on the error value in the error code field.
3	No carrier	The tunel could not be established because no carrier was detected
4	Busy	A busy signal was detected, causing the tunel to fail.
5	No dial tone	The outgoing call failed because no dial tone was detected.
6	Time-out	The PAC didn't establish the tunnel within the required amount of time.
7	Do not accept	The outgoing call was administratively denied.

Trong hầu hết các trường hợp chỉ có code 1, 2, 6, và 7 được sử dụng bởi vì chức năng.

PAC được triển khai thực tế trong một Client thay vì một thiết bị trung gian..

Gói tin **Incoming-Call-Request** được gửi từ PAC tới PNS để chỉ ra rằng một yêu cầu ngược trở lại sẽ được thiết lập từ PAC tới PNS.Gói tin này cho phép PNS thu nhận những thông tin về lời gọi trước đó được trả lời hoặc chấp nhận.

Tin **Incoming-Call-Reply** được gửi từ PNS tới PAC để trả lời chấp nhận hay từ chối một yêu cầu kết nối.Những gói tin này cũng có thể chứa những thông tin điều khiển luồng PAC phải sử dụng trong tunnel để truyền tới PNS.

Hình dưới đây cho ta những kết quả có thể xảy ra từ PNS:

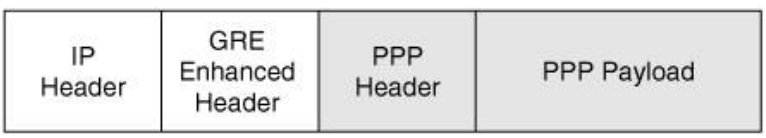
Code	Description
1	The PAC should answer the incoming call.
2	The incoming call can't be established based on the error value in the error code field.
3	The PAC should not accept the incoming call.

Gói **Incoming-Call-Connected** được gửi từ PAC tới PNS để đáp lại (response) những thông tin trả lời (reply).Do đó lời gọi incoming sẽ sử dụng cơ chế bắt tay 3 bước: request, reply, and connected.

b.2 Đóng gói dữ liệu truyền (Encapsulating the Payload)

GRE được sử dụng để chứa các gói PPP được truyền giữa PAC và PNS.Dưới đây là một ví dụ về gói PPTP, ta có thể nhìn thấy gói PPP được đóng gói trong GRE, những gói này sẽ được đóng gói trong một gói tin IP.Gói PPP chứa dữ liệu người dùng thực tế là gói chứa các giao thức như IP, IPX, hoặc một vài loại khác.

Figure 4-1. PPTP Tunnel Packet



GRE header được sử dụng để đóng gói gói PPP không phải là một standard GRE header, nhưng nó lại được một phần nhỏ cho PPTP.Sự khác nhau chính giữa standard GRE header và PPTP GRE header là PPTP GRE header có thêm một trường mới là acknowledgment được sử dụng để xác định xem có hay

không một gói GRE được nhận ở đầu cuối của tunnel.GRE acknowledgment này là quá trình không có bất cứ thứ gì làm việc với gói dữ liệu người dùng, thay vào đó, nó được dùng để xác định tốc độ của gói truyền qua tunnel. Nói cách khác, PPTP sử dụng một giao thức cửa sổ trượt để khống chế lưu lượng của những gói đưa vào tunnel bằng việc sử dụng trường sequence và acknowledgment .
Kích thước cửa sổ có thể được thay đổi động trong suốt quá trình tồn tại của tunnel.Mục đích của PPTP không phải là những gói tin truyền lại do bị mất hay đi ra ngoài cấu trúc cửa sổ hiện tại: điều này là trách nhiệm của thiết bị nguồn.

b.3 Cắt bỏ một kết nối tunnel (Tearing Down a Tunnel Connection)

Khi một kết nối tunnel không còn cần thiết, nó sẽ được gỡ bỏ bởi thiết bị PPTP.Hai thông báo được trao đổi để xử lí quá trình gỡ bỏ này là:

- **Call-Clear-Request.**
- **Call-Disconnect-Notify.**
- **Cả PAC và PNS đều có thể khởi tạo một huỷ bỏ kết nối tunnel.**

Thông báo **Call-Clear-Request** được gửi từ người yêu cầu nhằm báo hiệu kết nối tunnel đang được huỷ bỏ (torn down).
Một Call-Disconnect-Notify phản hồi lại cho người nhận biết tình trạng của tunnel được yêu cầu.

b.4 Ví dụ về kết nối (PPTP Example PPTP Connection)

Dưới đây là những giải thích về một xử lí cơ bản và thông báo đã thiết lập một kết nối PPTP.
Đây là một tổng quan ngắn gọn về việc cài đặt một phiên PPTP tiêu biểu:

1. The PAC connects to the PNS using TCP on port 1723.
2. The PAC sends a Start-Control-Connection-Request message.
3. The PNS responds with a Start-Control-Connection-Reply message.
4. The PAC sends an Outgoing-Call-Request message, including a caller ID to identify the PAC for the tunnel, to request a tunnel connection from the PNS.
5. The PNS responds with an Outgoing-Call-Reply message to the PAC and selects its own caller ID for the tunnel.
6. The PAC sends a Set-Link-Info message, specifying the PPP options it wants to use for the tunnel.
7. Once the tunnel is up, other Set-Link-Info messages can be shared to change parameters such as window size.

Nếu không có những thông báo nào nhận được trên kết nối điều khiển **(control connection)** trong 60 giây, thì PNS sẽ gửi những **Echo-Request** tơi PAC và giả sử PAC có thể đi tới được, PAC sẽ trả lời với một thông báo **Echo-Reply**.Những thông báo này được dùng để bảo đảm rằng điểm đích của tunnel vẫn còn hoạt động và có thể truyền tới đích.
Dần dần kết nối tunnel sẽ được huỷ bỏ.Một số lý do chung để tunnel bị huỷ bỏ bao gồm:

- Những vấn đề về khả năng vượt ngoài phạm vi được tìm thấy (Reachability problems have been found).
- Có lỗi xảy ra(An error condition exists).
- PAC và PNS đã bi ngắt (The PAC or PNS is shutting down).
- Tunnel không còn cần thiết (The tunnel is no longer needed).

Dưới đây là một ví dụ của một PAC đang hoàn thành một phiên truyền PPTP tới một PNS:

1. PAC đầu tiên gửi một thông báo Set-Link-Info để Thông tin với những tham số cấu hình của tunnel và sau đó gửi một yêu cầu kết thúc LCP Tới PNS, nhằm chỉ ra một phiên PPP cần phải được đóng.

2. Vệc phản hồi lại, PNS đầu tiên gửi một gói tin Set-Link-Info Thông tin với những tham số cấu hình của tunnel và sau đó gửi một LCP acknowledgement tới LCP termination request.

3. PAC gửi một Clear-Call-Request message tới một PAC Liên hệ với nó.

4. Những PNS phản hồi lại với một Call-Disconnected-Notify message tới PAC Tại điểm này tunnel được hoàn thành.

5. PAC gửi một Stop-Control-Connection-Request message tới PNS.

6. PNS trả lời với một Stop-Control-Connection-Reply message. Tại điểm này, kết nối điều khiển TCP đã được kết thúc và phiên truyền PPTP không còn tồn tại giữa PAC và PNS.

- **Những vấn đề với việc sử dụng PPTP (Issues with the Use of PPTP)**

Trong bất kỳ một sự thực thi VPN nào, bạn sẽ phải giải quyết những vấn đề nhất định về PPTP để thực hiện tối ưu và với cực tiểu những vấn đề,đây là một số vấn đề chung bạn sẽ cần để giải quyết:

- **Vấn đề phân mảnh (Fragmentation problems).**
- **Ván đề liên quan tới bảo mật (Security concerns).**
- **Vấn đề về chuyển đổi địa chỉ (Address translation issues).**

✓ **L2TP**

L2TP giống như PPTP đóng gói dữ liệu trong những frame PPP và truyền những frame này thông qua một IP backbone.Không giống như PPTP, L2TP sử dụng UDP như một phương thức đóng gói cả sự bảo trì tunnel lẫn dữ liệu người dùng.Trong khi PPTP sử dụng MPPE để mã hóa (thông qua PPP), thì L2TP lại dựa vào một giải pháp an toàn hơn:Những gói L2TP được bảo vệ bởi IPsec ESP đang sử dụng ở tầng transport trong mô hình OSI.Mặc dù ta có thể sử dụng L2TP Không có IPsec, vấn đề chính với cách tiếp cận này là với việc làm đó L2TP không thực hiện sự mã hóa và bởi vậy sự tin cậy không được đảm bảo.Bởi vậy, đa số L2TP sự thi hành sẽ bao gồm sự sử dụng của IPsec.

L2TP Là một giải pháp truy nhập từ xa.Nó gồm có hai thiết bị: một client và một server sự bảo trì tunnel và dữ liệu Đường hầm(tunnel) được dùng giữa hai thiết bị này sử dụng cấu trúc gói, đơn giản hoá chính là sự thực thi của L2TP.

Cho đến khi IPsec được giới thiệu XAUTH nhằm sự chứng thực người sử dụng, những phương pháp trên nền tiêu chuẩn duy nhất về sự chứng thực người dùng sử dụng PPTP và sau đó L2TP.Và ngay cả bây giờ, XAUTH còn ở một IETF- RFC, vì vậy sự thi hành của một nhà cung cấp có lẽ đã không thích hợp .

❖ **Hoạt động của L2TP**

Thiết lập một L2TP tunnel gồm có hai bước để sử dụng tunnel PPP cho một phiên truyền:

1. Thiết lập một kết nối điều khiển cho đường hầm (tunnel).
   (Establish a control connection for the tunnel).
2. Thiết lập một phiên truyền để truyền dữ liệu người sử dụng thông qua tunnel
   (Establish a session to transmit user data across the tunnel).

Những thành phần mà được dùng để hoàn thành hai bước trên là:

a.Tổng quan về IPSec (IPsec Review)

IPsec là một giao thức Lớp 3 nhằm bảo vệ gói tin IP ở Lớp-3 và các lớp trên trong mô hình OSI.Không kể việc định nghĩa những quá trình bảo vệ dữ liệu như sự toàn vẹn dữ liệu và sự chứng thực với những chức năng HMAC, và tính bảo mật dữ liệu với những giải thuật mã hóa, IPsec cũng định nghĩa khuôn dạng của những gói tin và làm sao để những gói tin được truyền qua đường hầm một cách an toàn và tối ưu nhất.Kiểu đường hầm **(Tunnel mode)** được sử dụng cho những kết nối site-to-site và remote access connections, trong khi mà kiểu vận chuyển **(transport mode)** được sử dụng cho những kết nối đặc biệt point-to-point.Trong tunnel mode IPsec bảo vệ toàn bộ gói nguyên bản.

Với việc được chấp nhận và sử dụng rộng rãi, IPSec có một số hạn chế sau:

- Chỉ IPsec làm việc với TCP/ IP những giao thức khác sẽ không làm việc trừ phi Tunnel đang sử dụng GRE.
- Những tham số được thống nhất giữa những hai mạng, một sự không thích ứng trong những tham số cũng là nguyên nhân gây ra kết nối bị hỏng.
- Bởi vì IPsec vận hành tại lớp mạng, nên tất cả các giao thức của lớp trên và những ứng dụng có để chấp nhận những chính sách ứng dụng vào kết nối IPsec giữa hai thiết bị; không có quá trình chuyên biệt với những lớp dưới khác .

b. Các kiểu Tunnel (Tunnel Types).

Với L2TP, Có hai kiểu tunnel:

Voluntary (tự nguyện): PC (của) người sử dụng và server tình nguyện là endpoints của tunnel.

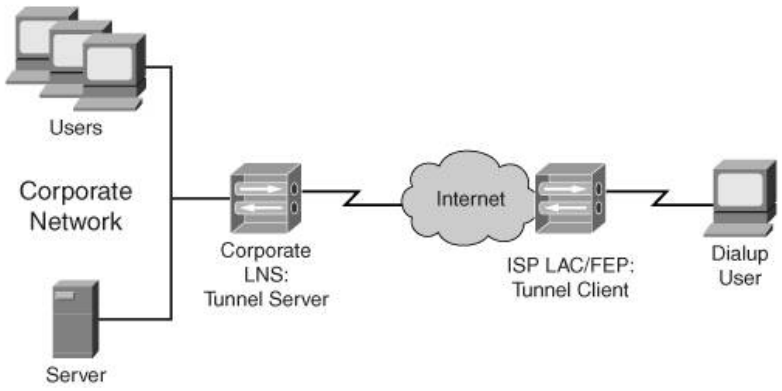
Compulsory(bắt buộc): PC của người sử dụng không là endpoint của tunnel thay vào đó, một thiết bị khác nào đó phía trước PC của người sử dụng, như một server truy cập, đóng vai trò tunnel endpoint điều này tương tự với việc sử dụng một hardware client thay vì một software client.

Với một tunnel tình nguyện(**Voluntary**), remote access client chạy phần mềm L2TP/IPsec và tạo nên kết nối VPN tới server, nó làm việc trong những tình huống nơi mà người sử dụng cũng đang sử dụng một kết nối dialup để đạt đến người phục vụ hay đang sử dụng LAN NIC .

Một đường hầm bắt buộc(**Compulsory**), thiết bị thay mặt người sử dụng chịu trách nhiệm để thiết lập đường hầm.Thiết bị mà bắt đầu đường hầm thông thường được gọi là L2TP Access Concentrator (LAC).Trong PPTP đây là quá trình kết thúc được gọi một Front End Process (FEP).Một server thông thường được gọi là L2TP Network Server (LNS).Vì khách hàng được đòi hỏi để sử dụng đường hầm được tạo ra bởi Gôm lắc/ FEP, Đường hầm được gọi là "Bắt buộc."

Thông thường, LAC/FEPs Được sử dụng trong những tình huống mà một công ty không muốn xử lý chức năng L2TP trên giao diện người sử dụng (của) nó, nhưng muốn giảm bớt L2TP VPN client-side ngoài đối với một ISP.Những người sử dụng sẽ sử dụng dialup hay PPPoE để thiết lập một kết nối PPP tới ISP.Thiết bị ISP sẽ là một LAC/FEP và ISP sẽ chịu trách nhiệm về lưu lượng xuyên qua tunnel PPP tới LNS của văn phòng công ty.

Figure 4-2. L2TP Compulsory Tunnel



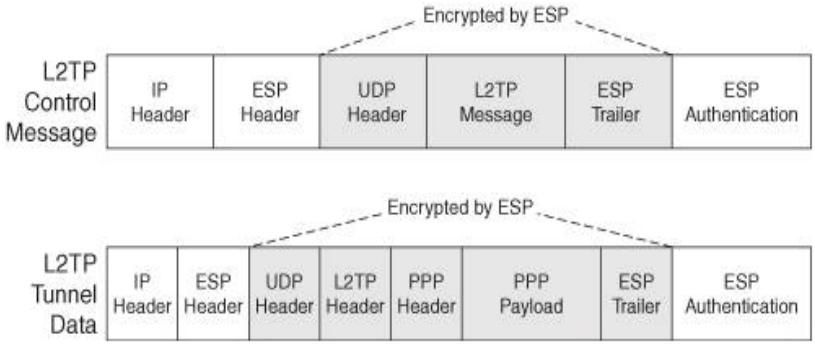
LAC/FEP điển hình có khả năng của lọc lưu lượng xuyên qua đường hầm tới đích được dựa vào mọi số điện thoại người sử dụng quay số hay username của người sử dụng,ý định được dựa vào cả hai phương pháp này, ISP biết sử dụng kết nối đường hầm LNS nào (trong trường hợp ở đâu ISP đang cung cấp dịch vụ này tới nhiều khách hàng).Người sử dụng đầu tiên mà những mặt số vào trong ISP sẽ gây ra LAC/ FEP mang lên trên đường hầm tới LNS tại người sử dụng là văn phòng công ty.Tất cả các khách hàng dialup khác của công ty này nối tới LAC/FEP sẽ sử dụng đường hầm tới văn phòng tập đoàn LNS.

c.IPsec Tunnel

Vì L2TP Sử dụng IPsec như một sự vận chuyển, kết nối IPsec đầu tiên phải được thiết lập giữa LAC và LNS.Đầu tiên, một kết nối quản lý ISAKMP/ IKE phải được xây dựng; sau vài giây một ESP transport mode phải được xây dựng.

Thông tin L2TP được đóng gói trong một ESP payload được hiển thị như hình dưới:

Figure 4-3. L2TP Encapsulation



D .L2TP Control Messages

Với PPTP, một kết nối TCP được sử dụng để trao đổi những gói tin điều khiển control messages).TCP bảo đảm một sự truyền thông đáng tin cậy của PPTP control messages. Vì L2TP tin cậy trên UDP để truyền những control messages, L2TP sử dụng một quá trình bổ sung để bảo đảm sự truyền thông của control messages.Bên trong một L2TP có một trường Next-Received.Những trường server này làm một chức năng tương tự như trường Acknowledgment trong TCP header,một trường khác, Next-Sent, servers làm một chức năng tương tự như trường Number trong TCP header.Những trường này có thể được sử dụng cho sự sắp xếp thứ tự và sự khống chế lưu lượng của những control messages và tunneled packets.

L2TP sử dụng phần lớn những control messages sử dụng PPTP.

Table 4-5. L2TP Control Messages

Message	Description
Start-Control-Connection-Request	L2TP client gửi điều này tới L2TP server để thiết lập kết nối điều khiển; nó cũng bao gồm giá trị Tunnel-ID mà sẽ được sử dụng để xác định duy nhất phiên truyền; thông báo này có thể cũng được dùng để chuyển vào một phiên bản ghép nối, yêu cầu một sự bắt đầu lại của kết nối.
Start-Control-Connection-Reply	L2TP servergửi thông báo này để trả lời cho một Start-Control-Connection-Request message.
Start-Control-Connection-Connected	L2TP Client gửi tới L2TP server sau khi nhận được L2TP server, chỉ ra rằng tunnel đã được thiết lập thành công .
Outgoing-Call-Request	L2TP Client gửi điều này để tạo ra đường hầm dữ liệu.Nó cũng bao gồm một Call-ID, mà được sử dụng để theo dõi mỗi phiên truyền bên trong tunnel.Tình huống này có thể xảy ra trong tunnel mode bắt buộc, nơi mà nhiều dialup clients đang sử dụng giống LAC.Giá trị Call-ID thông thường được tham chiếu tới như một giá trị Session-ID
Outgoing-Call-Reply	L2TP server acknowledges ghi nhận Outgoing-Call-Request message; sau khi nhận được điều này,L2TP client phản hồi với một Start-Control-Connection-Connected message.
Set-Link-Info	Đây được sử dụng bởi L2TP client và server để đàm phán hay những thay đổi tham số kết nối PPP .
Hello	Sử dụng L2TP client và server như một cơ chế keepalive.Khi một lời chào gửi được, một chứng thực được chờ đợi từ thiết bị khác; nếu nó không được thừa nhận bên trong một thời gian, đường hầm được hoàn thành.
WAN-Error-Notify	Được gửi bởi L2TP tới tất cả L2TP clients, chỉ ra một lỗi trên giao diện PPP
Call-Disconnect-Notify	Cả hai L2TP client và server có thể phát sinh thông báo này, chỉ ra một kết nối bên trong một đường hầm (Call-ID) đang được hoàn thành.
Stop-Control-Connection-Notification	Cả hai L2TP client và server có thể phát sinh thông báo này chỉ ra L2TP tunnel được huỷ bỏ.

- **L2TP/IPSec Versus PPTP**

Đầu tiên ta sẽ khảo sát một số sự khác nhau cơ bản giữa những hai giao thức L2TP và PPTP sau đó tìm hiểu những lợi thế mà mỗi giao thức có.

a.Sự khác nhau giữa hai giao thức (Protocol Differences)

Có một vài sự khác nhau giữa PPTP Và L2TP / IPsec.Tuy nhiên, ta sẽ chỉ tập trung vào ba sự khác nhau cơ bản:

- **Quá trình mã hoá (Encryption process).**
- **Thuật toán mã hoá (Encryption algorithms).**
- **Chứng thực người dùng (User authentication).**

Với PPTP, chỉ PPP payload được mã hóa ở phía ngoài phần header được gửi vào trong clear text.Mặt khác, L2TP/IPsec mã hóa toàn bộ gói tin L2TP (control or data).PPTP sử dụng MPPE để mã hóa PPP payload.MPPE sử dụng giải thuật mã hóa RC-4 của RSA, nó hỗ trợ 40- 56 và 128 bit khoá mã hoá (chỉ điểm bắt đầu và điểm cuối cùng là được thực hiện cho PPTP điển hình).L2TP/IPsec hỗ trợ các thuật toán mã hoá **DES (56-bit keys), 3DES (168-bit keys), và AES (128, 192, and 256 bit keys)**. Đã được có chứng minh rằng RC-4 có thể bị cracked.Giống như các ứng dụng DES với Ipsec, tuy nhiên điều này không được chứng minh với 3DES và AES, làm cho L2TP / IPsec có một sự lựa chọn mã hóa an toàn hơn.

PPTP có thể cũng được sử dụng với những hệ thống Windows 95 và cao hơn.L2TP Chỉ được hỗ trợ trên Windows 2000, XP.

b. Những lợi thế của PPTP (PPTP Advantages)

Dưới đây là những lợi thế của PPTP so với L2TP/IPsec:
PPTP là một giao thức hầu như đơn giản hơn so với L2TP/IPsec vì vậy nó dễ dàng hơn cho việc thiết lập và dò tìm lỗi.
PPTP có thể cũng được sử dụng với những hệ thống Windows 95 và cao hơn.L2TP chỉ được hỗ trợ trên Windows 2000 XP và windows server 2003 .
Những PPTP clients và servers PPTP có thể được cài đặt giữa những thiết bị NAT và cũng có thể là những thiết bị PAT, nếu những bản đồ thiết bị PAT có giá trị là caller-ID cho những thiết bị khác nhau.L2TP/IPsec cũng làm việc với NAT, nhưng sẽ bị phá huỷ với PAT trừ phi có NAT-T, IPsec trên TCP, hoặc một vài pương thức của nhà cung cấp khác được sử dụng.Những phương thức IPsec yêu cầu cấu hình đặc biệt trên những thiết bị IPsec, PPTP thì không cần.

c.Những lợi thế của L2TP(L2TP/IPsec Advantages)

Dưới đây là những lợi thế của L2TP/IPsec so với PPTP :
IPsec hỗ trợ sự chứng thực mạnh mẽ hơn thông qua sử dụng những thẻ hay EAP hơn so với PPP's PAP/CHAP/MS-CHAP.
IPsec có thể cung cấp sự chứng thực dữ liệu, sự toàn vẹn dữ liệu, tính bí mật dữ liệu, và sự bảo vệ trong khi mà chỉ PPTP cung cấp tính bí mật cho dữ liệu.
IPsec mã hóa toàn bộ gói PPP trong tất cả các trường hợp.PPTP không mã hóa để điều chỉnh một khởi tạo LCP, bởi vậy nó dễ bị ảnh hưởng hơn đối với phiên truyền hay một sự tấn công trở lại phiên truyền.

- **PHÂN TÍCH NHU CẦU THỰC TIỄN ĐỂ LỰA CHỌN GIẢI PHÁP VÀ GIAO THỨC VPN THÍCH HỢP**
- **VPN VỚI CÁC DOANH NGHIỆP**

Khai thác những thế mạnh của công nghệ để tối ưu hóa quá trình hoạt động, kinh doanh là một trong những mối quan tâm hàng đầu của các doanh nghiệp (DN) hoạt động trong nhiều lĩnh vực khác nhau.Một hệ thống mạng hoàn hảo không chỉ giải quyết tốt những vấn đề bên trong mạng nội bộ mà còn phải có khả năng kết nối linh hoạt, đáp ứng tốt nhu cầu kết nối giữa các điểm khác nhau nhằm tạo thành một hệ thống mạng thống nhất.Việc đáp ứng các nhu cầu kết nối từ xa này không thể nói khác hơn là dịch vụ VPN mà một hệ thống mạng năng động phải được tích hợp.VPN hiện nay không chỉ đáp ứng tốt những yêu cầu về kết nối chia sẻ dữ liệu mà nó còn có khả năng cung cấp đường truyền cho những ứng dụng trên nền tảng IP như VoIP, Video Conferencing.
Những ứng dụng này sẽ mang lại cho người sử dụng sự tối ưu, tiết kiệm, linh hoạt.Để thiết lập một hệ thống như vậy, ta có thể sử dụng phần mềm hay phần cứng dựa trên nền tảng hệ thống mạng IP trên các đường truyền như Leasedline, ATM, Frame Relay, ISDN hay các đường truyền xDSL như SHDSL, ADSL,...
Sau đây là những thông tin cơ bản về công nghệ VPN và các yêu cầu cần thiết để thiết lập một hệ thống mạng riêng ảo.Vậy VPN là gì? Làm sao để xây dựng một hệ thống VPN tiện lợi, bảo mật, tiết kiệm chi phí và phù hợp cho DN?
VPN-Virtual Private Network (mạng riêng ảo) là một kỹ thuật thông qua các kênh riêng để tạo kết nối **Point-to-Point** (điểm đến điểm) hay **Point-to-MultiPoint** (điểm đến nhiều điểm) giữa các điểm giao dịch thông qua hạ tầng mạng công cộng (như mạng Internet) hay những đường thuê bao riêng.Các kênh truyền dẫn riêng như Leasedline, Frame Relay có một chi phí đầu tư phần cứng khá cao và tăng dần theo khoảng cách giữa các điểm kết nối, hoạt động trên nền tảng công nghệ định tuyến IP cũ nên với những lưu lượng giao thông mạng lớn các tuyến nối kết này không được tối ưu lắm.Với một chi phí thuê bao khá cao, như vậy các đường thuê bao riêng này chỉ thích hợp cho những công ty lớn có nhiều chi nhánh nằm ở các địa điểm khác nhau.Sự phát triển của công nghệ **Multi Protocol Label Switching (MPLS)** với khả năng truyền tải cao, linh hoạt, bảo mật hơn sẽ là một giải pháp mạng đường trục có khả năng truyền tải tất cả các tín hiệu và đang dần thay thế các đường thuê bao truyền thống trong giải pháp VPN.Với các DN vừa và nhỏ, có thể thực hiện VPN trên công nghệ MPLS qua đường truyền băng rộng ADSL hay SHDSL.Dữ liệu trên các tuyến kết nối này được bảo vệ bởi các cơ chế mã hoá khác nhau tùy khả năng của các thiết bị phần cứng hay chương trình phần mềm nhằm đảo bảo dữ liệu của bạn không bị thất thoát, bị ngăn chặn bởi các truy cập trái phép trên đường truyền chung.Những cơ chế thông dụng bao gồm IPSec và SSL (Secure Sockets Layer).
Dịch vụ VPN giúp được gì cho DN?Triển khai được một hệ thống mạng tích hợp dịch vụ VPN sẽ giúp DN có được một hệ thống mạng linh hoạt, uyển chuyển và có khả năng đáp ứng nối kết cho mọi nhân viên, hay các đối tác tin cậy truy cập vào hệ thống mạng nội bộ của công ty nhằm mang lại hiệu quả hoạt động cao nhất cho DN.Vấn đề khoảng cách đã trở nên đơn giản hơn bao giờ hết, khi ta thực thi được các kết nối về trung tâm thông qua những kênh kết nối công cộng bất kỳ như trên đường truyền

Internet hay trên đường modem kết nối quay số về hệ thống lưu trữ trung tâm.Hơn nữa có thể hợp nhất các mạng lại thành một vùng mạng thống nhất nhằm chia sẻ dữ liệu dùng chung trên các mạng này với nhau và cho bạn một giải pháp sao lưu dữ liệu.Không chỉ là việc chia sẻ dữ liệu trên đường truyền, với một thuê bao có chất lượng tốt, bạn có thể triển khai thêm những dịch vụ hữu ích khác như thiết lập một hệ thống VoIP nhằm tiết kiệm tối đa chi phí liên lạc giữa trung tâm và các chi nhánh văn phòng, công ty nằm ở các vùng địa lý khác nhau với một chi phí cuộc gọi theo mô hình Trung tâm -Chi nhánh là bằng 0.Đây là một giải pháp khá ấn tượng và hiệu quả trên mọi phương diện phần cứng và phấn mềm.Bên cạnh một dịch vụ mới mang lại nhiều hiệu quả cũng được thực hiện trên đường truyền này đó là dịch vụ hội thảo truyền hình, một dịch vụ giúp DN có thể tổ chức các cuộc họp trực tuyến giữa trung tâm và nhân viên các phòng ban ở các chi nhánh vào bất kỳ lúc nào nhằm giảm bớt chi phí đi lại như các cuộc gặp mặt truyền thống giữa các các đối tượng này và trung tâm lãnh đạo.
Dựa vào thực tế ta nhận thấy có 2 giải pháp để bạn có thể tham khảo với một chi phí đầu tư ban đầu không quá cao.

VPN trên nền tảng phần mềm: với sự hỗ trợ của thiết bị dẫn đường (Router ADSL) trên đường truyền ADSL.Sử dụng một Router có khả năng hỗ trợ DDNS, Virtual Server …bạn có thể kết hợp với ISA 2006 Server để có được một hệ thống VPN Server có chi phí tiết kiệm nhất.Tuy nhiên, với một hệ thống như vậy chỉ đáp ứng có giới hạn số lượng người truy cập vào hệ thống mạng tại cùng một thời điểm.

VPN trên nền tảng phần cứng và kênh thuê riêng: khả năng quản lý dễ dàng, có tích hợp những tính năng Firewall sáng giá giúp bảo vệ những tuyến kết nối bảo mật hơn so với việc dùng VPN mềm.Các thiết bị phần cứng cho phép bạn tạo nhiều chính sách truy cập khác nhau nhằm bảo mật hệ thống bên trong của bạn.Thường thì các phần cứng đi theo số lượng từ 500 đơn vị người sử dụng trở lên.Các thiết bị chuyên dùng thường có chi phí đầu tư khá cao nhưng khả năng chúng mang lại tương ứng với mức độ đầu tư của DN.Bên cạnh đó có những thiết bị phần cứng VPN Server của các hãng sản xuất thứ ba với chi phí thấp hơn, phù hợp cho một DN có quy mô vừa và nhỏ với số lượng nhân viên di động thường xuyên công tác ngoài công ty có nhu cầu kết nối về hệ thống mạng của công ty để truy xuất dữ liệu phục vụ công việc.

Giải pháp 1: Dựa vào hạ tầng mạng ADSL sẵn có của bạn với chi phí đầu tư thấp nhất:
Đối với DN vừa và nhỏ, số lượng nhân viên di động ra ngoài không quá nhiều thì giải pháp dùng thiết bị phần cứng của các hãng thứ ba sẽ giúp bạn giải quyết tốt những yêu cầu này.Trên thị trường hiện nay, có một số hãng đã sản xuất Router có tích hợp khá tốt chức năng của một VPN Server phần cứng.Và chi phí đầu tư các thiết bị này khá khiêm tốn so với các thiết bị chuyên dụng của các hãng nổi tiếng khác.

Với một Router ADSL và một đường thuê bao băng thông rộng tương đối cao (ADSL hay ADSL2+) là bạn có thể thiết lập được một hệ thống mạng có khả năng đáp ứng tốt dịch vụ VPN cho các máy PC từ xa.Việc kết nối về máy chủ bạn có thể đăng ký một địa chỉ IP tĩnh hay sử dụng IP động dựa trên công nghệ DDNS mà Router này hỗ trợ.Với khả năng hỗ trợ 16 đến 32 tuyến kết nối bảo mật đồng thời, thiết nghĩ đã đáp ứng khá tốt cho nhu cầu của một DN vừa và nhỏ.Hơn nữa, nếu bạn cần nối mạng LAN với một chi nhánh của mình, việc thiết lập cũng được Router hỗ trợ dễ dàng thông qua khả năng kết nối Site to Site, Site to MultiSite.Và bạn nên thiết lập một máy Server làm Radius Server dùng xác thực quyền của người sử dụng muốn truy cập vào hệ thống mạng LAN, như vậy mạng của bạn sẽ bảo mật hơn so với việc dùng chỉ đơn thuần khả năng hỗ trợ của thiết bị.Với giải pháp này, vấn đề là bạn chỉ cần chọn cho mình một thiết bị băng thông rộng phù hợp, có khả năng phục vụ tốt yêu cầu cần thiết của mình với một chi phí không quá cao.

Giải pháp 2: Dựa vào một nhà cung cấp đường truyền với các thiết bị phần cứng của các nhà sản xuất thứ 3:
Với mức đầu tư tương đối, ta có thể chọn cho mình giải pháp thuê một kênh truyền dẫn riêng thông qua một số nhà cung cấp dịch vụ.Trong đó có thể kể đến VTN (Công ty Viễn Thông liên tỉnh) cung cấp dịch vụ MegaWAN sẽ cho bạn 2 chọn lựa: đường truyền SHDSL hay ADSL với tốc độ đường truyền riêng đạt được khá cao (SHDSL-WAN tốc độ cao nhất đạt 2,3Mbps hay ADSL-WAN tốc độ cao nhất đạt được 8MBps) và có thêm những địa chỉ IP tĩnh.Thuê bao MegaWAN, với mỗi điểm đầu cuối bạn cần thuê bao các đường kết nối tới VNPT.Thông qua hệ thống Router dẫn đường, qua giao thức chuyển mạch thế hệ mới MLPS (Multi Protocol Label Switching) sẽ giúp các thiết bị của bạn chuyển tải các gói tin nhanh chóng và bảo mật.Tuỳ theo khoảng cách giữa các vùng được VTN phân định mà có các mức thuê bao khác nhau.Thiết kế sử dụng cho kết nối nội bộ nhưng trên đường truyền riêng này bạn có thể đăng ký sử dụng thêm dịch vụ Internet với mức chi phí hợp lý.VTN cung cấp 3 dịch vụ VPN cơ bản: MegaWAN nội tỉnh, MegaWAN liên tỉnh và MegaWAN quốc tế.

Thiết bị đầu cuối CPE (Modem/Router ADSL-SHDSL) sử dụng cho các đường truyền này có thể sử dụng các thiết bị của các nhà cung cấp có uy tín trên thế giới như Cisco, Netgreen, Juniper, CheckPoint,... với giá thành khá đắt, nhưng những gì mà các thiết bị này mang lại đáng với giá trị mà phải đầu tư.Nếu không ta có thể sử dụng các thiết bị mạng của các nhà sản xuất khác có giá thành thấp hơn rất nhiều nhưng về cơ bản có thể đáp ứng khá tốt các yêu cầu về kết nối cho hệ thống mạng.

Thông tin các gói thuê bao đường truyền mà ta có thể lựa chọn:

Thực hiện VPN trên đường truyền MegaWAN, tại mỗi điểm kết nối ta cần những yêu cầu sau:

Cước thuê cổng megaWAN: bao gồm cước đấu nối hoà mạng và cước thuê cổng

Cổng	Lắp đặt đường dây thuê bao mới	Lắp đặt đường dây thuê bao có sẵn, đủ điều kiện kỹ thuật	Cước thuê cổng
ADSL (2M/640K)	*600.000 đ/lần/cổng*	*300.000 đ/lần/cổng*	*181.818 VNĐ/cổng/tháng*
SHDSL (2M/2M)	*1000.000 đ/lần/cổng*	*700.000 đ/lần/cổng*	*272.727 VNĐ/cổng/ tháng.*

Cước thuê kênh đường lên cho dịch vụ MegaWAN nội tỉnh:

Tốc độ (Kb/s)	Cước đường lên (1000đ/tháng)	Cước đấu nối hoà mạng(bắt buộc)
256	*688*	-Tốc độ dưới 512Kb/s: 150.000 đồng/lần -Tốc độ trên 512Kb/s:500.0000 đồng/lần
512	*1.107*	
768	*1.340*	
1024	*1.661*	
1600	*2.399*	
2048	*2.753*	

Cước thuê kênh đường lên MegaWAN liên tỉnh(một số tốc độ làm chuẩn)

Tốc độ kênh (Kb/s)	Cước đường lên (1000đ)			Cước đấu nối hoà mạng (bắt buộc)
	Nội vùng	Cận vùng	Cách vùng	Không thấp hơn cước đấu nối hòa mạng kênh đường lên MegaWAN nội tỉnh, không cao hơn cước đấu nối hòa mạng kênh MegaWAN quốc tế
128	*1105*	*1616*	*2354*	
256	*1550*	*2175*	*3137*	
1024	*106*	*2932*	*4187*	
1544/1536	*417*	*6591*	*10240*	
2048	*6303*	*7668*	*10997*	
Với các qui định về vùng cước :+Vùng 1: Bao gồm các tỉnh thuộc miền Bắc đến tỉnh Quảng Bình +Vùng 3: Bao gồm các tỉnh từ Quảng trị đến các kênh MegaWAN liên tỉnh có hai điểm kết nối cùng nằm trong một vùng (1,2,3) tỉnh Khánh Hòa và tỉnh Đắc Lắc, Đắc Nông +Vùng 2: Các tỉnh còn lại Cước nội vùng: Áp dụng cho Cước cận vùng: áp dụng cho các kênh MegaWAN liên tỉnh kết nối từ vùng 1 đến vùng 3 và ngược lại, vùng 2 đến vùng 3 và ngược lại				

Song song đó, VTN cũng cung cấp những tuyến kết nối MegaWAN quốc tế.Tuy nhiên do dịch vụ MegaWAN là mạng đường trục riêng của VNPT nên bạn chỉ có thể thực hiện được dạng kết nối điểm-điểm, điểm-đa-điểm giữa trung tâm và chi nhánh mà không thực hiện được kết nối dạng Remote từ một PC trên mạng Internet vào bên trong mạng LAN của công ty.Để thực hiện điều này bạn có thể kết hợp thêm giải pháp 1 vào.

Giải pháp 3: thuê bao đường truyền Internet riêng (Lesea-Line), thiết bị chuyên dùng:

Đây là giải pháp có chi phí đầu tư cao nhất với kênh truyền Internet riêng và những thiết bị chuyên dụng của các hãng thiết bị mạng nổi tiếng như Cisco, Nortel, Juniper,...Sử dụng giải pháp kết nối này sẽ mang lại cho bạn sự linh hoạt, uyển chuyển tối đa.Hệ thống mạng luôn sẵn sàng với mọi kết nối từ bất cứ nơi đâu, tại bất cứ thời điểm nào.
Sau khi thiết lập được một hệ thống VPN ổn định, bảo mật.Xem như ta đã thiết lập xong nền tảng để chạy những ứng dụng hữu ích khác như VoIP, Video Conferencing (hội thảo truyền hình).Những công nghệ hiện nay đang được ứng dụng, khai thác có hiệu quả trong hầu hết các DN có qui mô lớn trên thế giới nhằm giảm thiểu các chi phí liên lạc, giao dịch nhờ vào hệ thống mạng sẵn có của công ty.
Để thực thi hệ thống VoIP, tại mỗi điểm đầu cuối chỉ cần trang bị thêm một VoIP Gateway có khả năng đấu nối vào hệ thống tổng đài nội bộ PBX là ta có thể thực hiện các cuộc giữa các hệ thống tổng đài thông qua các tuyến kết nối này.Các thiết bị này cũng có nhiều lựa chọn từ các nhà cung cấp thiết bị mạng VoIP khác nhau, từ những sản phẩm bình dân cho tới những sản phẩm chuyên nghiệp có khả năng chạy trên những hệ thống lớn với khả năng đáp ứng nhiều cuộc gọi đồng thời.Ứng dụng VoIP giúp tiết kiệm tối đa chi phí liên lạc giữa trung tâm và tất cả các chi nhánh khác nhau.
Để thực thi Video Conferencing ta cần trang bị thêm những thiết bị chuyên dùng hay có thể thuê bao các thiết bị này thông qua VTN (đối với những cuộc họp có qui mô) hay FPT. Đối với những cuộc họp hay trao đổi qui mô nhỏ ta có thể sử dụng những phần mềm hỗ trợ khả năng hội thảo qua mạng LAN với giá thành không quá cao.
Qua các phần trên chúng ta nhận thấy rằng, kết nối VPN mang lại cho DN nhiều lợi ích thực tế, giúp cho những nhân viên thường xuyên đi công tác xa chủ động hơn trong công việc.DN có thể triển khai dễ dàng, nhanh chóng với chi phí thấp nhất dựa vào hạ tầng mạng sẵn có (đường truyền ADSL tốc độ cao).Giờ đây, nhờ vào VPN mà khoảng cách đã được xóa mờ.

LỰA CHỌN GIAO THỨC PHÙ HỢP VỚI NHU CẦU THỰC TẾ

ISA Firewall hỗ trợ ba giao thức VPN cho mạng riêng ảo site-to-site: **IPSec tunnel mode**, **L2TP/IPSec** và **PPTP**.
IPSec tunnel mode được giới thiệu cùng ISA 2004.Với giao thức này, ISA Firewall có thể được dùng như một cổng vào VPN site-to-site cùng với các cổng vào VPN thuộc nhóm thứ ba.Điều này chỉ thực hiện được với các IPSec tunnel mode, vì mô hình này vốn bị xem là kém an toàn và khả năng thực thi thấp hơn so với L2TP/IPSec.Ngoài ra, hỗ trợ định tuyến cho mô hình IPSec tunnel mode là rất khó, nặng nề và bị giới hạn.
L2TP/IPSec là giao thức VPN site to site được yêu thích hơn vì cả hai mặt của mạng riêng ảo site-to-site đều dùng ISA Firewall và cổng vào VPN thuộc nhóm thứ ba hỗ trợ L2TP/IPSec.L2TP/IPSec hỗ trợ các khóa pre-shared nên trong môi trường sản xuất an toàn, bạn có thể dùng thông tin thẩm định chứng chỉ cho cả tài khoản máy và tài khoản người dùng để chứng thực "đường hầm" mạng riêng ảo (VPN tunnel).Đây là kiểu cấu hình rất an toàn, nhưng hầu hết các công ty đều thích dùng chế độ thẩm định non-EAP cho tài khoản người dùng giao diện deman-dial và thẩm định chứng chỉ cho tài khoản máy.
PPTP là giao thức hỗ trợ các kết nối VPN site to site dễ dàng nhất.Không cần chứng chỉ, PPTP "chỉ làm việc và làm việc".Có một điểm hạn chế là PPTP kém an toàn hơn L2TP/IPSec vì hàm băm thông tin thẩm định được gửi qua kênh không được mã hóa. Do đó, mức bảo mật kết nối PPTP cung cấp phụ thuộc lớn vào độ phức tạp của mật khẩu. PPTP không cung cấp các chức năng từ chối và bảo vệ trong quá trình lặp lại như ở L2TP/IPSec.
Sử dụng IPSec tunnel mode để kết nối tới cổng vào mạng riêng ảo của nhóm thứ ba là cách dễ nhất.Việc đầu tiên là bạn nên xem xét thông tin sử dụng ISA Firewall với các cổng vào VPN của nhóm thứ ba tại website của Microsoft.
Nếu phần hướng dẫn này không giải quyết được vấn đề, bạn cần phải xem xét đến IPSec. Hãy đảm bảo chắc chắn rằng các tham số IPSec đã chính xác trên cả hai mặt.Ngay cả khi đã có các tham số chính xác, bạn vẫn có thể gặp phải vấn đề với cổng vào VPN phụ thuộc non-RFC.Ví dụ, ta đã từng nghe nói đến một số báo cáo về tường lửa Sonicwall không làm việc với cổng vào ISA Firewall VPN.Lý do bởi chúng không phải là bản thể của RFC và không cho phép IKE sử dụng cổng nguồn thay vì UDP 500.Do ISA Firewall là một bản thể của RFC, nó có thể dùng một cổng luân phiên và do đó, không cần kết nối tới thiết bị Sonicwall.Với Sonicwall, bạn có thể dùng bản update phần mềm để biến thiết bị thành kiểu RFC.
Một vấn đề phổ biến khác là các tài khoản người dùng VPN site-to-site không được cấu hình chính xác phù hợp với tên giao diện demand-dial.Khi điều này diễn ra (có một số lần xuất hiện cả lúc mạng riêng ảo đã được kết nối), không có bất kỳ lưu lượng nào đi qua được cổng vào VPN từ mạng này tới mạng khác.Hoặc có thể bạn sẽ thấy dường như các kết nối được phép thực hiện, nhưng không phải từ mạng khác.Lý do là bởi kết nối VPN site-to-site không được thiết lập. Bạn có thể kiểm chứng điều

này bằng cách mở console RRAS và kiểm tra nút Remote Access Clients ở khung bên trái. Nếu thấy có một kết nối client truy cập từ xa cho cổng vào VPN từ xa, chứng tỏ kết nối VPN client truy cập từ xa đã được thực hiện chứ không phải là kết nối VPN site to site.Các kết nối client truy cập từ xa sẽ không cho phép định tuyến qua cổng vào VPN.
Vì những lý do đó, khuyến cáo các admin quản trị ISA Firewall nên sử dụng L2TP/IPSec với một máy thẩm định chứng chỉ. Tuy nhiên hầu hết các trường hợp triển khai ban đầu đều cài đặt mạng riêng ảo site-to-site dùng khóa "tiền chia sẻ" nhằm xây dựng khả năng đáng tin cậy vào giải pháp và loại bỏ một số thừa kế phức tạp trong PKI. Sau khi giải pháp VPN site to site hoàn chỉnh thời gian thử nghiệm cuối cùng, nên chuyển khách hàng sang máy có cơ chế thẩm định chứng chỉ và nói lời tạm biệt với các khóa tiền chia sẻ.
Sau đây ta hãy đặt vấn đề tìm kiếm, lựa chọn giải pháp an toàn dữ liệu trong VPN, trong đó đề cập, so sánh hai giải pháp về VPN, đó là giải pháp VPN truyền thống dựa trên IPSec (Internet Protocol Security) và giải pháp SSL (Secure Socket Layer) giúp cho việc quyết định lựa chọn giải pháp VPN phù hợp.

IPSEC VPN: VPN Ở LỚP MẠNG (Network Layer VPN)

IPSec (Internet Protocol Security) là giao thức mạng về bảo mật và thường được liên kết với VPN (tất nhiên có thể dùng IPsec ở trong mạng cục bộ LAN).IPSec cho phép việc truyền tải dữ liệu được mã hóa an toàn ở lớp mạng (Network Layer) theo mô hình OSI thông qua mạng công cộng như Internet.VPN lớp mạng đề cập đến những thách thức trong việc dùng Internet như là một môi trường truyền đưa các lưu lượng đa giao thức và nhạy cảm .
Việc thiết lập một đường hầm IPSec (IPsec tunnel) giữa hai thực thể, trước tiên, phải thỏa thuận về chính sách an ninh (security policy), giải thuật mã hóa (encryption algorithm), kiểu xác thực (authentication method) sẽ được dùng để tạo kênh.Trong IPSec tất cả các nghi thức lớp trên lớp mạng (từ lớp 4) như TCP, UDP, SNMP, [Only registered and activated users can see links] POP, SMTP, KaZaa…đều được mã hóa một khi kênh IPSec được thiết lập.

SSL VPN LÀ GÌ?

Thuật ngữ SSL VPN được dùng để chỉ một dòng sản phẩm VPN mới và phát triển nhanh chóng dựa trên giao thức SSL.Cũng cần nói rõ là bản thân giao thức SSL không mới nhưng liên kết SSL với VPN là mô hình mới.Dùng SSL VPN, kết nối giữa người dùng từ xa và tài nguyên mạng công ty thông qua kết nối [Only registered and activated users can see links] ở lớp ứng dụng thay vì tạo "đường hầm" ở lớp mạng như giải pháp IPSec.SSL VPN là giải pháp VPN hướng ứng dụng (application based VPN).

SSL VPN hay IPsec VPN?

Trước tiên, cần phải khẳng định là SSL VPN và IPSec VPN không phải là hai công nghệ loại trừ lẫn nhau.Thường thì hai công nghệ này đồng thời được triển khai trong cùng một công ty.Việc xem xét các khía cạnh liên quan đến chi phí/lợi nhuận (cost/benefit) cũng như các vấn đề công nghệ mà hai giải pháp SSL và IPsec đề cập giúp cho việc lựa chọn triển khai VPN sẽ trở nên dễ dàng hơn. Chúng ta xem xét vấn đề dưới các mặt sau đây:

- **Kiểu kết nối, kiểu truy cập:**

IPSec VPN phù hợp cho các kết nối theo kiểu site-to-site.Nó là sự lựa chọn tốt nhất cho các mạng LAN từ xa kết nối với nhau hay kết nối với mạng trung tâm.Các kết nối yêu cầu băng thông rộng, hiệu suất cao, dữ liệu lớn, kết nối liên tục (always on), cố định là đối tượng cung cấp của giải pháp IPsec VPN truyền thống này.Tuy nhiên, khi được dùng cho mục đích truy cập tài nguyên tập trung từ các vị trí phân bố rải rác khắp nơi, hay khi người dùng di động từ xa từ các vị trí công cộng ít tin cậy như sân bay, nhà ga, khách sạn, tiệm cà phê internet muốn truy cập vào tài nguyên của công ty họ thì giải pháp IPSec VPN tỏ ra nhiều bất cập và đó chính là ưu điểm của SSL VPN.
Có thể lấy một ví dụ điển hình việc triển khai SSL VPN của Công ty Bảo hiểm Việt Nam (Bảo Việt) được trình bày trong hội thảo về An ninh mạng do Công ty Juniper Networks tổ chức tại TP. Hồ Chí Minh ngày 30/11/2004.Giải pháp SSL VPN của Juniper dựa trên dòng sản phẩm NetScreen phù hợp nhu cầu của Bảo Việt.Bảo Việt có hàng ngàn các đại lý bảo hiểm rải khắp các tỉnh thành trong cả nước, từ đó có hàng trăm các kết nối di động đến Trung tâm dữ liệu của Bảo Việt.Do đó giải pháp SSL VPN là rất phù hợp.Tuy nhiên, Bảo Việt dự tính xây dựng thêm một trung tâm dữ liệu thứ hai và việc kết nối hai trung tâm này (dạng site-to-site) qua môi trường Internet thì giải pháp IPSec cần được xem xét.

- **Phần mềm khách (Client software):**

IPSec VPN yêu cầu cần phải có phần mềm client cài đặt tại các máy tính để bàn hoặc máy tính xách tay.Điều này làm hạn chế tính linh động của người dùng vì không thể kết nối VPN nếu không có phần mềm IPSec client được nạp.Trong khi với giải pháp SSL VPN, chỉ cần hệ điều hành có tích hợp một trình duyệt (browser) bất kỳ hỗ trợ SSL là thực hiện được một kết nối an toàn.Sự có mặt khắp nơi của

trình duyệt trên tất cả các thiết bị từ máy tính đến PDA, điện thoại thông minh… làm công nghệ VPN dựa trên SSL dễ triển khai hơn.
Vì cần phải cài phần mềm IPsec client trên các thiết bị truy cập từ xa, nên điều này làm tăng thêm chi phí quản trị, cấu hình.Với một công ty có hàng trăm, thậm chí hàng ngàn người dùng từ xa thì việc cài đặt, quản lý, hỗ trợ người dùng trong giải pháp IPSec là công việc tốn nhiều thời gian, công sức, tài nguyên và tiền bạc của công ty.SSL VPN thật sự là giải pháp hiệu quả trong trường hợp này.

- **Độ tin cậy của thiết bị truy nhập hay mạng từ xa:**

Với IPSec VPN, người dùng từ xa hay mạng LAN từ xa kết nối với trung tâm có thể dễ dàng truy cập đến toàn bộ tài nguyên mạng như thể họ đang ngồi tại trung tâm.Vì vậy, các thiết bị hay mạng từ xa phải tin cậy (trusted), mặt khác vì các thiết bị truy cập được quản lý và cài đặt cấu hình nên IPSec VPN đáp ứng nhu cầu này.Tuy nhiên, mọi việc trở nên khó khăn nếu như chúng ta cung cấp giải pháp này cho người dùng từ xa không có độ tin cậy tương tự và các thiết bị truy cập đa dạng như PDA, điện thoại thông minh (smart phone) không do chúng ta quản lý hay cài đặt cấu hình IPSec client.

- **Kiểm soát truy cập (Access Control):**

IPSec VPN được thiết kế để mở rộng phạm vi của mạng LAN.Người dùng ở các chi nhánh văn phòng cũng muốn truy cập không hạn chế tài nguyên mạng một cách hiệu quả, đòi hỏi các chính sách an ninh của mạng từ xa cũng tương tự như của mạng tại trung tâm. Do đó các giải pháp IPSec được áp dụng rất hiệu quả cho mô hình site-to-site.Sự việc sẽ khác đi nếu chúng ta cho phép các nhân viên thường xuyên di chuyển, các đại lý, các nhà cung cấp, nhà thầu, các đối tác thương mại kết nối vào mạng chúng ta.Và giải pháp SSL VPN là một lựa chọn hợp lý nhằm giảm thiểu nguy cơ đến từ các kết nối này nhờ cơ chế kiểm soát chi tiết (granular access control).

- **Độ bảo mật (security):**

Khi so sánh SSL VPN và IPsec VPN thường có câu hỏi được đặt ra "Giao thức nào an toàn hơn?"Thật ra, cả hai nghi thức bảo mật này đều hoàn tất nhiệm vụ tương tự.Chúng đều cung cấp một phương pháp trao đổi khóa an toàn (secure key exchange) và phương pháp mã hóa mạnh. Mặc dù hai công nghệ khác nhau, tiến hành thiết lập, triển khai trên các hệ thống theo các phương thức khác nhau, thế nhưng chúng đều chia sẻ chung một số đặc trưng cơ bản đó là cơ chế mã hóa mạnh, dùng khóa phiên (session key), khả năng xác thực sử dụng các phương pháp, công nghệ như: Triple DES, 128-bit RC4, MD5, SHA1, RADIUS, Active Directory, LDAP, X.509.

- **Tương thích Firewall, NAT:**

Việc kết nối IPSec thông qua Firewall cũng là một khó khăn.IPSec dùng các giao thức AH (Authenticated Header) hoặc/và ESP (Encapsulating Security Payload).Nếu Firewall của ISP ngăn không cho hai nghi thức này đi qua hoặc ngăn cổng UDP mà IKE (Internet Key Exchange) dùng để thương lượng các thông số bảo mật trước khi kết nối thì IPSec không thể thực hiện được.Một thách thức khác là sự không tương thích của IPSec với dịch địa chỉ mạng NAT (Network Address Translation).Trong khi đó, giải pháp SSL VPN tương thích hoàn toàn với Firewall, NAT hay server proxy.

- **Ứng dụng:**

IPSec VPN hỗ trợ tất cả các ứng dụng trên nền tảng IP.Một khi kênh IPSec được thiết lập, tất cả các dịch vụ ứng dụng từ các ứng dụng truyền thống như web, thư điện tử, truyền tệp đến các ứng dụng khác như ICMP, VoIP, SQL* net, Citrix ICA, các ứng dụng đa dịch vụ… đều cho phép đi ngang qua kênh này. Đây là một ưu điểm của IPSec VPN, nhất là IPSec VPN có thể cung cấp kết nối an toàn cho các ứng dụng không dựa trên nền Web (non Web-based applications). Vì vậy, các máy khách (client) dùng IPSec thực hiện kết nối VPN được gọi là fat-client do khả năng cung ứng nhiều dịch vụ và ứng dụng.Trong khi đó, khả năng truy cập các ứng dụng, dịch vụ của giải pháp SSL VPN dường như hạn chế hơn. SSL VPN cung cấp các ứng dụng trên nền Web (Web-based application), các ứng dụng e-mail (POP3/IMAP/SMTP).Các máy khách (client) chỉ cần dùng trình duyệt (browser) có hỗ trợ SSL thực hiện kết nối VPN mà không cần cài đặt phần mềm client nên được gọi là clientless hoặc thin-client.Đa số các giải pháp SSL VPN không cung cấp các ứng dụng dùng cổng TCP động như FTP hay VoIP.Hiện nay, mọi người vẫn chỉ biết đến SSL VPN chỉ hỗ trợ các ứng dụng trên nền Web. Thật ra, SSL VPN hỗ trợ cả các ứng dụng trên nền TCP sử dụng chương trình chuyển tiếp cổng (port forwarding applet) như Terminal Services (RDP protocol) hoặc ứng dụng chia sẻ tệp CIFS (Common Internet File Service), Citrix ICA… (riêng dòng sản phẩm Cisco VPN 3000 Concentrator hiện chưa hỗ trợ Citrix ICA, hãng Cisco dự định sẽ hỗ trợ ứng dụng này trong phiên bản sắp tới).

- **XU HƯỚNG**

Hiện nay, với xu hướng thương mại điện tử, nhiều ứng dụng trên nền Web được xây dựng.Hãng Gartner đã dự đoán: "Đến cuối năm 2004, 60 % công ty sử dụng thin-client VPN (SSL VPN) thay vì full, fat-client VPN (IPSec VPN)"[7].Thêm vào đó, hãng Frost and Sullivan đánh giá đến năm 2008,

doanh số giải pháp SSL VPN sẽ vượt qua 1 tỷ USD và chi phí trung bình cho một người dùng của giải pháp SSL VPN từ 60 USD đến 200 USD so với 150 USD đến 300 USD khi dùng giải pháp IPSec VPN[7]. Nhìn vào con số ấn tượng trên, chúng ta có cảm tưởng tương lai thuộc về SSL VPN. Tuy nhiên theo nghiên cứu mới nhất của Infonetics Research ([Only registered and activated users can see links]) (quý 3 năm 2004), giải pháp VPN và Firewall phần cứng chiếm 82%, phần mềm VPN chiếm 12%, SSL VPN chỉ chiếm có 5% và dự báo đến năm 2007 mới chiếm 14% thị phần VPN và Firewall.Vì vậy, có thể tạm kết luận giảI pháp IPSec VPN đang chiếm ưu thế, nhưng khuynh hướng dùng giải pháp SSL VPN đang gia tăng.

Hãng Juniper sau khi mua lại hãng chuyên về sản phẩm bảo mật mạng NetScreen vào đầu năm 2004 hiện dẫn đầu thị trường SSL VPN với 57 % (Hình 3).Kế tiếp là F5 (14%), Aventail (12 %), Nokia (9%).Chàng khổng lồ Cisco hình như chậm chân trong cuộc chơi này. Sản phẩm chuyên về Firewall series 500 PIX của hãng hiện chỉ hỗ trợ IPSec.Dòng sản phẩm chủ đạo về VPN 3000 Concentrator mới hỗ trợ cả hai công nghệ IPSec và SSL VPN. Nhưng xét về tổng thể các giải pháp VPN và Firewall thì Cisco System vẫn đứng đầu, tiếp theo là Checkpoint Software Technologies, thứ ba là Juniper Network.

- **KẾT LUẬN**

Giải pháp VPN nào là tốt nhất cho kết nối từ xa? Điều này phụ thuộc nhiều yếu tố như phân tích ở trên.IPSec VPN phù hợp cho các kết nối thường trực site-to-site, nhằm đảm bảo an toàn cho tất cả các dịch vụ trên nền IP từ Web, email, truyền tệp đến các ứng dụng VoIP và đa dịch vụ.Trong khi đó, SSL VPN thích hợp cho các ứng dụng trên nền Web, cho phép kết nối an toàn bất kỳ thiết bị nào hỗ trợ trình duyệt web. Cả hai công nghệ đều an toàn hay có nguy cơ mất an toàn giống nhau.Tùy trường hợp mà giải pháp nào sẽ được ưu tiên thiết lập, nhưng thường thì các tổ chức triển khai cả hai công nghệ VPN này trên hạ tầng cơ sở mạng của họ.

- **Bảo mật Wi-Fi: Lựa chọn giải pháp**

Bảo mật là vấn đề rất quan trọng và đặc biệt rất được sự quan tâm của những doanh nghiệp.Không những thế, bảo mật cũng là nguyên nhân khiến doanh nghiệp e ngại khi cài đặt mạng cục bộ không dây (*wireless LAN*).Họ lo ngại về bảo mật trong WEP (*Wired Equivalent Privacy*), và quan tâm tới những giải pháp bảo mật mới thay thế an toàn hơn.

IEEE và Wi-Fi Alliance đã phát triển một giải pháp bảo mật hơn là: Bảo vệ truy cập Wi-Fi WPA (*Wi-Fi Protected Access*) và IEEE 802.11i (cũng được gọi là "WPA2 Certified" theo Wi-Fi Alliance) và một giải pháp khác mang tên VPN Fix cũng giúp tăng cường bảo mật mạng không dây.

Theo như Webtorial, WPA và 802.11i được sử dụng tương ứng là 29% và 22%.Mặt khác, 42% được sử dụng cho các "giải pháp tình thế" khác như: bảo mật hệ thống mạng riêng ảo VPN (*Vitual Private Network*) qua mạng cục bộ không dây.

Vậy, chúng ta nên lựa chọn giải pháp bảo mật nào cho mạng không dây?

WEP: Bảo mật quá tồi

WEP (Wired Equivalent Privacy) có nghĩa là bảo mật không dây tương đương với có dây. Thực ra, WEP đã đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn.WEP sử dụng một khoá mã hoá không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit) được sử dụng để xác thực các thiết bị được phép truy cập vào trong mạng, và cũng được sử dụng để mã hoá truyền dữ liệu.

Rất đơn giản, các khoá mã hoá này dễ dàng bị "bẻ gãy" bởi thuật toán brute-force và kiểu tấn công thử lỗi (*trial-and-error*). Các phần mềm miễn phí như Airsnort hoặc WEPCrack sẽ cho phép hacker có thể phá vỡ khoá mã hoá nếu họ thu thập đủ từ 5 đến 10 triệu gói tin trên một mạng không dây. Với những khoá mã hoá 128 bit cũng không khá hơn: 24 bit cho khởi tạo mã hoá nên chỉ có 104 bit được sử dụng để mã hoá, và cách thức cũng giống như mã hoá có độ dài 64 bit nên mã hoá 128 bit cũng dễ dàng bị bẻ khoá.Ngoài ra, những điểm yếu trong những vector khởi tạo khoá mã hoá giúp cho hacker có thể tìm ra mật khẩu nhanh hơn với ít gói thông tin hơn rất nhiều.

Không dự đoán được những lỗi trong khoá mã hoá, WEP có thể được tạo ra cách bảo mật mạnh mẽ hơn nếu sử dụng một giao thức xác thực mà cung cấp mỗi khoá mã hoá mới cho mỗi phiên làm việc. Khoá mã hoá sẽ thay đổi trên mỗi phiên làm việc.Điều này sẽ gây khó khăn hơn cho hacker thu thập đủ các gói dữ liệu cần thiết để có thể bẽ gãy khoá bảo mật.

Giải pháp tình thế: VPN (Vitual Private Network) Fix:

Nhận ra sự yếu kém của WEP, những người sử dụng doanh nghiệp đã khám phá ra một cách hiệu quả để bảo vệ mạng không dây WLAN của mình, được gọi là VPN Fix.Ý tưởng cơ bản của phương pháp này là coi những người sử dụng WLAN như những người sử dụng dịch vụ truy cập từ xa.

Trong cách cấu hình này, tất các những điểm truy cập WLAN, và cũng như các máy tính được kết nối vào các điểm truy cập này, đều được định nghĩa trong một mạng LAN ảo (*Vitual LAN*).Trong cơ sở hạ tầng bảo mật, các thiết bị này được đối xử như là "không tin tưởng".Trước khi bất cứ các thiết bị WLAN được kết nối, chúng sẽ phải được sự cho phép từ thành phần bảo mật của mạng LAN.Dữ liệu cũng như kết nối của các thiết bị sẽ phải chạy qua một máy chủ xác thực như RADIUS chẳng hạn...Tiếp đó, kết nối sẽ được thiết lập thành một tuyến kết nối bảo mật đã được mã hoá bởi một giao thức bảo mật ví dụ như IPSec, giống như khi sử dụng các dịch vụ truy cập từ xa qua Internet. Tuy nhiên, giải pháp này cũng không phải là hoàn hảo, VPN Fix cần lưu lượng VPN lớn hơn cho tường lửa, và cần phải tạo các thủ tục khởi tạo cho từng người sử dụng. Hơn nữa, IPSec lại không hỗ những thiết bị có nhiều chức năng riêng như thiết bị cầm tay, máy quét mã vạch... Cuối cùng, về quan điểm kiến trúc mạng, cấu hình theo VPN chỉ là một giải pháp tình thế chứ không phải là sự kết hợp với WLAN.

Giải pháp bảo mật bằng xác thực

Một sự thật là khi đã khám phá ra những lỗi về bảo mật trong mạng LAN không dây, ngành công nghiệp đã phải tốn rất nhiều công sức để giải quyết bài toán này.Một điều cần ghi nhớ là chúng ta cần phải đối diện với 2 vấn đề: xác thực và bảo mật thông tin. Xác thực nhằm đảm bảo chắc chắn người sử dụng hợp pháp có thể truy cập vào mạng. Bảo mật giữ cho truyền dữ liệu an toàn và không bị lấy trộm trên đường truyền.

Một trong những ưu điểm của xác thực là IEEE 802.1x sử dụng giao thức xác thực mở rộng EAP (*Extensible Authentication Protocol*).EAP thực sự là một cơ sở tốt cho xác thực, và có thể được sử dụng với một vài các giao thức xác thực khác.Những giao thức đó bao gồm **MD5, Transport Layer Security (TLS), Tunneled TLS (TTLS), Protected EAP (PEAP)** và **Cisco's Lightweight EAP (LEAP)**.

Thật may mắn, sự lựa chọn giao thức xác thực chỉ cần vài yếu tố cơ bản.Trước hết, một cơ chế chỉ cần cung cấp một hoặc 2 cách xác thực, có thể gọi là sự xác thực qua lại (*mutual authentication*), có nghĩa là mạng sẽ xác thực người sử dụng và người sử dụng cũng sẽ xác thực lại mạng.Điều này rất quan trọng với mạng WLAN, bởi hacker có thể thêm điểm truy cập trái phép nào đó vào giữa các thiết bị mạng và các điểm truy cập hợp pháp (kiểu tấn công *man-in-the-middle)*, để chặn và thay đổi các gói tin trên đường truyền dữ liệu.Và phương thức mã hoá MD5 không cung cấp xác thực qua lại nên cũng không được khuyến khích sử dụng WLAN.

Chuẩn mã hoá 802.11i hay WPA2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance.Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES (*Advanced Encryption Standard*).AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit.

Để đánh giá chuẩn mã hoá này,Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mĩ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã đối xứng này.Và chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mĩ để bảo vệ các thông tin nhạy cảm.

Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard).Để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip.Tuy nhiên, rất ít card mạng WLAN hoặc các điểm truy cập có hỗ trợ mã hoá bằng phần cứng tại thời điểm hiện tại. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

WPA (Wi-Fi Protected Access)

Nhận thấy được những khó khăn khi nâng cấp lên 802.11i, Wi-Fi Alliance đã đưa ra giải pháp khác gọi là Wi-Fi Protected Access (WPA).Một trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP (*Temporal Key Integrity Protocol*).WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit.Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin.Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu.Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check).Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền.

Một trong những điểm hấp dẫn nhất của WPA là không yêu cầu nâng cấp phần cứng.Các nâng cấp miễn phí về phần mềm cho hầu hết các card mạng và điểm truy cập sử dụng WPA rất dễ dàng và có sẵn.Tuy nhiên, WPA cũng không hỗ trợ các thiết bị cầm tay và máy quét mã vạch. Theo Wi-Fi Alliance, có khoảng 200 thiết bị đã được cấp chứng nhận tương thích WPA.

WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise.Cả 2 lựa chọn này đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu.WPA Personal thích hợp cho gia đình và

mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm.Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.
Trong khi Wi-Fi Alliance đã đưa ra WPA, và được coi là loại trừ mọi lỗ hổng dễ bị tấn công của WEP, nhưng người sử dụng vẫn không thực sự tin tưởng vào WPA.Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal.Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu.Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán (đừng sử dụng những từ như "PASSWORD" để làm mật khẩu).
Điều này cũng có nghĩa rằng kĩ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất.WPA chỉ thích hợp với những công ty mà không không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm...WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

❖ **Kết luận:**

Trong khi sử dụng VPN Fix qua các kết nối WLAN có thể là một ý tưởng hay và cũng sẽ là một hướng đi đúng.Nhưng sự không thuận tiện cũng như giá cả và tăng lưu lượng mạng cũng là rào cản cần vượt qua.Sự chuyển đổi sang 802.11i và mã hoá AES đem lại khả năng bảo mật cao nhất.Nhưng các tổ chức, cơ quan vẫn đang sử dụng hàng nghìn những card mạng WLAN không hỗ trợ chuẩn này.Hơn nữa AES không hỗ các thiết bị cầm tay và máy quét mã vạch hoặc các thiết bị khác...Đó là những giới hạn khi lựa chọn 802.11i.
Sự chuyển hướng sang WPA vẫn còn là những thử thách.Mặc dù, vẫn còn những lỗ hổng về bảo mật và có thể những lỗ hổng mới sẽ được phát hiện.Nhưng tại thời điểm này, WPA là lựa chọn tốt.
Chắc hẳn những ai làm việc trong môi trường công nghệ thông tin đều ít nhiều có nghe đến các giải pháp truyền thông mạng bằng công nghệ VPN thông qua mạng Internet giúp các hệ thống mạng nội bộ vẫn có thể liên kết với nhau hay các người dùng ở xa, thường xuyên di chuyển ra khỏi văn phòng của mình vẫn có thể truy cập tài nguyên hệ thống mạng để làm việc như đang ở chính văn phòng của mình bất chấp khoảng cách địa lý, không kể không gian, thời gian mà chỉ cần có sẵn đường kết nối Internet.
Các kỹ thuật sử dụng trong VPN
Do đặc điểm của kỹ thuật tunneling là truyền các gói dữ liệu trong các "đường hầm" do các kết nối đầu cuối tạo ra nên ta phải chú ý việc thiết lập các cơ chế bảo mật, đảm bảo an toàn dữ liệu trên đường truyền (IPSec, PPTP, L2TP, L2TP/IPSec). Các kỹ thuật và tiêu chuẩn được sử dụng trong VPN nhằm mục đích đảm bảo cho sự lưu thông của các dữ liệu nhạy cảm trở nên an toàn hơn khi truyền qua môi trường Internet không được bảo mật, điển hình là các kỹ thuật như:
• **Encryption:** là quá trình mã hóa dữ liệu, chỉ có thể giải mã bởi các hệ thống được chỉ định trước đó, nghĩa là hệ thống nhận phải có khóa mã hóa mới có thể giải mã được các dữ liệu này. Có hai hệ thống khóa mã hóa:
+ **Hệ thống khóa mã hóa bí mật (secret-key)**: thiết bị gửi và thiết bị nhận cùng sử dụng chung một khóa để mã hóa và giải mã dữ liệu.
+ **Hệ thống khóa mã hóa dùng chung (public key)**: sử dụng đến hai khóa, một trong hai khóa được công khai để bất cứ ai cũng có thể sử dụng. Tên của public key do một người dùng quản lý, các người dùng khác sẽ sử dụng public key này để giao tiếp với người dùng quản lý public key đó.Tương ứng với public key sẽ có thêm một private key khác nữa của riêng người dùng tạo ra private key này.Lúc này mọi người đều có thể sử dụng public key để mã hóa dữ liệu, nhưng chỉ những ai có private key mới có thể giải mã các dữ liệu đó mà thôi.Hai hệ thống mã hóa thông dụng nhất hiện nay là PGP (Pretty Good Privacy) và DES (Data Encryption Standard).
• **Authentication**: cơ chế kiểm tra để chắc chắn rằng dữ liệu đã được truyền đến đúng người nhận muốn gửi, cũng như đảm bảo cho các dữ liệu đã được truyền một cách chính xác và toàn vẹn.
• **Authorization:** từ chối hoặc cho phép truy cập vào các tài nguyên mạng sau khi người dùng đã được nhận dạng và xác thực thành công.
Các giao thức chính sử dụng trong VPN
Có 4 giao thức phổ biến với tính bảo mật cao được sử dụng trong VPN bao gồm:
• **IPSec (IP Security)**: là một tiêu chuẩn được phát triển bởi IETF nhằm đảm bảo an toàn trong quá trình truyền dẫn và xác thực người dùng truy cập qua mạng công cộng. Không giống như các kỹ thuật mã hóa khác, IPSec hoạt động ở tầng Network trong mô hình OSI, vì thế việc triển khai IPSec không bị lệ thuộc vào các ứng dụng trong toàn mạng.

• **PPTP (Point-to-Point Tunneling Protocol)**: do Microsoft, 3COM, và Ascend Communications phát triển, hoạt động ở tầng Data link thấp hơn để bổ sung và thay thế cho IPSec.
• **L2TP (Layer 2 Tunneling Protocol)**: giao thức này kết hợp giữa 2 giao thức L2F (Layer 2 Forwarding) và PPTP (Point to Point Tunneling Protocol) do Cisco nghiên cứu để thay thế cho IPSec.L2TP được dùng để gói các frame PPP (Point-to-Point Protocol) để gửi qua các mạng X25, FR, và ATM
• **SSL (Secure Sockets Layer)**: là giao thức đa mục đích được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (socket 443) nhằm mã hóa toàn bộ thông tin đi/đến, mà ngày nay được sử dụng rộng rãi cho giao dịch điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân (PIN) trên Internet.Sắp tới có thể SSL là một lựa chọn tối ưu cho các tuyến kết nối VPN.Mặc dù vậy, IPSec vẫn là giao thức VPN được sử dụng nhiều nhất hiện nay.

Ưu / Nhược điểm của VPN

Sự ra đời của VPN đã đánh dấu một bước phát triển mới của công nghệ mạng máy tính nhờ áp dụng những kỹ thuật và giao thức tối ưu tạo ra những lợi ích mà không ai có thể phủ nhận được như: • Giảm bớt chi phí triển khai: giá thành đầu tư cho VPN thấp hơn rất nhiều so với các giải pháp truyền thông mạng khác vì VPN không nhất thiết phải sử dụng các đường truyền trực tiếp như các giải pháp Frame Relay, ATM, hay ISDN.Thay vào đó là các hạ tầng mạng sẵn có của các ISP để truyền thông.
• **Giảm bớt chi phí triển khai**: giá thành đầu tư cho VPN thấp hơn rất nhiều so với các giải pháp truyền thông mạng khác vì VPN không nhất thiết phải sử dụng các đường truyền trực tiếp như các giải pháp Frame Relay, ATM, hay ISDN.Thay vào đó là các hạ tầng mạng sẵn có của các ISP để truyền thông.
• **Giảm chi phí nhân viên và quản lý**: do giảm được các kênh truyền đường dài nên chi phí điều hành các mạng WAN sẽ giảm đáng kể. Nghĩa là bạn sẽ không còn phải đầu tư chi phí và nhân lực cho việc điều hành, quản lý, đào tạo nhân lực quản trị các hệ thống mạng dựa trên các kênh truyền riêng nữa khi sử dụng VPN vì tất cả đều được ISP quản lý và kiểm soát.
• **Tăng cường khả năng kết nối**: bạn có thể yên tâm kết nối vào các mạng nội bộ ở cách xa hàng ngàn km để làm việc khi có sẵn một đường truyền Internet.
• **Giao dịch an toàn**: VPN sử dụng giao thức tunneling để truyền dữ liệu trên các mạng với các công nghệ tiên tiến như mã hóa dữ liệu, xác thực người dùng, quản lý quyền truy cập, v.v… đảm bảo độ an toàn bảo mật tối đa và giảm thiểu các lỗi truyền xuống mức tối thiểu.
• **Tận dụng hiệu quả băng thông đường truyền**: các doanh nghiệp, tổ chức thường sử dụng các đường truyền leased line với băng thông lớn nhưng lại không sử dụng hết băng thông gây ra tình trạng lãng phí. Nếu sử dụng VPN chung với các ứng dụng Internet, bạn vừa tiết kiệm được chi phí thuê các kênh truyền khác cho VPN, vừa tận dụng triệt để lượng băng thông dư thừa đó vào các ứng dụng hữu ích như: VoIP, Video conference…
Tuy nhiên, bên cạnh đó VPN cũng còn tồn tại một vài khuyết điểm khiến người dùng phải cân nhắc trước khi sử dụng như
• **Bị lệ thuộc vào đường truyền Internet**: nếu băng thông và sự ổn định của đường truyền Internet không tốt sẽ ảnh hưởng rất lớn đến giao tiếp VPN (với các kết nối VPN sử dụng Internet làm đường truyền chính).
• **Thiếu đồng bộ về giao thức**: mặc dù dựa trên công nghệ IP rộng khắp toàn cầu nhưng các giao thức hỗ trợ cho VPN còn chưa thống nhất, mỗi nơi sử dụng giao thức và thiết bị hỗ trợ VPN khác nhau nên khả năng tương thích giữa các mạng còn thấp.Các chuyên gia mạng vẫn có thể giải quyết được vấn đề này nhưng sẽ gây nhiều khó khăn và làm giảm hiệu năng của toàn mạng khi sử dụng các giải pháp non-IP.

Những yếu tố cần cân nhắc khi sử dụng VPN

Trước khi quyết định chọn và đầu tư giải pháp VPN để thực hiện các phiên kết nối từ xa cho hệ thống mạng của mình, bạn cần phải cân nhắc kỹ một số yếu tố sau đây:
• **Yếu tố bảo mật**: do dữ liệu được trung chuyển qua các mạng công cộng rất hỗn loạn và mất an toàn trong khi tính bảo mật đóng vai trò sống còn đối với các dữ liệu nhạy cảm của các tổ chức và doanh nghiệp.Ngoài ra còn phải đảm bảo cho các dữ liệu truyền-nhận được chính xác, không bị mất hoặc sai sót, và dữ liệu phải được mã hóa trước khi truyền ra môi trường bên ngoài.Khi quyết định triển khai VPN trong các hệ thống mạng lớn thì phải chọn các giải pháp tương thích với các giải pháp bảo mật dữ liệu như firewall, proxy, v.v…
• **Kiểm tra tính tương thích và chất lượng của các thiết bị**: nếu không kiểm tra khả năng tương thích và chất lượng của các thiết bị trong hệ thống mạng VPN trước khi triển khai thì sẽ rất khó đảm bảo được chất lượng dịch vụ cho toàn hệ thống khi đưa vào sử dụng, đặc biệt là khi sử dụng các thiết bị từ nhiều hãng sản xuất khác nhau.Vì vậy, các thiết bị này cần phải được đầu tư trang bị từ một

hãng sản xuất duy nhất để đồng bộ và đạt được hiệu năng cao nhất, cũng như cần phải được thử nghiệm ở các khoảng cách càng xa càng tốt trước khi đưa vào triển khai.
• **Khả năng quản lý tập trung**: hệ thống mạng cần phải được cấu hình, quản lý tập trung thông qua một ứng dụng cụ thể duy nhất để hệ thống kiểm soát có thể lưu lại các file log giám sát giúp cho việc theo dõi, quản lý và khắc phục sự cố dễ dàng hơn trước khi toàn bộ hệ thống bị sụp đổ hoàn toàn, gây ảnh hưởng nghiêm trọng đến công việc.
• **Tính dễ triển khai**: giải pháp VPN phải dễ triển khai và cấu hình, khi triển khai các hệ thống mạng VPN mở diện rộng thì cần phải chắc chắn rằng ứng dụng quản lý phải có khả năng theo dõi và lưu lại mọi hoạt động của mọi kênh tunnel trên toàn hệ thống.
• **Tính dễ sử dụng**: các phần mềm máy chủ và client sử dụng cho mạng VPN phải dễ sử dụng và không quá phức tạp, đặc biệt là các ứng dụng client để người dùng đầu cuối dễ dàng triển khai và sử dụng.
• **Khả năng mở rộng**: không chỉ đáp ứng nhu cầu sử dụng hiện tại mà hệ thống mạng VPN còn phải có khả năng mở rộng phục vụ cho các nhu cầu nâng cao của tương lai. Và các thành phần, thiết bị bổ sung phải liền lạc cũng như giảm thiểu tối đa sự thay đổi các thiết bị có sẵn.
• **Hiệu suất hoạt động của hệ thống mạng**: cần phải lựa chọn các thiết bị thật chính xác sao cho vừa hoạt động liền lạc với nhau, vừa có khả năng xử lý tốt mọi tác vụ xử lý một cách nhanh chóng và hiệu quả, đặc biệt là tiến trình mã hóa dữ liệu.Nếu sử dụng các thiết bị có hiệu năng xử lý kém sẽ làm hiệu năng hoạt động của toàn hệ thống mạng giảm sút nghiêm trọng và mất ổn định.
• **Quản lý băng thông**: để đạt được hiệu năng hoạt động, luôn luôn sẵn sàng với chất lượng cao nhất thì bắt buộc bạn phải quản lý băng thông đường truyền của toàn hệ thống sao cho hiệu quả nhất, kể cả băng thông dành cho các người dùng, nhóm làm việc, các ứng dụng đòi hỏi giao tiếp mạng với các chính sách ưu tiên hợp lý.
• **Chọn ISP để truyền thông**: chọn lựa ISP cũng là một yếu tố rất quan trọng ảnh hưởng rất lớn đến hiệu suất của mạng VPN, ISP được chọn phải thực sự ổn định và có thể hỗ trợ cho người dùng VPN bất cứ lúc nào.

Các kiểu mạng VPN

VPN được nghiên cứu và phát triển nhằm mục đích giúp người dùng từ xa và người dùng của các mạng trong cùng một đơn vị ở các vị trí địa lý khác nhau đều có thể truy cập vào các nguồn tài nguyên nội bộ thống nhất, tập trung.Đồng thời có thể kiểm soát truy cập các tài nguyên mạng của khách hàng, nhân viên hỗ trợ, và các đối tác kinh doanh một cách chặt chẽ để đảm bảo an toàn cho hệ thống mạng. Xuất phát từ các nhu cầu này, VPN đã được phát triển và chia loại ra làm 3 kiểu mạng chính sau đây:

Remote Access VPN

Kiểu mạng này thường dành cho nhóm người có nhu cầu làm việc từ xa, nhân viên kinh doanh hay di chuyển ra khỏi văn phòng làm việc của mình vẫn có thể truy cập vào các nguồn tài nguyên chung trong mạng. Đơn giản bạn chỉ cần có sẵn một đường Internet là có thể kết nối về hệ thống mạng chính của mình (có thể dùng modem quay số hay tại các điểm truy cập Internet công cộng).

Intranet VPNs

Đây là kiểu mạng VPN dùng để liên kết các chi nhánh văn phòng ở nhiều nơi khác nhau vào cùng một hệ thống mạng Intranet nội bộ.Nếu không áp dụng công nghệ VPN thì bắt buộc các chi nhánh phải thiết lập các kênh kết nối đường trục trực tiếp vào mạng Intranet bằng các Backbone router như là một Backbone WAN mà chi phí đầu tư rất cao, khó triển khai và khó mở rộng về sau.Trong trường hợp này, giải pháp Intranet VPN sẽ tiết kiệm được rất nhiều chi phí đầu tư khi áp dụng giải pháp Backbone WAN và làm giảm bớt tổng giá thành đầu tư cho toàn bộ hệ thống mạng Intranet xuống nhiều lần và còn rất nhiều ưu điểm khác so với Backbone WAN:

Cấu hình Intranet dạng Backbone WAN

• Sẽ không còn phải lo lắng với khoản chi phí đầu tư rất lớn để trang bị các Backbone router cho các thiết bị đầu và cuối trong mạng Backbone WAN khi triển khai Intranet VPN.
• Giảm bớt chi phí và số lượng nhân viên hỗ trợ kỹ thuật cho các mạng chi nhánh ở xa so với Backbone WAN.
• Cung cấp các kênh kết nối dạng Pear-to-Pear dễ dàng hơn nhờ sử dụng Internet làm môi trường giao tiếp.
• Có thể triển khai các biện pháp dự phòng tốt nhất khi sử dụng các VPN tunnel kết hợp với công nghệ chuyển mạch tốc độ cao như FR.

Cấu hình mạng Extranet VPN

Extranet VPNE

Extranet VPN không hoàn toàn cách ly với "thế giới bên ngoài" như Remote Access VPN và Intranet VPN, mà mở rộng hơn và có thể cho phép các nhóm người dùng bên ngoài như các đối tác, khách hàng, nhân viên có liên quan truy cập vào các nguồn tài nguyên mạng.
Nếu áp dụng các giải pháp Extranet VPN, việc thiết lập các mạng Extranet trở nên dễ dàng hơn rất nhiều và mang lại cho bạn nhiều lợi nhuận hơn với rất nhiều ưu điểm như: giá thành đầu tư rất thấp so với mạng truyền thống; dễ dàng triển khai, duy trì cũng như sửa đổi, bổ sung về sau; có nhiều lựa chọn để tìm được nhà cung cấp dịch vụ phù hợp với nhu cầu sử dụng của từng tổ chức, doanh nghiệp do sự phát triển mạnh mẽ của Internet; giảm bớt chi phí đào tạo và thuê các chuyên viên quản lý do một phần hạ tầng hệ thống mạng Extranet VPN (đường truyền Internet) do các ISP quản lý, nhờ đó làm giảm bớt chi phí vận hành hệ thống mạng.
Qua các thông tin trên chúng ta có thể nhận thấy những lợi ích thiết thực mà giải pháp VPN mang lại cho DN khi triển khai, tích hợp chúng vào hạ tầng mạng của mình. Và tôi sẽ giới thiệu sâu hơn về các giao thức mạng VPN và hướng dẫn các bước đơn giản nhất để thiết lập một hệ thống mạng VPN trên cả server lẫn client trong bài viết tiếp theo của số báo tới, các bạn nhớ đón đọc nhé.

- **ỨNG DỤNG VPN TRONG CÁC TRƯỜNG HỌC**

Nhiệm vụ cấp bách đặt ra hiện nay cho các nhà quản trị mạng của các trường học là làm sao có thể thiết lập được một hệ thống bảo mật an toàn cho hệ thống thông tin của trường học.Hệ thống bảo mật này vừa phải đảm bảo tính riêng tư ngăn chặn mọi thâm nhập phá hoại trái phép từ bên ngoài, vừa phải đảm bảo việc kết nối và khai thác thông tin trên mạng Internet được thông suốt.Sau đây là những giải pháp hiện đang được ứng dụng rất phổ biến trong các mạng Intranet của các công ty đa quốc gia như: Siemens, Ericsson... đó là công nghệ mạng riêng ảo (VPN).
Hiện nay các trường (Đại học, Cao đẳng, Trung cấp…) ở Việt Nam đã và đang tiến hành xây dựng hệ thống mạng Intranet riêng để phục vụ cho việc nghiên cứu và học tập của giáo viên, sinh viên, học sinh.Hầu hết các mạng này đều được kết nối với mạng Internet, các kết nối này được dùng để trao đổi thông tin nội bộ cũng như với các trường học khác và giúp cho giáo viên, sinh viên có điều kiện tiếp cận và khai thác nguồn tài nguyên khoa học phong phú trên Internet.Internet mang lại các lợi ích không thể phủ nhận đối với công việc học tập và nghiên cứu, tuy nhiên nó cũng còn có điểm bất lợi không thể tránh khỏi.Cụ thể đó là các kẽ hở mà những kẻ phá hoại lợi dụng để đánh cắp thông tin, phá hoại mạng nội bộ của các trường. Đây là một thách thức đối với các cán bộ quản trị mạng tại các trường.Đặc biệt là trong thời gian gần đây khi các Hacker thường xuyên thâm nhập phá hoại đánh cắp thông tin và tung ra nhiều loại virus nguy hiểm làm tê liệt hệ thống mạng.

- **Các kỹ thuật sử dụng trong VPN**
  - **Tường lửa**

Tường lửa là một hệ thống nằm giữa mạng nội bộ và mạng công cộng nhằm kiểm soát tất cả các gói tin đi qua bộ định tuyến cổng và do đó nó được xem như một hệ thống lọc gói.

  - **Mã hóa và xác thực**

Ngoài kỹ thuật bức tường lửa thì mã hóa và xác thực cũng là một trong những kỹ thuật quan trọng được sử dụng trong VPN.

  - **Mật mã trong truyền thông mạng**

Vấn đề "truyền dữ liệu qua những kênh không an toàn" được giải quyết bằng cách: phải đảm bảo tính riêng tư của kênh truyền.Đối với VPN không cần bất cứ sự thay đổi nào trong hệ thống giao nhận trên mạng, dữ liệu vẫn được truyền qua các kênh thông tin không an toàn nhưng ở dạng mã hóa để cho những người mà có khoá giải mã mới có thể nhận được.

- **Mã hóa và xác thực trong VPN:**

Tất cả các kết nối an toàn nhất thiết phải bảo đảm được 3 chức năng sau:
- Khả năng mã hóa dữ liệu.
- Khả năng xác thực.
- Khả năng bảo đảm tính toàn vẹn dữ liệu.

Đây cũng chính là các chức năng cơ bản nhất của một mạng VPN.

Các giao thức VPN

+ IPSec

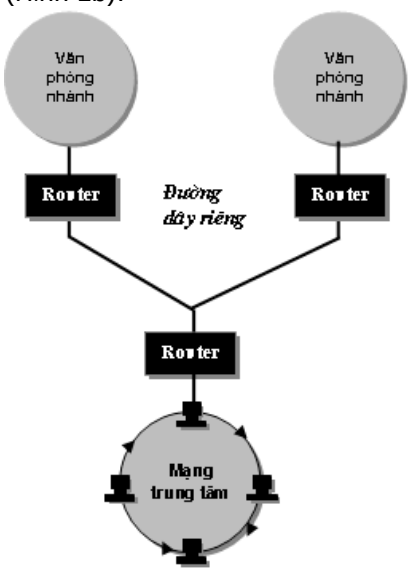
IPSec là khung của chuẩn mở nhằm đảm bảo các kết nối an toàn qua mạng IP với khả năng mã hóa và xác thực ở lớp mạng. Nó được sử dụng để bảo vệ một hoặc nhiều đường kết nối giữa các cặp trạm chủ (host) hoặc các cặp cổng an ninh (router, firewall).IPSec sử dụng hai giao thức: AH và ESP để cung cấp tính bảo mật cho dữ liệu, các giao thức này có thể sử dụng độc lập hoặc thực hiện kết hợp với nhau để tạo ra các dịch vụ an ninh ở cả IPv4 và IPv6.Mỗi giao thức đều hỗ trợ hai chế độ: truyền tải và đường hầm (transport và tunnel).

+ Radius:

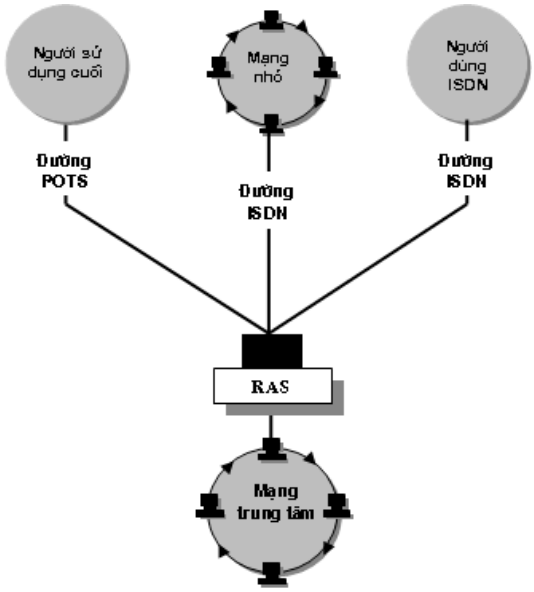
Những nét đặc trưng của Radius:
Cấu trúc Client/server: Network Access Server (NAS) hoạt động như một client của Radius server.Radius server có trách nhiệm nhận các yêu cầu kết nối của người dùng thông qua NAS, xác thực người dùng và gửi trả lại các thông tin cấu hình cho client để chuyển tới người dùng.
An ninh mạng (Network Security): Các giao dịch được xác thực thông qua việc sử dụng chung một khóa (secret) mà khóa này không bao giờ được gửi qua mạng.
Cơ chế xác thực mềm dẻo: Radius server có thể xác thực một loạt các phương pháp xác thực người dùng khác nhau chẳng hạn như: CHAP, Unix login…
+ **CHAP (Challenge-Handshake Authentication Protocol)**
Thông thường thì quá trình xác thực là không bắt buộc, nếu các bên kết nối muốn xác thực thì thông tin về quá trình này phải được xác định trong giai đoạn thiết lập kết nối. Các quá trình diễn ra như sau:
- Sau khi kết nối vật lý được thiết lập một bên sẽ gửi "Challenge message" cho bên kia.
- Bên nhận được "Challenge message" sẽ xác thực bằng một giá trị có được qua thuật toán băm một chiều với đầu vào là các thông tin được cung cấp trong "Challenge message"
- Bên yêu cầu xác thực sẽ kiểm tra lại giá trị nhận được đó với giá trị mà nó tính toán được.Nếu phù hợp thì kết nối được thiết lập, nếu không thì kết nối bị hủy bỏ .
- Sau một khoảng thời gian nào đó các bước trên có thể được tiến hành lại và xác thực có thể tiến hành trên cả 2 chiều của kết nối.

- **Mạng WAN, dịch vụ truy nhập từ xa (RAS) và VPN**

Một mạng diện rộng WAN (Wide Area Network) gồm 2 mạng hoặc nhiều hơn kết nối với nhau qua các kênh thuê riêng (leased line). WAN có thành phần cơ bản như sau: mạng, bộ định tuyến cổng, đường dây điện thoại (Hình 1a).
Dịch vụ truy nhập từ xa (RAS: Remote Access Services) sử dụng RAS server cho phép người dùng từ xa thông qua server này truy nhập vào mạng trung tâm như một người sử dụng trong mạng (Hình 1b).

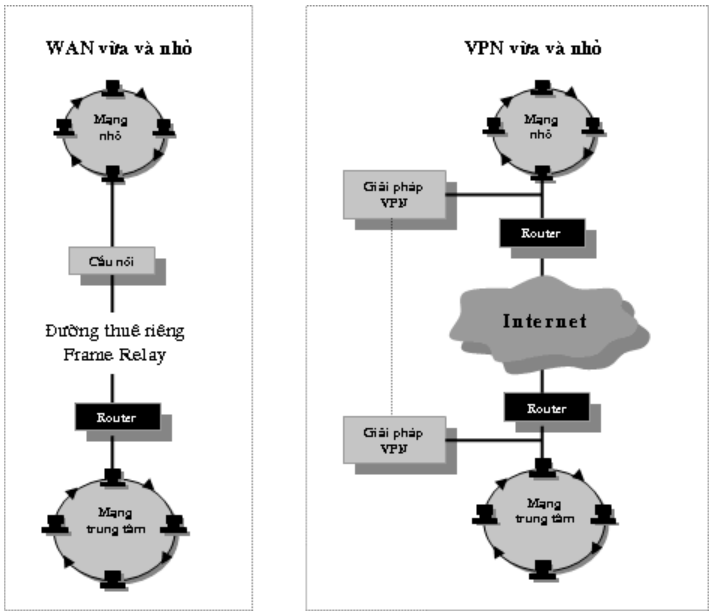


Hình 1a: WAN



Hình 1b: RAS

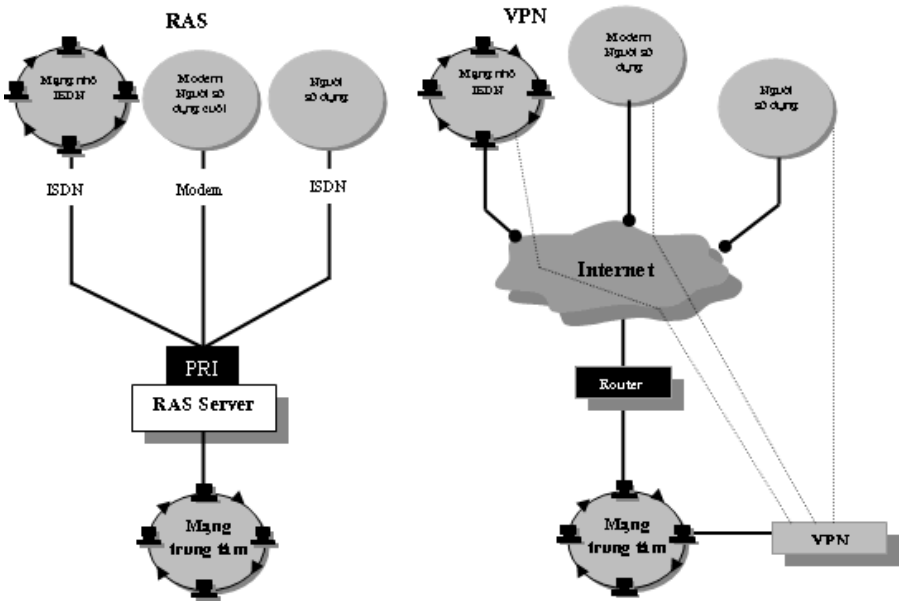
Mối quan hệ giữa VPN và WAN
Giải pháp cho mạng vừa và nhỏ:



Hình 2. VPN & WAN cho mạng vừa và nhỏ

Mối quan hệ giữa VPN và RAS

Giải pháp cho mạng vừa và nhỏ:



Hình 3. VPN & RAS cho mạng vừa và nhỏ

- **Giải pháp xây dựng một ứng dụng thực tế**
  - **Altavista Tunnel 98**

Altavista Tunnel là một sản phẩm của Digital Equipment Corporation (nay là Compaq) hỗ trợ thiết lập các kết nối đường ngầm.

Altavista Tunnel 98 có 2 version: Extranet Server và Telecommuter Client. Extranet Server quản lý các kết nối ở trong mạng LAN (hoặc WAN) còn Telecommuter Client được sử dụng để thiết lập và quản lý kết nối tới Extranet Server.Extranet Server cũng có thể hoạt động như một client và khi đó nó cho phép 2 mạng LAN kết nối với nhau.Server lưu trữ các thông tin về người dùng như: User name, password và các thông tin khác dùng để xác thực.Các cơ cấu để đảm bảo an toàn dữ liệu được sử dụng thông qua xác thực người dùng và mã hóa luồng dữ liệu.

- **Các ưu điểm của Altavista Tunnel**

Trong khi các giải pháp VPN khác sử dụng các địa chỉ IP cố định được cấu hình trước trên máy ở cả 2 phía để cung cấp các kết nối an toàn thì Altavista Tunnel thực hiện bằng một cách khác.Altavista Tunnel cho phép người dùng đăng nhập từ nhiều khu vực khác nhau và sử dụng các địa chỉ IP khác nhau.Khả năng này cho phép người dùng di chuyển từ khu vực này sang khu vực khác mà vẫn duy trì được kết nối vào mạng LAN.

Altavista Tunnel sử dụng thuật toán RSA 1024 bit mã công khai (puclic key) để xác thực. Sau khi người dùng đã được xác thực Altavista Tunnel sử dụng RSA RC4 để mã hóa gói tin.Thuật toán MD5 được sử dụng để đảm bảo tính toàn vẹn của các gói tin.Các khóa được sử dụng trong kết nối được thay đổi sau từ 30 đến 1440 phút (tùy thuộc cấu hình được thiết lập trên server), quá trình này được thực hiện tự động và không ảnh hưởng tới các hoạt động của người dùng.

- **Cơ chế làm việc của Altavista Tunnel**

Mạng Altavista Tunnel bao gồm 2 phía: người dùng ở xa (remote user hoặc remote LAN/WAN) và mạng nội bộ (có một số host và Altavista Tunnel server) và cả hai phía đều có khả năng kết nối Internet.

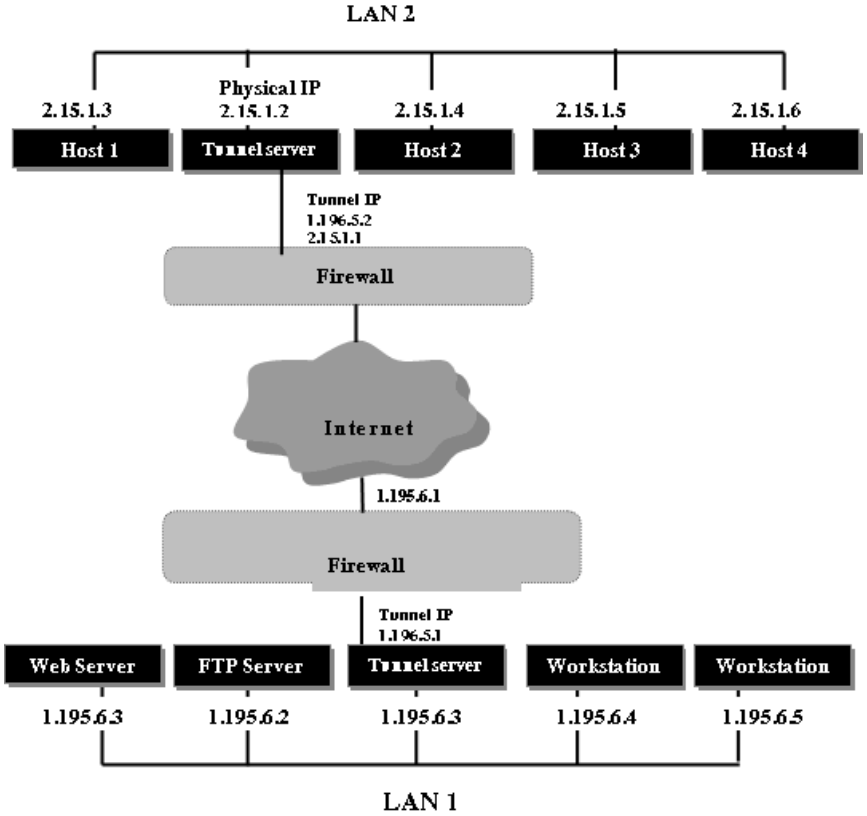
Tunnel và Host trên mạng LAN có các địa chỉ IP vật lý và ngoài ra trên Tunnel Server còn có một dải địa chỉ IP ảo sẵn sàng để gán cho các kết nối đường ngầm.Mỗi kết nối được nhận 2 địa chỉ IP ảo, một cho phía client và một cho phía server.

Các luồng dữ liệu tới mạng riêng ảo đầu tiên được định tuyến bằng phần mềm trên client: **Từ địa chỉ vật lý của client → địa chỉ ảo của nó → địa chỉ IP ảo của tunnel server**.

Tại Tunnel Server các gói tin lại được định tuyến tới các host trong mạng riêng.Theo cách này thì client hoạt động như là một node trong mạng LAN.

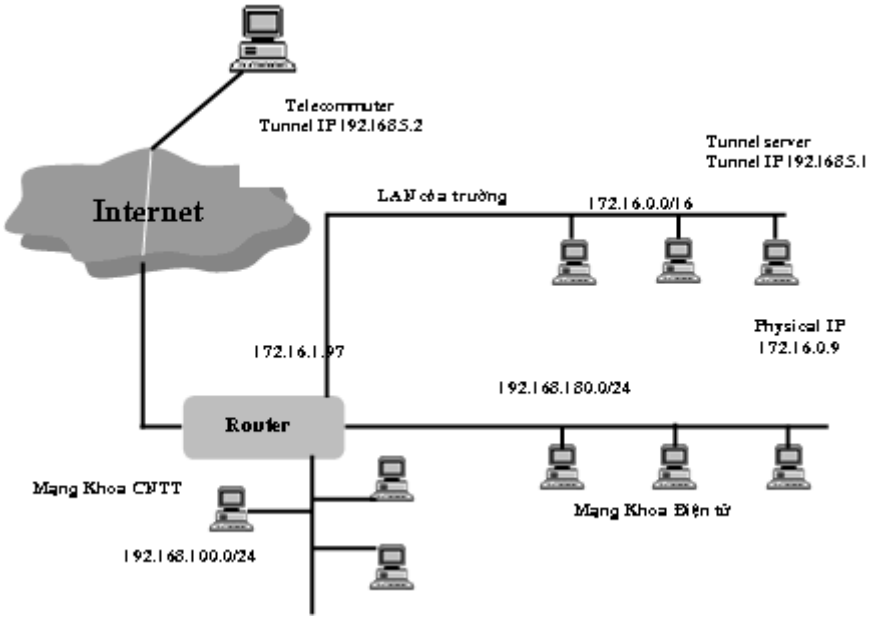
Khi remote user khởi động một phiên kết nối với tunnel server thì yêu cầu kết nối đã mã hóa được gửi đi.Yêu cầu này được xác thực trên tunnel server qua các thông tin về người dùng được lưu ở đây.Nếu yêu cầu được chấp nhận thì server sẽ gửi một đáp ứng đã mã hóa cho client rồi 2 bên trao đổi các khóa để tiến hành thiết lập kết nối.

Các phần mềm Altavista Tunnel 98 ở cả hai phía đề được cài đặt như các giao thức mạng riêng biệt do đó nó không làm ảnh hưởng tới các kết nối khác.Người dùng có thể cùng lúc thiết lập nhiều kết nối đường ngầm khác nhau.



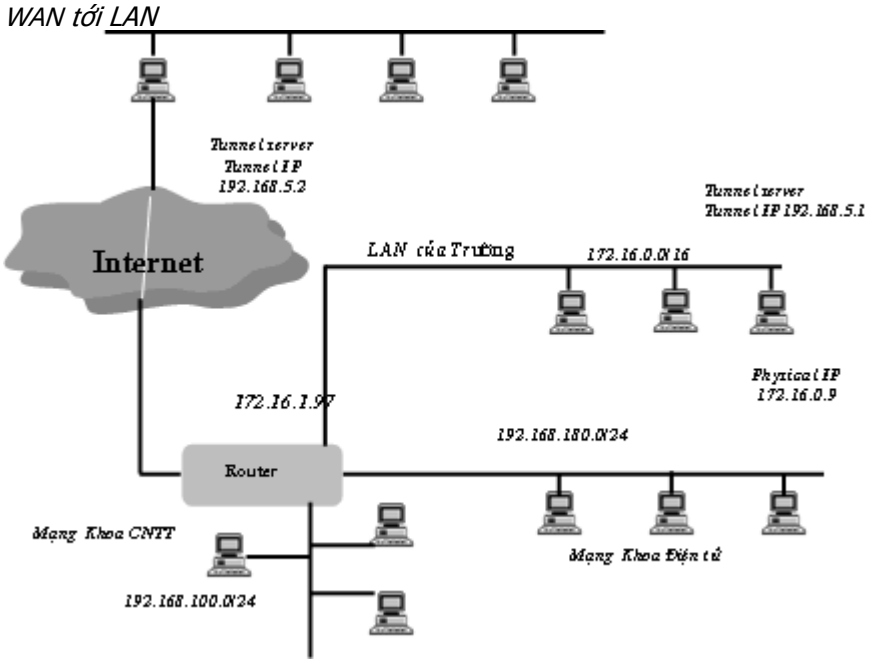
Hình 4. Mô hình một mạng sử dụng Altavista Tunnel

- **Cấu hình Altavista sử dụng cho mạng BKNet**
  - **Kết nối đơn tới LAN**



Hình 5. Mô hình thực tế (client to WAN)

WAN tới LAN



Hình 6. Mô hình thực tế (LAN to WAN)

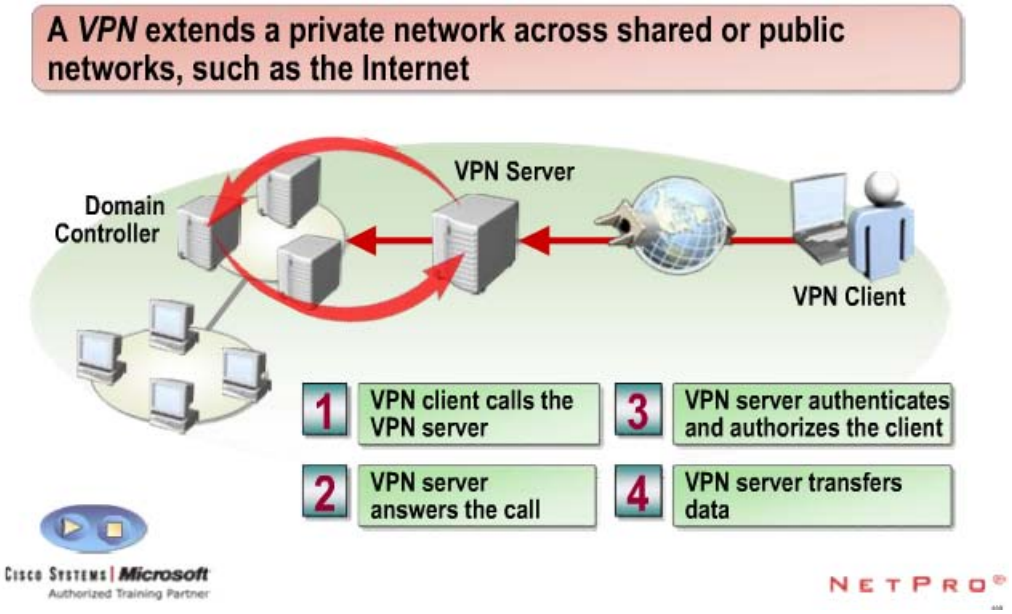
Cấu hình các máy trong mạng WAN hoàn toàn giống trong trường hợp trên.Các Tunnel Server ở đây đóng vai trò như các security gateway, xử lý các gói tin trước khi gửi chúng vào mạng nội bộ.

❖ **Kết luận**

Với những điểm mạnh của mình, rõ ràng công nghệ VPN đang là một trong những giải pháp hữu hiệu nhất để bảo mật về mạng Intranet của các trường khi kết nối vào Internet.Tuy nhiên việc nghiên cứu và xây dựng thành công một mạng riêng ảo đòi hỏi nhiều công sức cũng như chi phí, đòi hỏi nhiều kiến thức chuyên sâu về hệ thống mạng đặc biệt là các kỹ thuật và giao thức mạng LAN, WAN.Trên đây là những các thông tin cần thiết nhất về công nghệ VPN và phương án xây dựng một ứng dụng thực tế.Việc triển khai một VPN cụ thể sẽ giúp các trường bảo mật thông tin khi mở rộng các kết nối mạng ra bên ngoài và Internet, đồng thời tận dụng triệt để các lợi ích của mạng toàn cầu Internet một cách an toàn nhất.Với các công nghệ về an toàn dữ liệu được áp dụng trong mạng riêng ảo thì nó hoàn toàn có đủ độ tin cậy để có thể được triển khai trên diện rộng. Trong điều kiện kinh tế hiện nay của Việt Nam thì việc thiết lập các mạng riêng ảo sẽ giúp các trường có thể tự bảo vệ mình và tổ chức khai thác thông tin trên mạng Internet một cách hiệu quả và an toàn nhất.

THIẾT LẬP MÔ HÌNH VPN

❖ **Các bước để diễn ra một kết nối VPN (How a VPN connection work)**



- **VPN client calls the VPN Server:**

VPN client thực hiện việc kết nối đến VPN Server thông qua việc gửi yêu cầu hay thực hiện một cuộc gọi ảo đến VPN Server.
VPN Server ở đây đóng vai trò nhu là một VPN getway cho phép các VPN client truy cập vào toàn bộ mạng bên trong.

- **VPN Server answer the call:**

VPN server trả lời yêu cầu đó bằng một cuộc gọi ảo

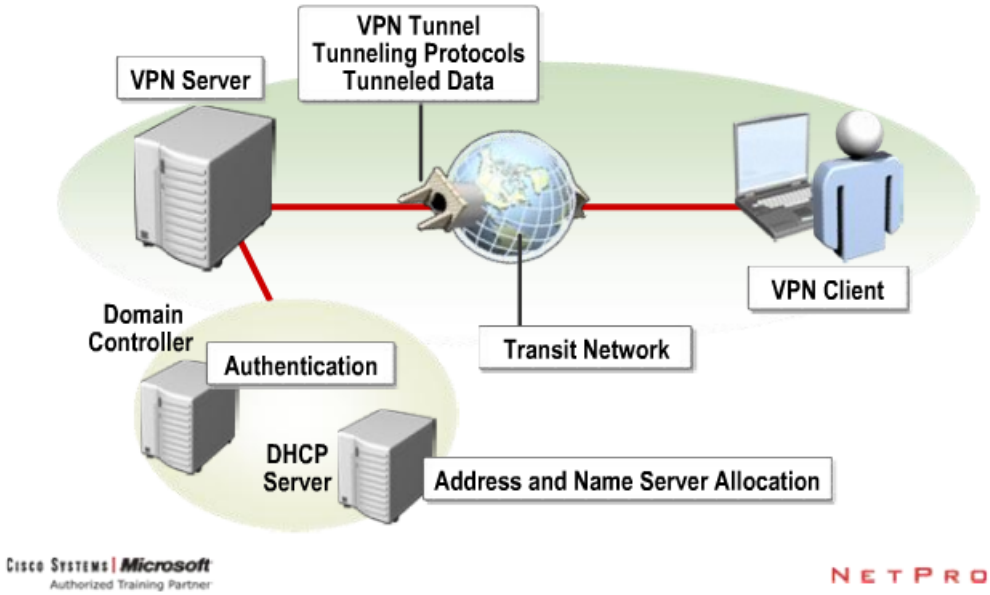
- **VPN Server Authentication and Authorizes the client:**

VPN Server thực hiện quyền xác thực bằng cách liên hệ với Domain controller và xác nhận các user đó được ủy quyền cho phép kết nối hay không.

- **VPN Server transfer data:**

Khi đã hình thành 1 VPN tunnel VPN server sẽ làm nhiệm vụ chuyển tải giữa VPN client và mạng nội bộ bên trong.
Qua đó ta thấy được tạo ra một kết nối VPN rất đơn giản, chi phí thấp, không cần một đường dây vật lí, và yêu cầu phần cứng.
Ngoài ra còn nâng cao khả năng bảo mật bằng viêc xác thực và mã hóa, bảo mật địa chỉ IP qua mạng internet do quá trình mã hóa đường truyền.

❖ **Componsents of a VPN Connection (Các thành phần của một kết nối VPN).**



Một kết nối VPN bao gồm các thành phần sau:

- ✓ **VPN Server:**

Là một server cài đặt các dịch vụ Routing and Remote Access và được cấu hình với vai trò là một VPN servet để tạo ra một kết nối VPN giữa VPN client và mạng internal bên trong.

- ✓ **VPN Client:**

Là một máy tính bất kỳ thực hiện quá trình yêu cầu kết nối VPN đầu tiên đến VPN server.

- ✓ **Transit Network:**

Là một mạng chia sẻ ở đó cho phép các dữ liệu được đóng gói đi qua.Transit Network ở đây chính là mạng internet.

- ✓ **VPN Tunnel:**

Là một phần của kết nối ở đó dữ liệu được đóng gói và mã hóa.

- ✓ **Tunneling Protocol:**

Là giao thức được sử dụng để quản lí các Tunnel và đóng gói dữ liệu (Giao thức TCP/IP).

- ✓ **Tunnel Data:**

Dữ liệu được truyền qua kết nối riêng Point – to – point

- ✓ **Authentication:**

Quá trình xác thực cho phép ta nhận ra VPN client nào được ủy quyền truy cập vào mạng bên trong

- ✓ **Domain Controller:**

Cung cấp các nhân tố bảo mật, là các user và ủy quyền cho các VPN client khi truy cập vào mạng kết nối internal bên trong

- ✓ **Address and name Server Allocation:**

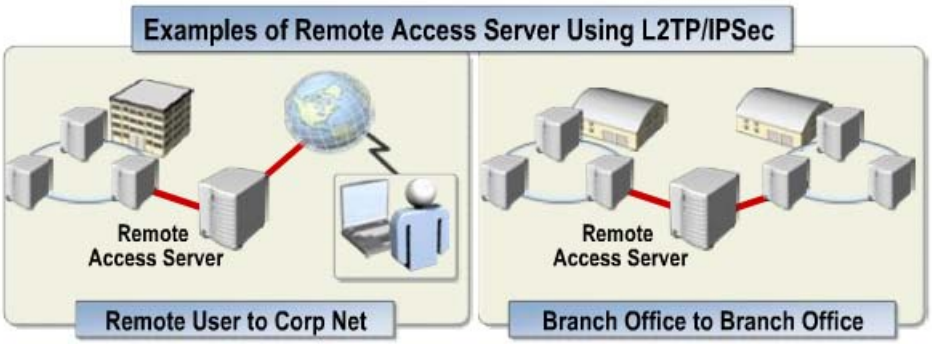
Cấp phát địa chỉ IP và phân giải DNS.Thường dùng DHCP Server để cấp IP hoặc cấp dải địa chỉ IP tĩnh trên máy chủ VPN Server.

- ❖ **Encryption Protocols for a VPN Connection (Các giao thức mã hóa kết nối VPN).**

Trong winserver 2003 có sử dụng 2 giao thức mã hóa là: **PPTP** và **L2TP/IPSec**.

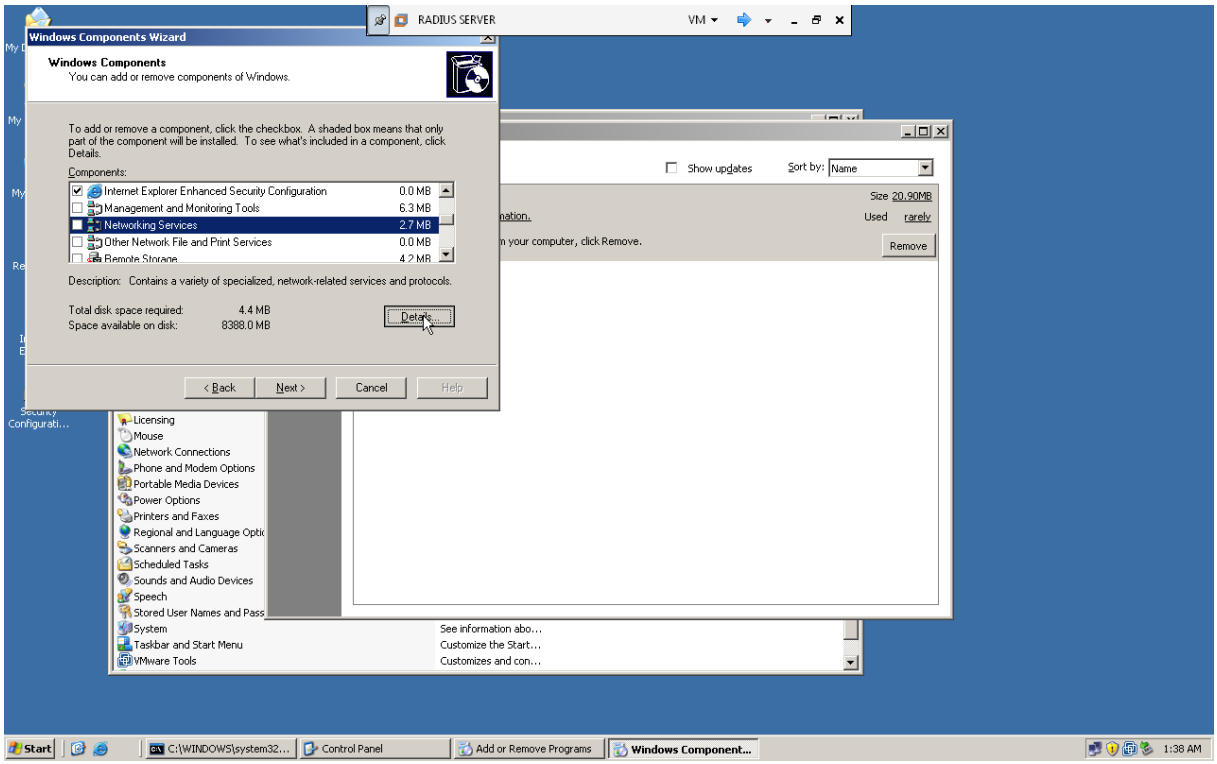
Category	Description
PPTP	Uses PPP user authentication and MPPE
L2TP/IPSec	Uses PPP user authentication over a connection that is encrypted with IPSec

Hiện nay L2TP/ IPSec là giao thức mã hóa và bảo mật rất tốt nên nó được khuyến cáo sử dụng trong các mô hình truy cập tù xa như: VPN Client (Client thực hiện việc kết nối VPN đến VPN server trước, khi kết nối được thiết lập Client có thể truy cập đến bên trong mạng Internal), VPN site–to–site (Một VPN server của site này sẽ kết nối đến một VPN Server của site khác thông qua mạng internet, khi kết nối được thiết lập thì máy tính cả cả 2 site có thể truy cập lẫn nhau).

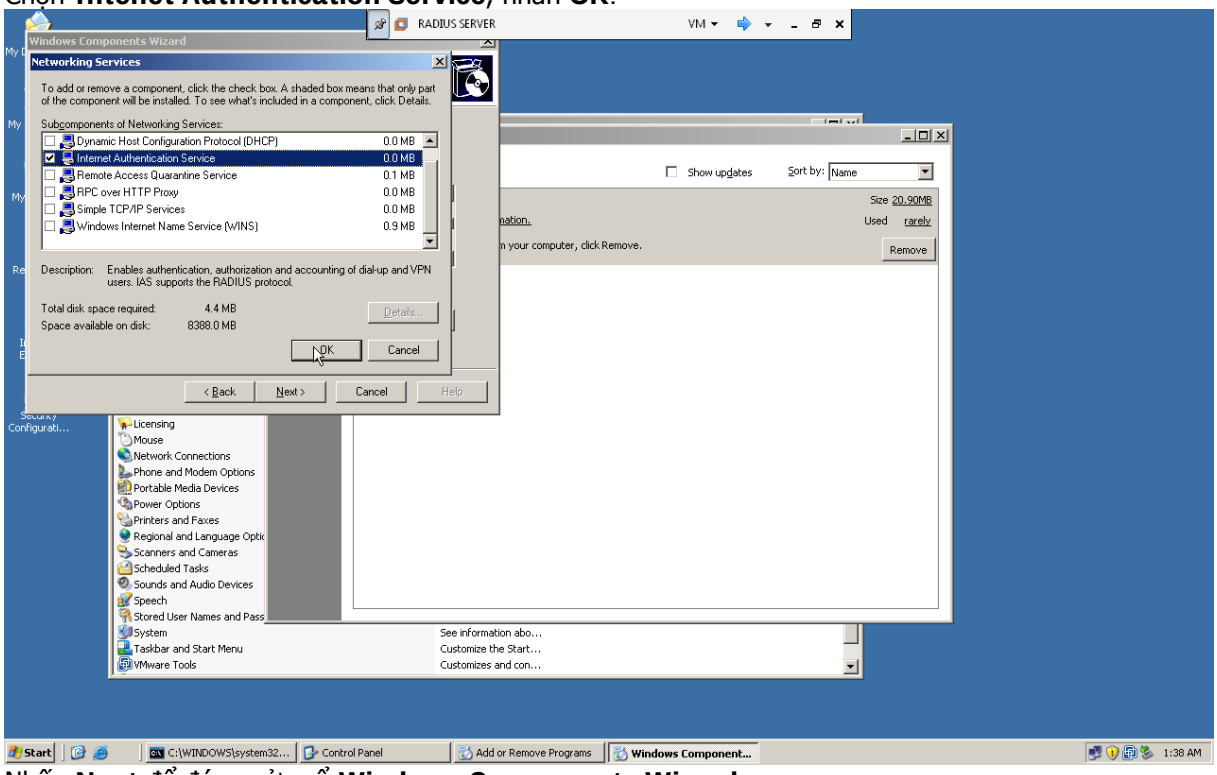


- **Lab thực hành cấu hình VPN**
- ✓ **VPN Client-to-Site with Radius**
- **Trên máy Radius Server**:

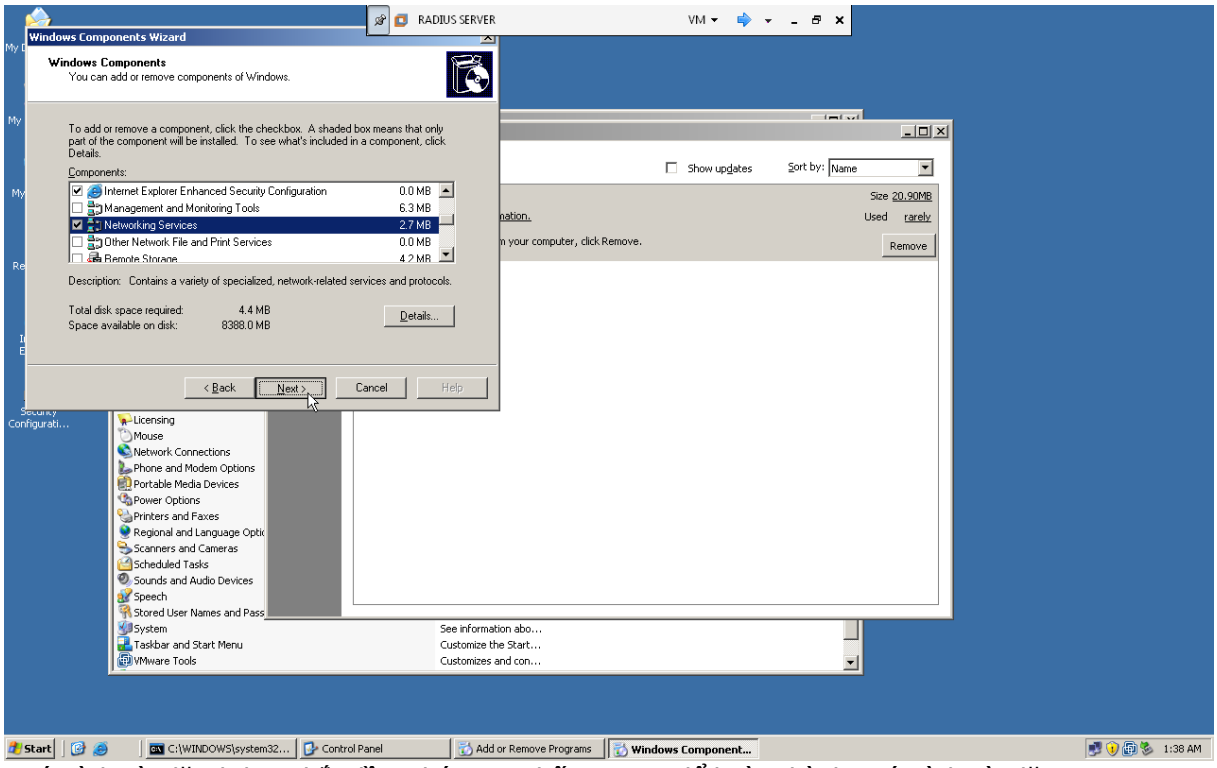
Vào **Control Panel->Add Remove Programs**, chọn **Add Windows Components**, sau đó chọn **Networking Services**, nhấn **Details**:



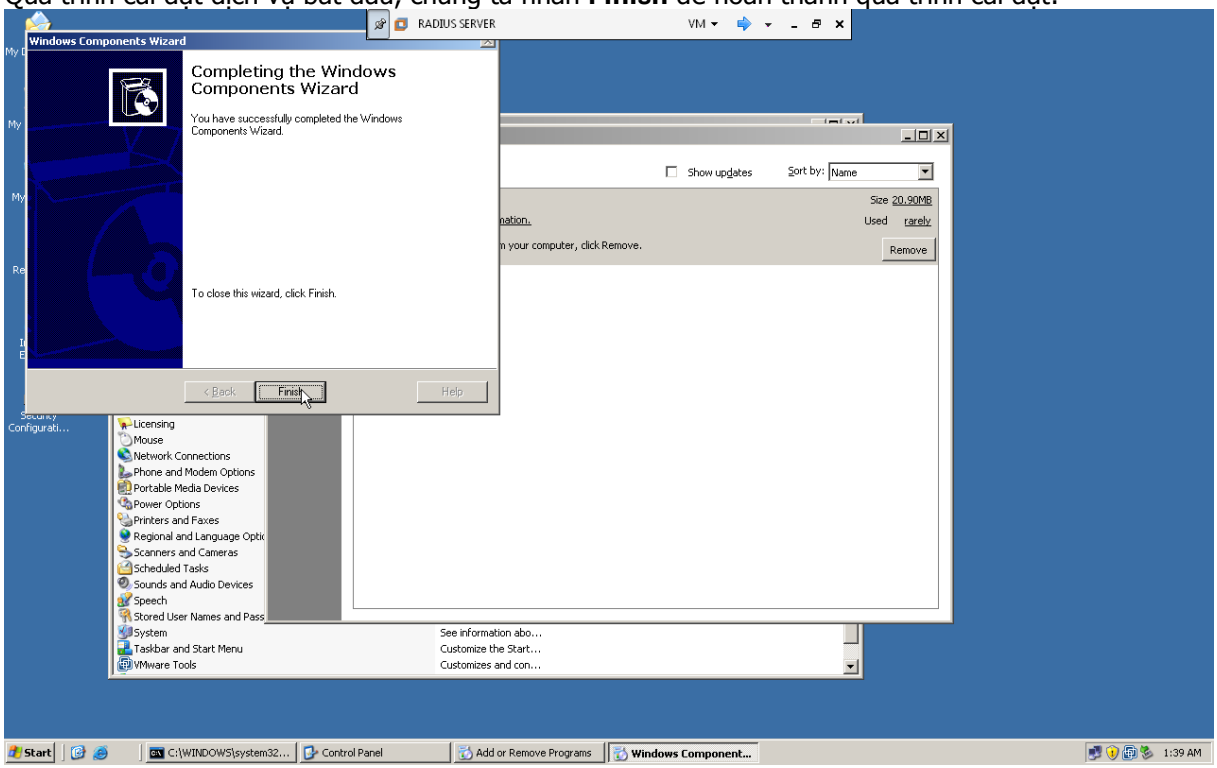
Chọn **Intenet Authentication Service**, nhấn **OK**:



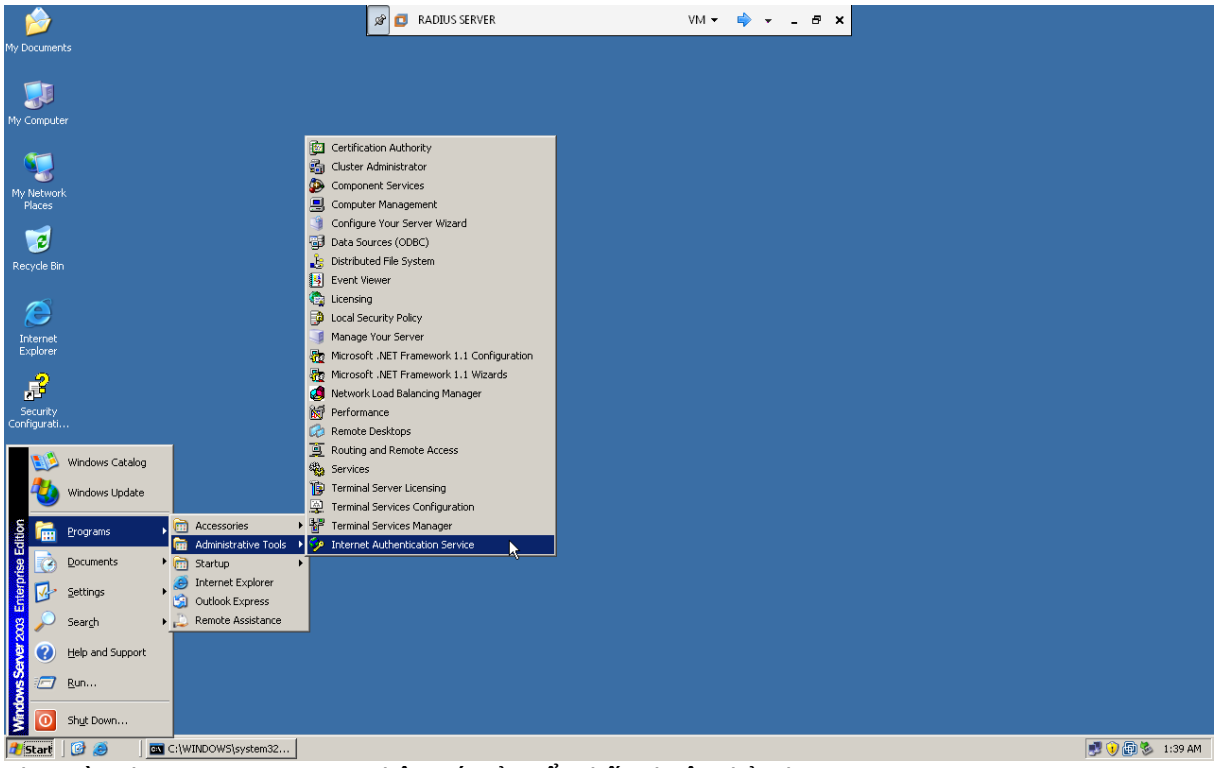
Nhấn **Next** để đóng cửa sổ **Windows Components Wizard**:



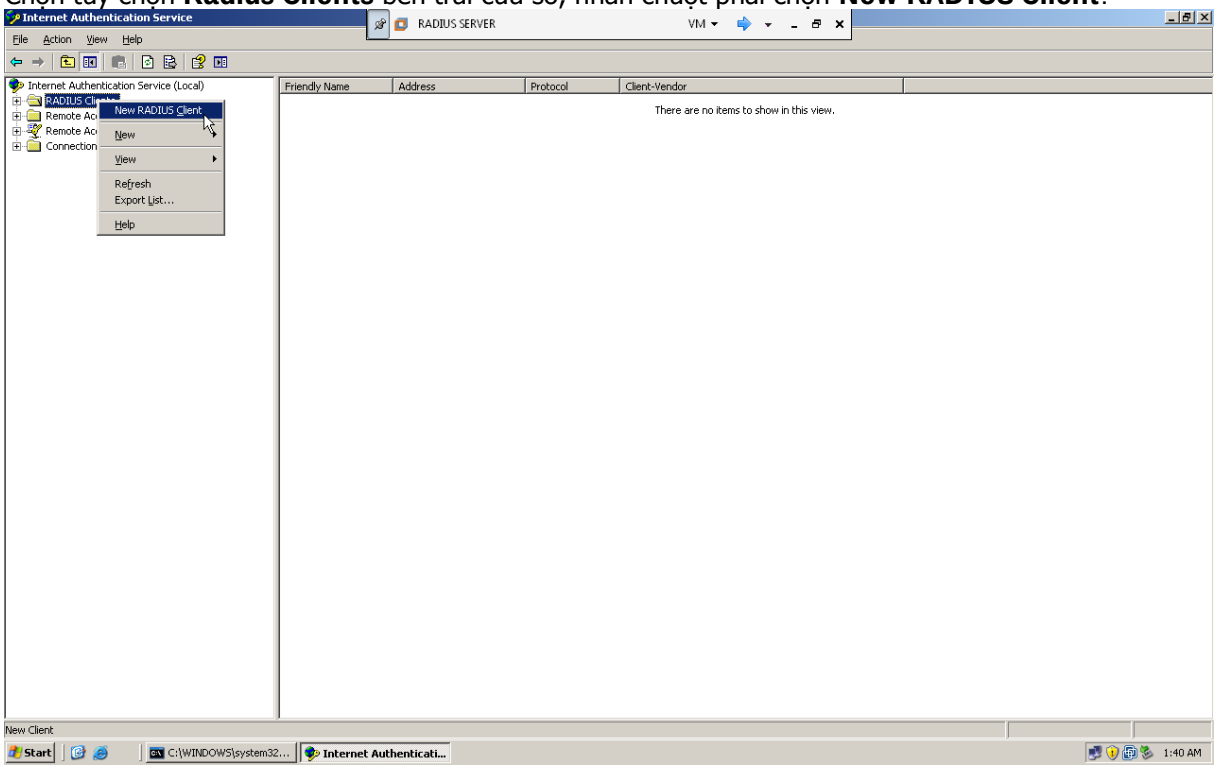
Quá trình cài đặt dịch vụ bắt đầu, chúng ta nhấn **Finish** để hoàn thành quá trình cài đặt:



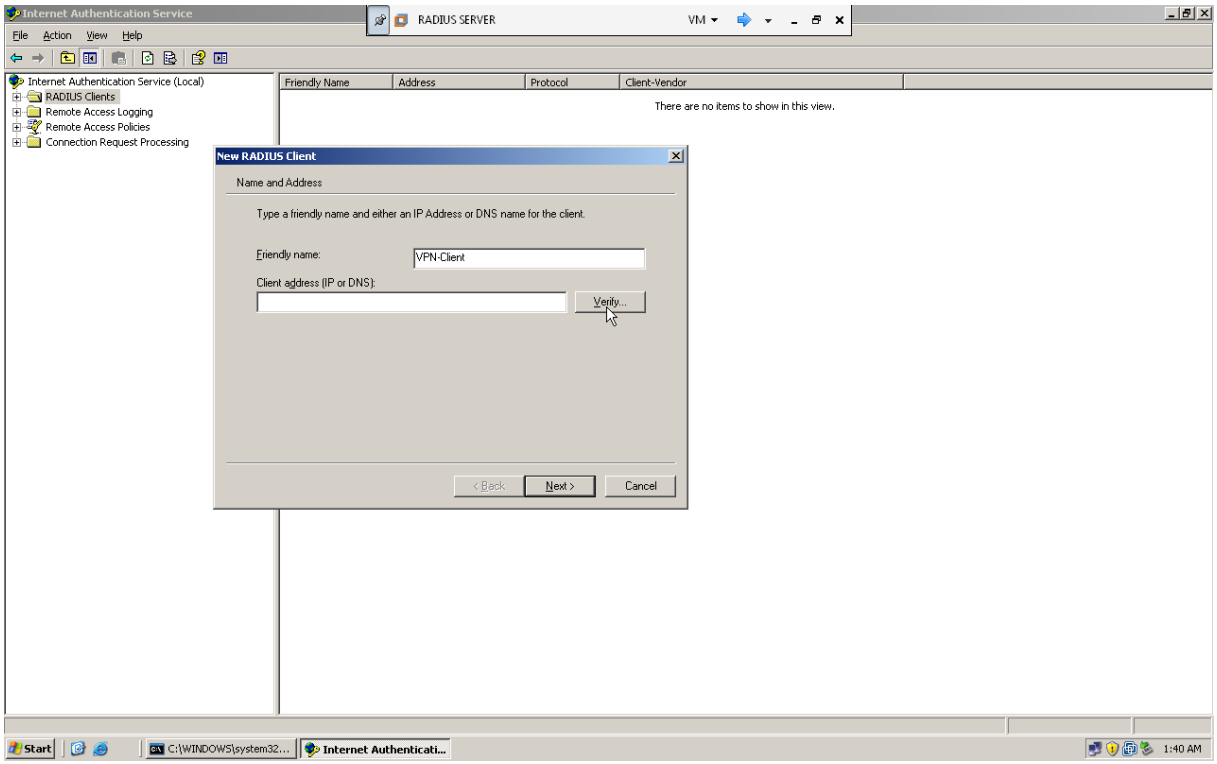
Cấu hình Radius Server bằng cách vào **Start->Programs->Administrative Tool-> Intenet Authentication Service**:



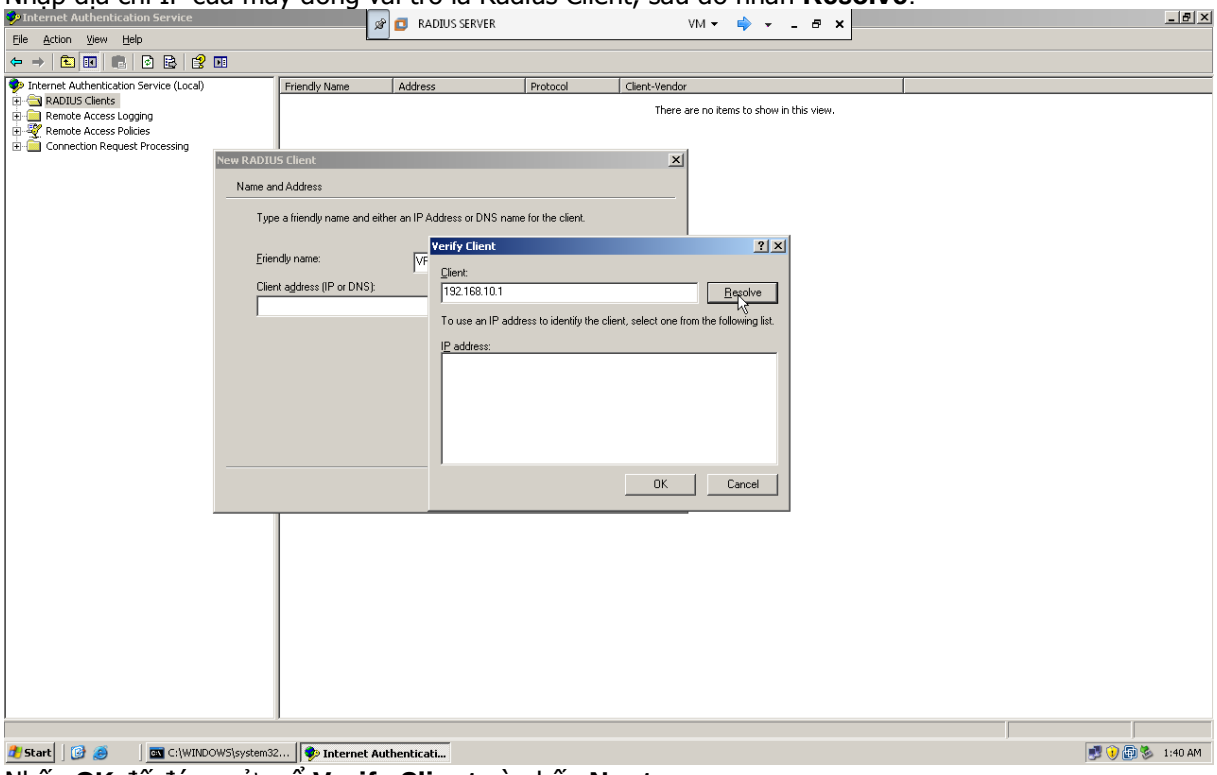
Chọn tùy chọn **Radius Clients** bên trái cửa sổ, nhấn chuột phải chọn **New RADIUS Client**:



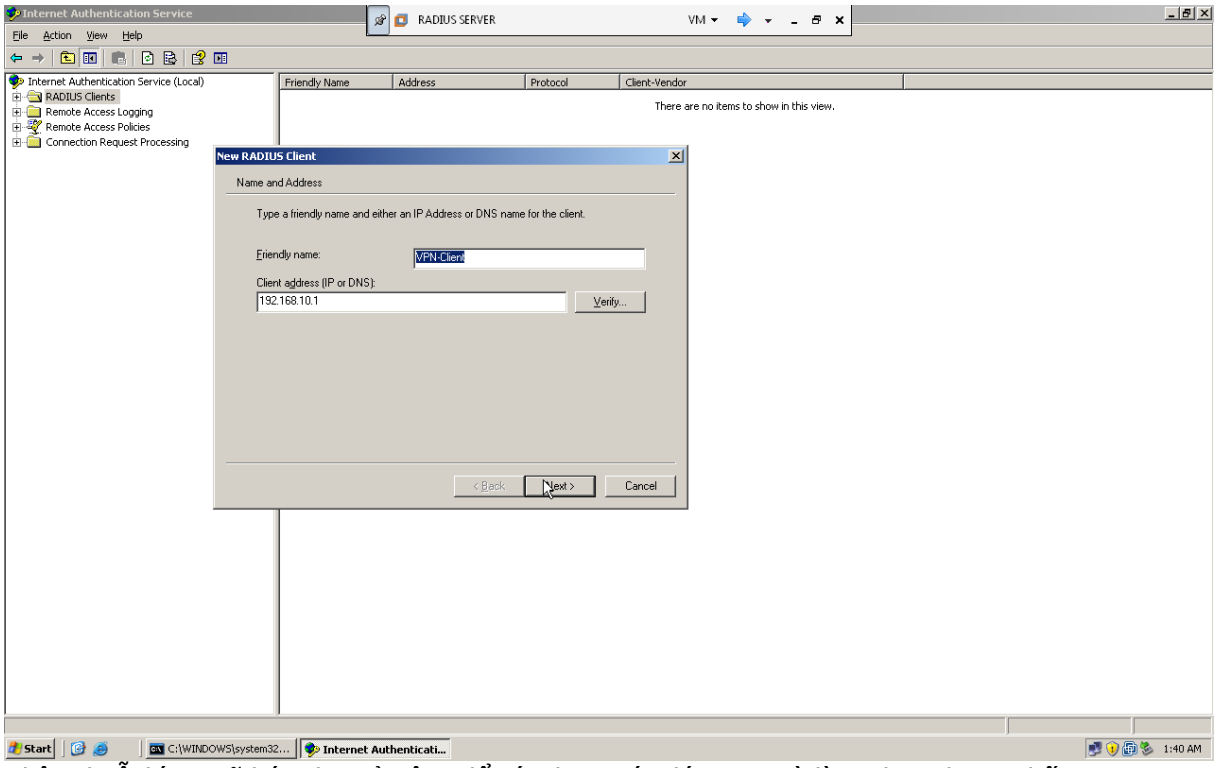
Đặt tên cho máy đóng vai trò là **Radius Client** (ở đây chính là Root Domain), sau đó nhấn **Verify**:



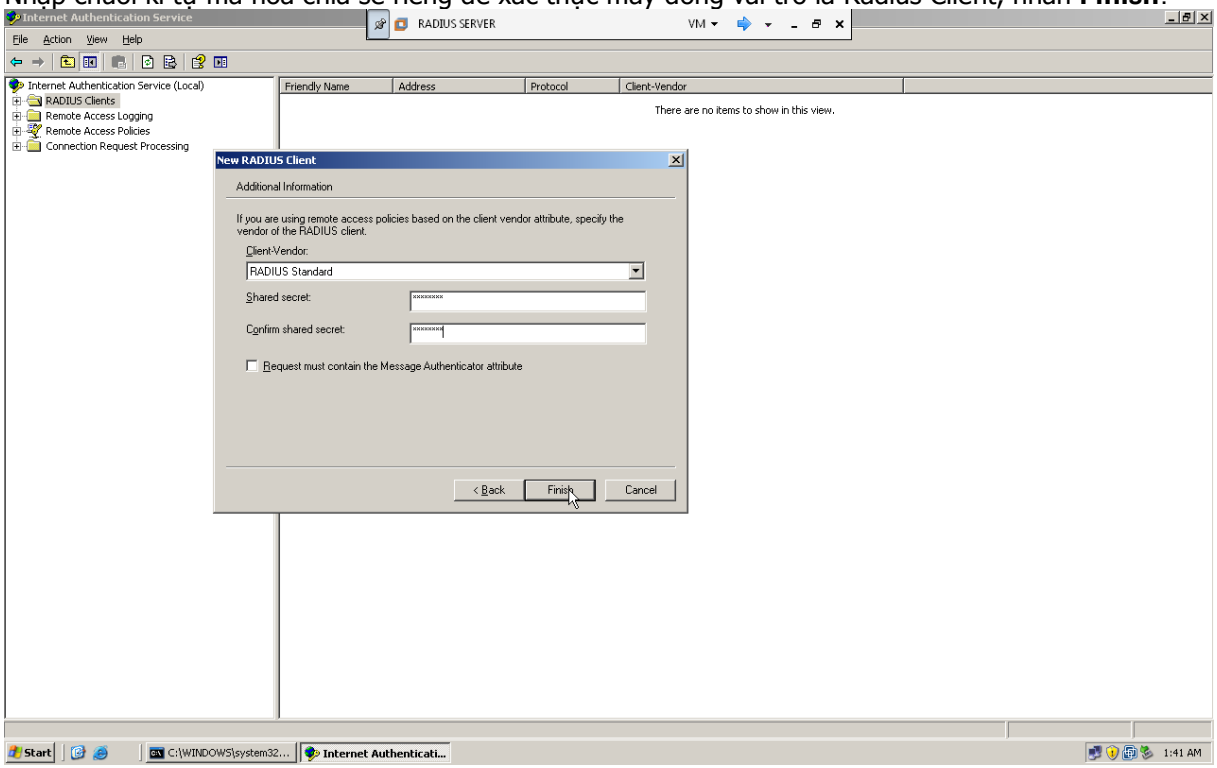
Nhập địa chỉ IP của máy đóng vai trò là Radius Client, sau đó nhấn **Resolve**:



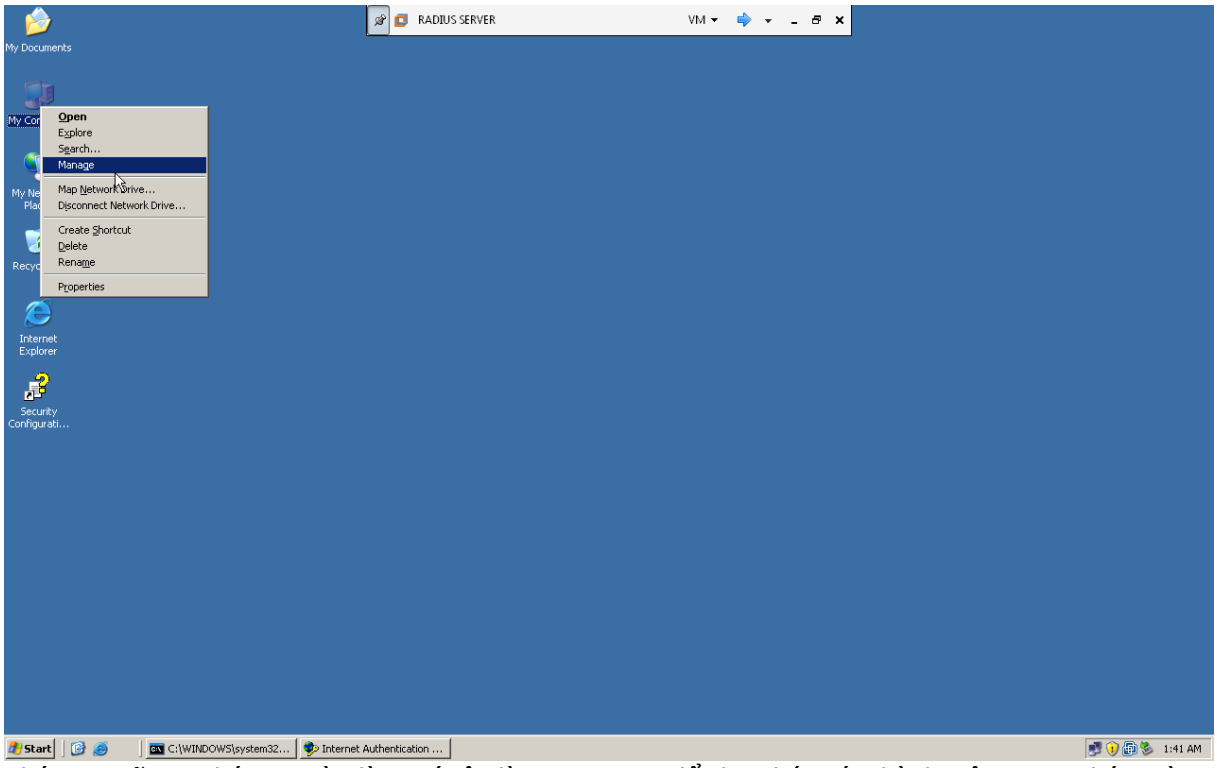
Nhấn **OK** để đóng cửa sổ **Verify Client** và nhấn **Next**:



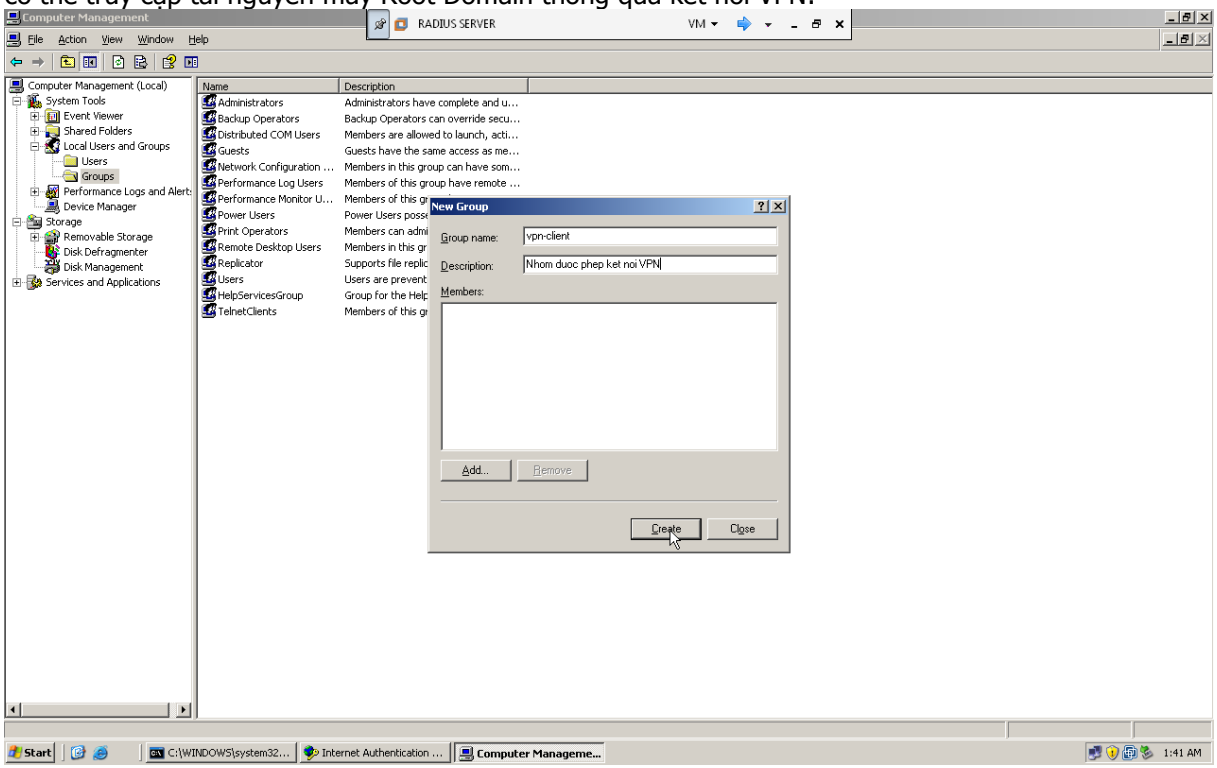
Nhập chuỗi kí tự mã hóa chia sẻ riêng để xác thực máy đóng vai trò là Radius Client, nhấn **Finish**:



Chúng ta ra ngoài màn hình **Desktop**, chọn **My Computer**, nhấn **Manage**:

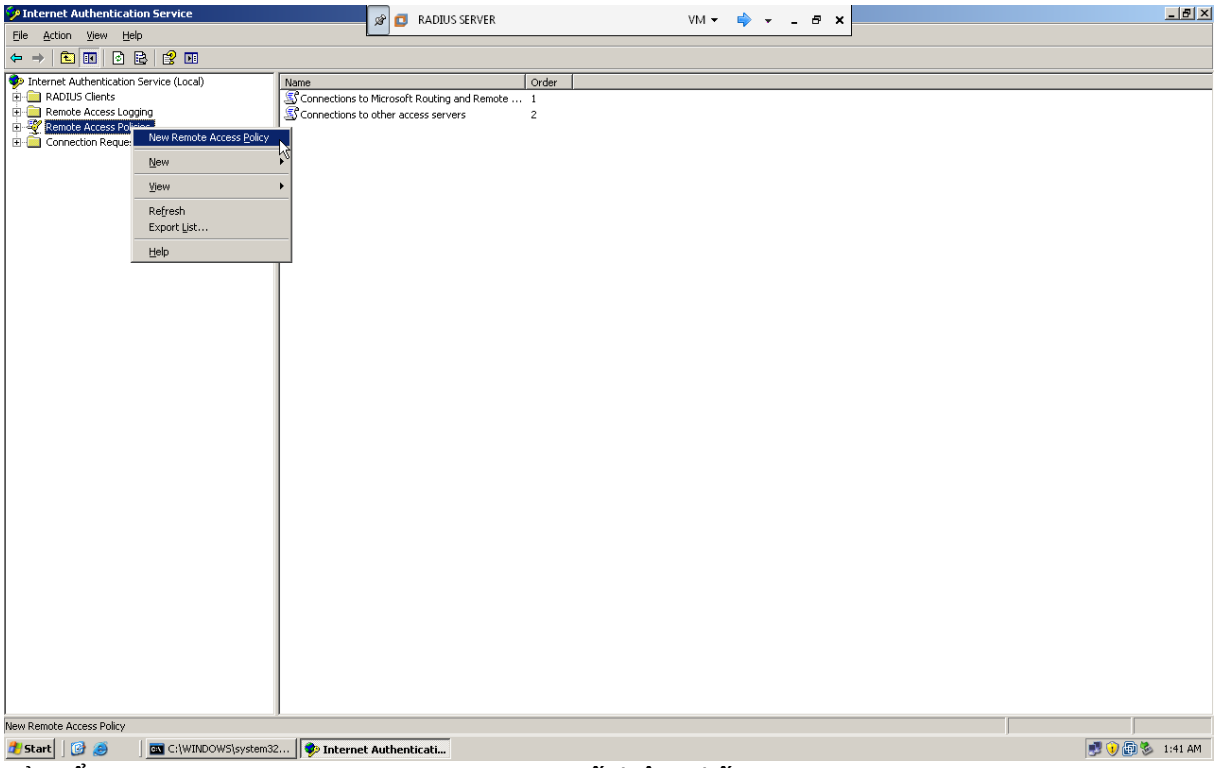


Chúng ta sẽ tạo nhóm người dùng có tên là **vpn-client** để cho phép các thành viên trong nhóm này có thể truy cập tài nguyên máy Root Domain thông qua kết nối VPN:

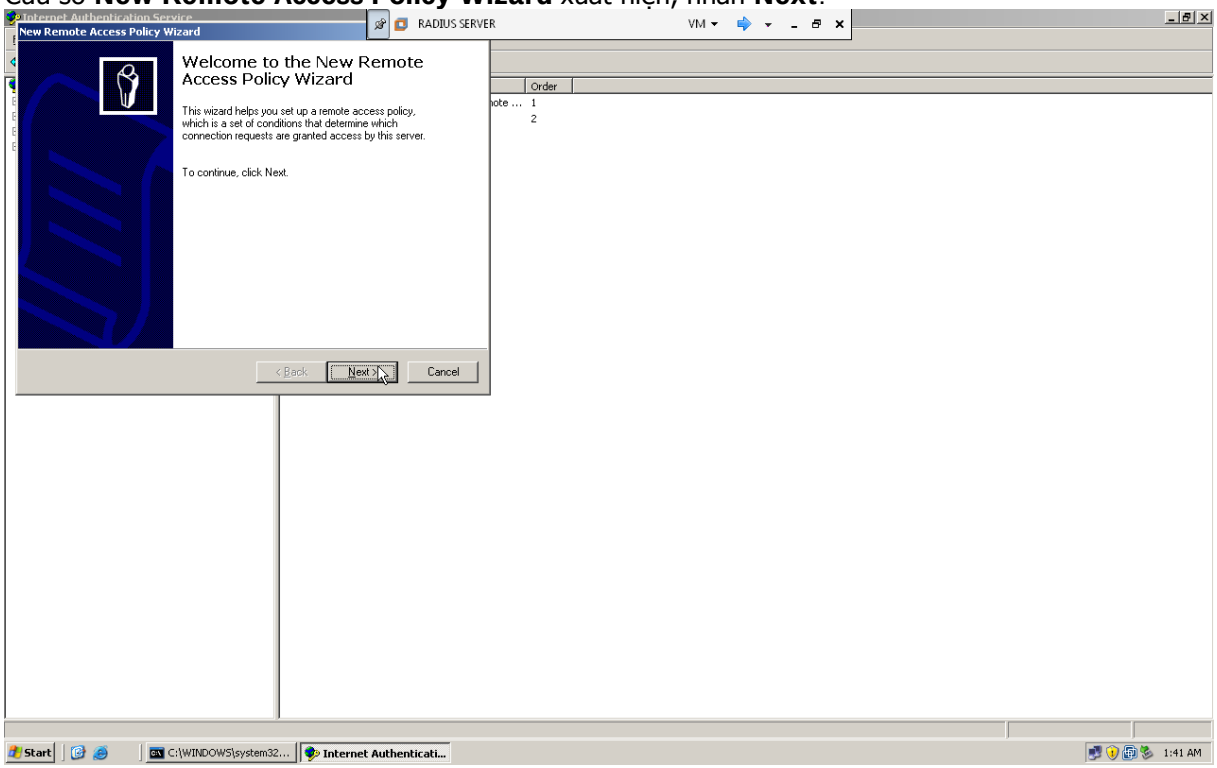


Đồng thời chúng ta sẽ tạo một tài khoản người dùng và cho tài khoản này là thành viên của nhóm **vpn-client**.

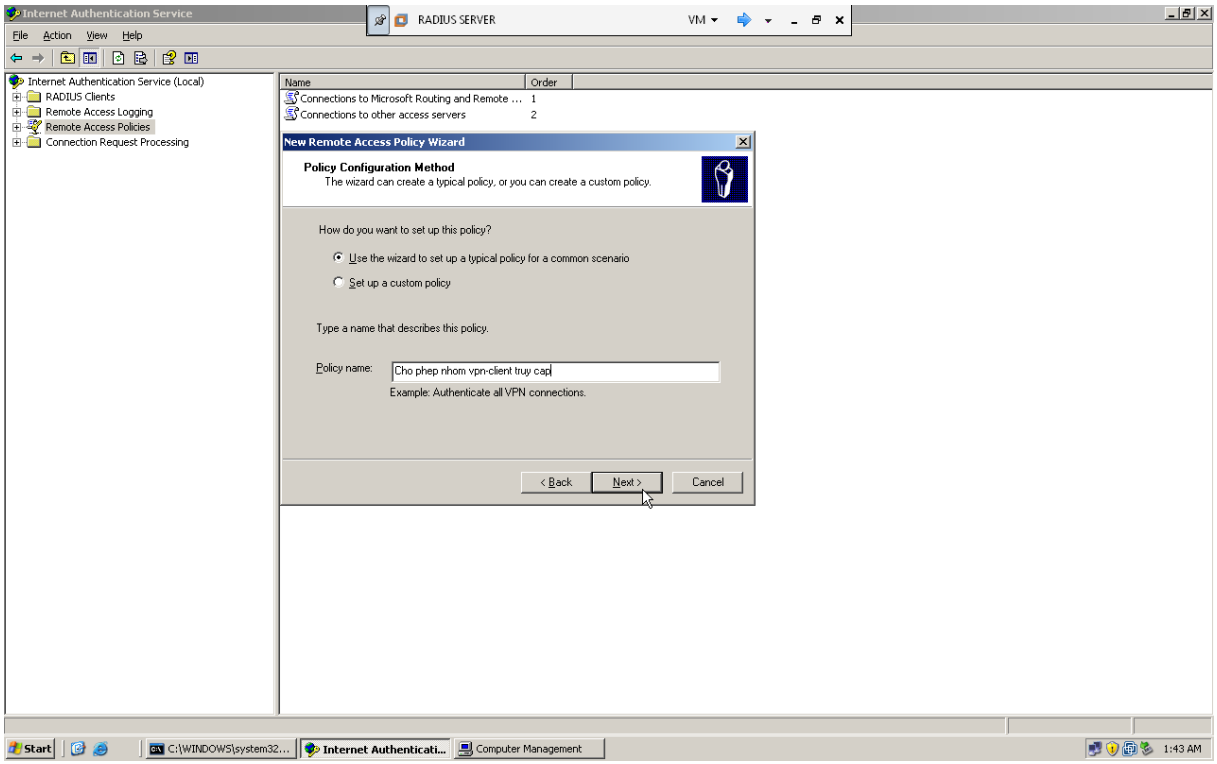
Chúng ta mở cửa sổ **Internet Authentication Service**, chọn tùy chọn **Remote Access Policies**, nhấn chuột phải chọn **New Remote Access Policy**:



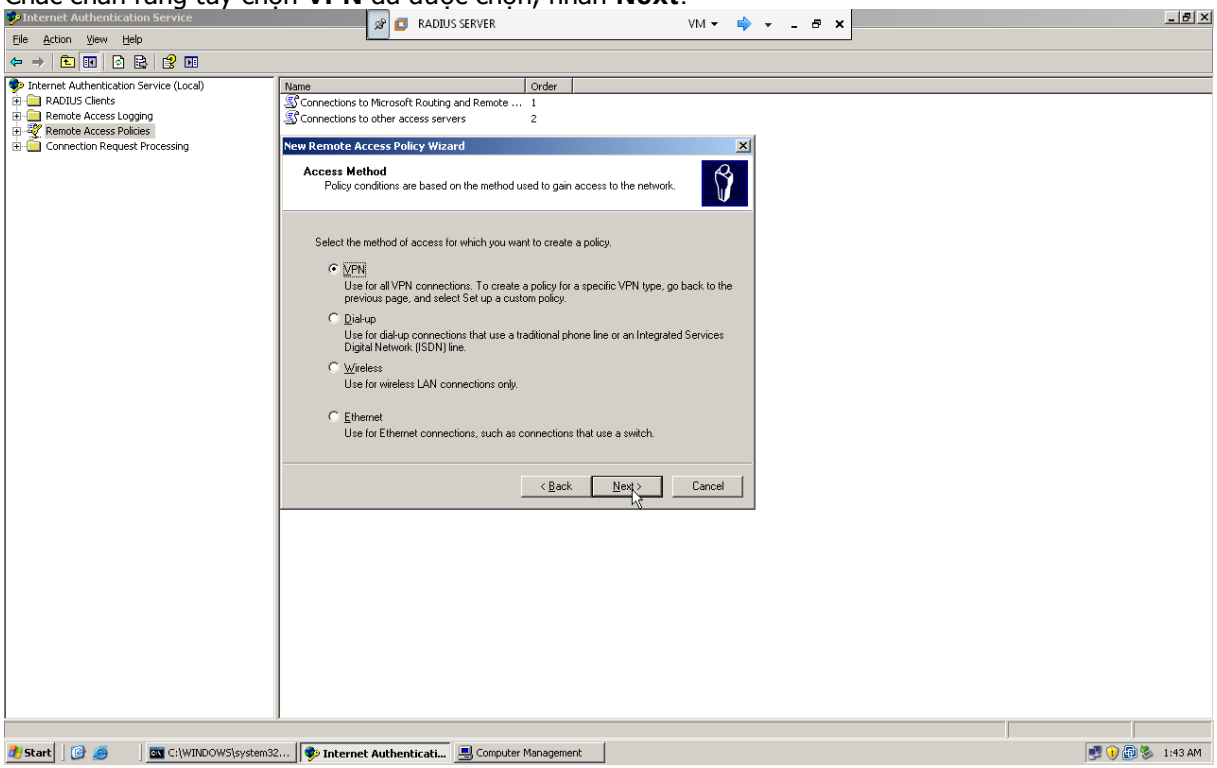
Cửa sổ **New Remote Access Policy Wizard** xuất hiện, nhấn **Next**:



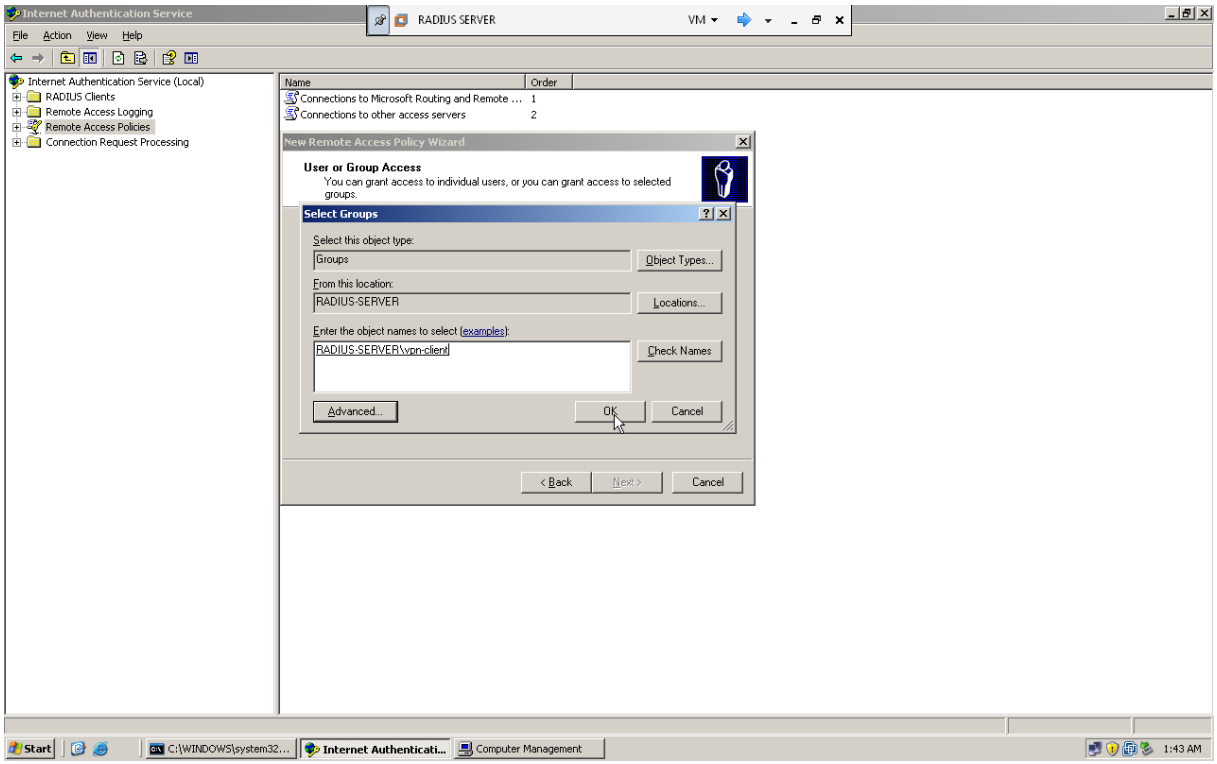
Đặt tên cho chính sách là **"Cho phep nhom vpn-client truy cap"**, nhấn **Next**:



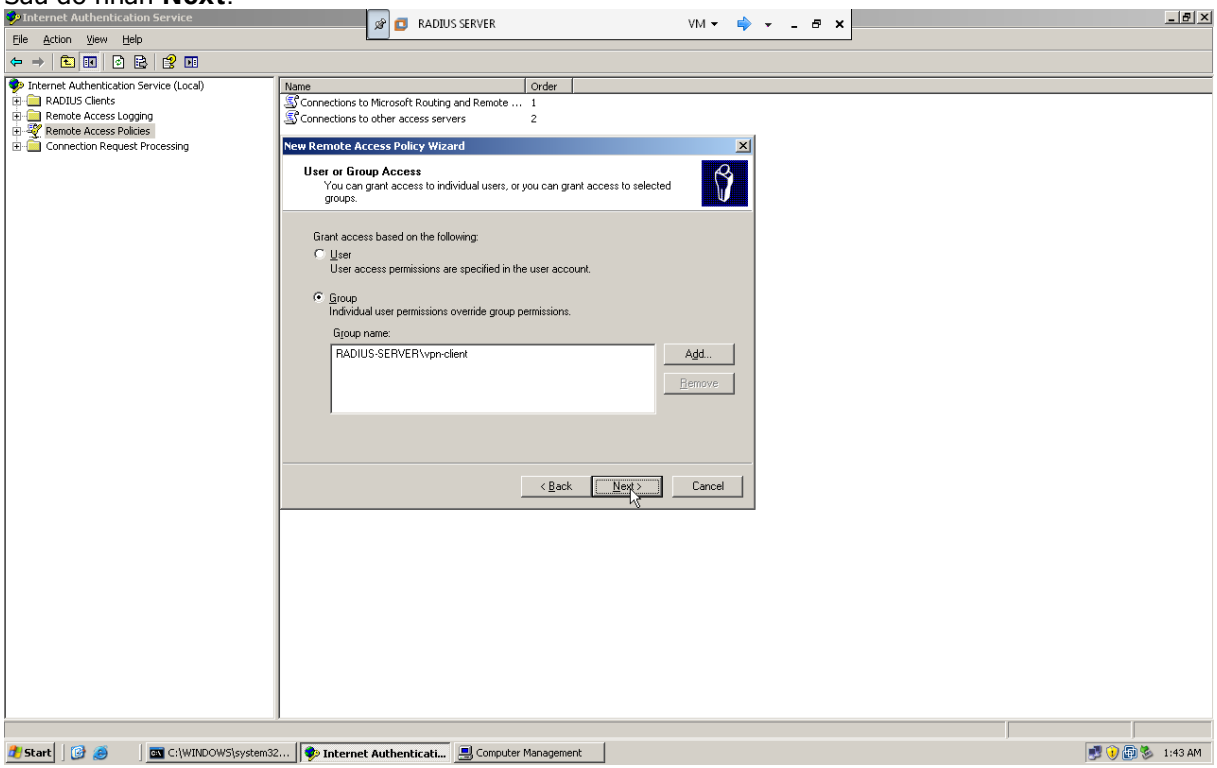
Chắc chắn rằng tùy chọn **VPN** đã được chọn, nhấn **Next**:



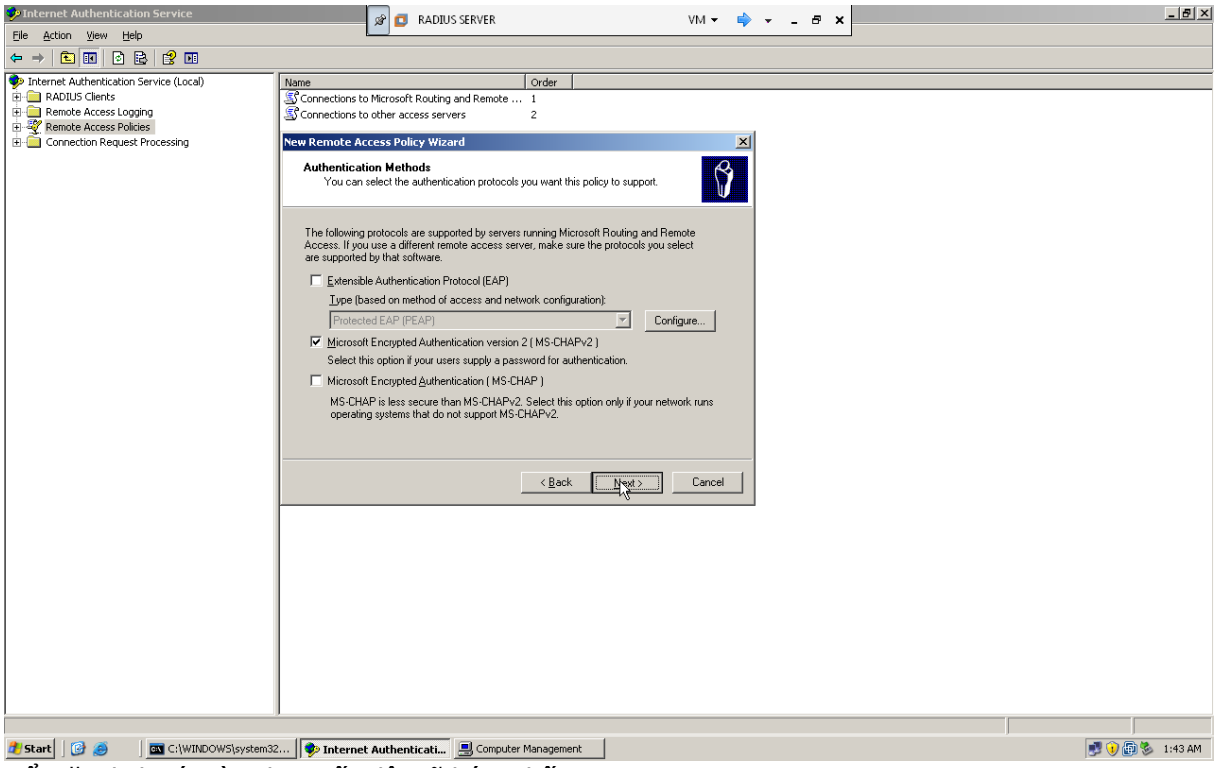
Chúng ta thêm nhóm vpn-client bằng cách nhấn nút **Add** và chọn nhóm, sau đó nhấn **OK**:



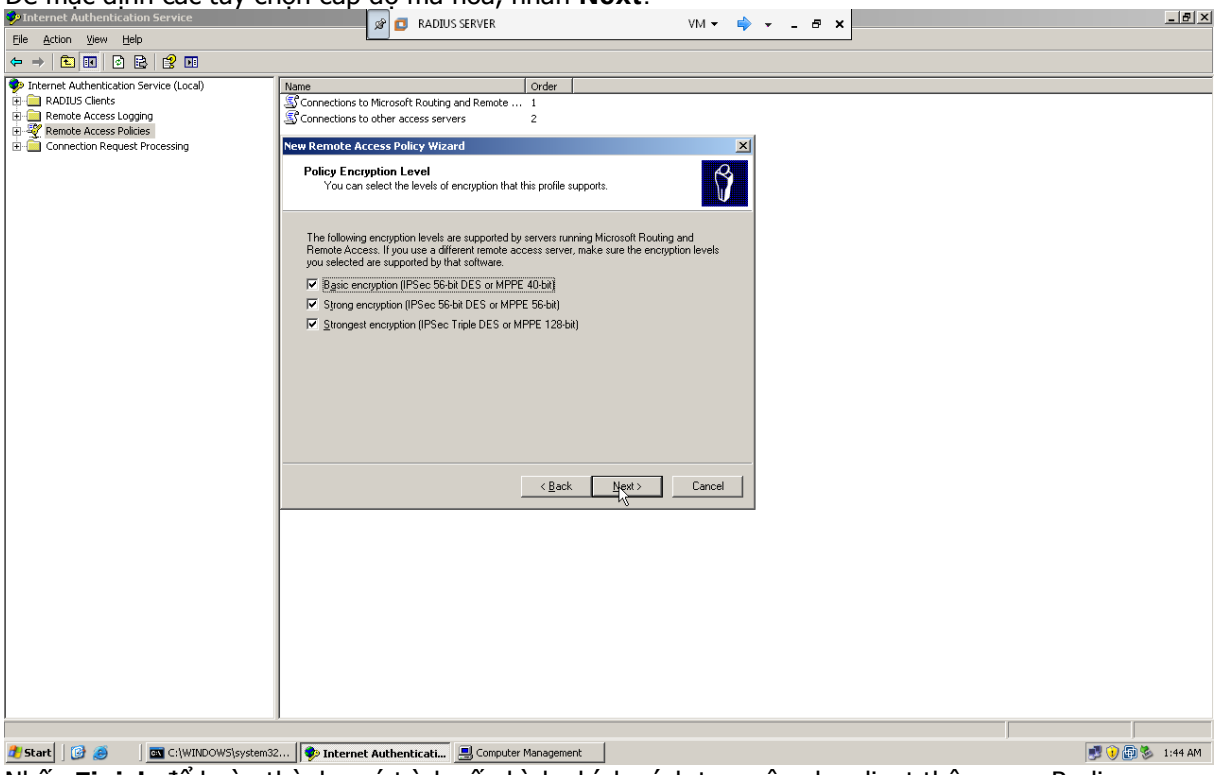
Sau đó nhấn **Next**:



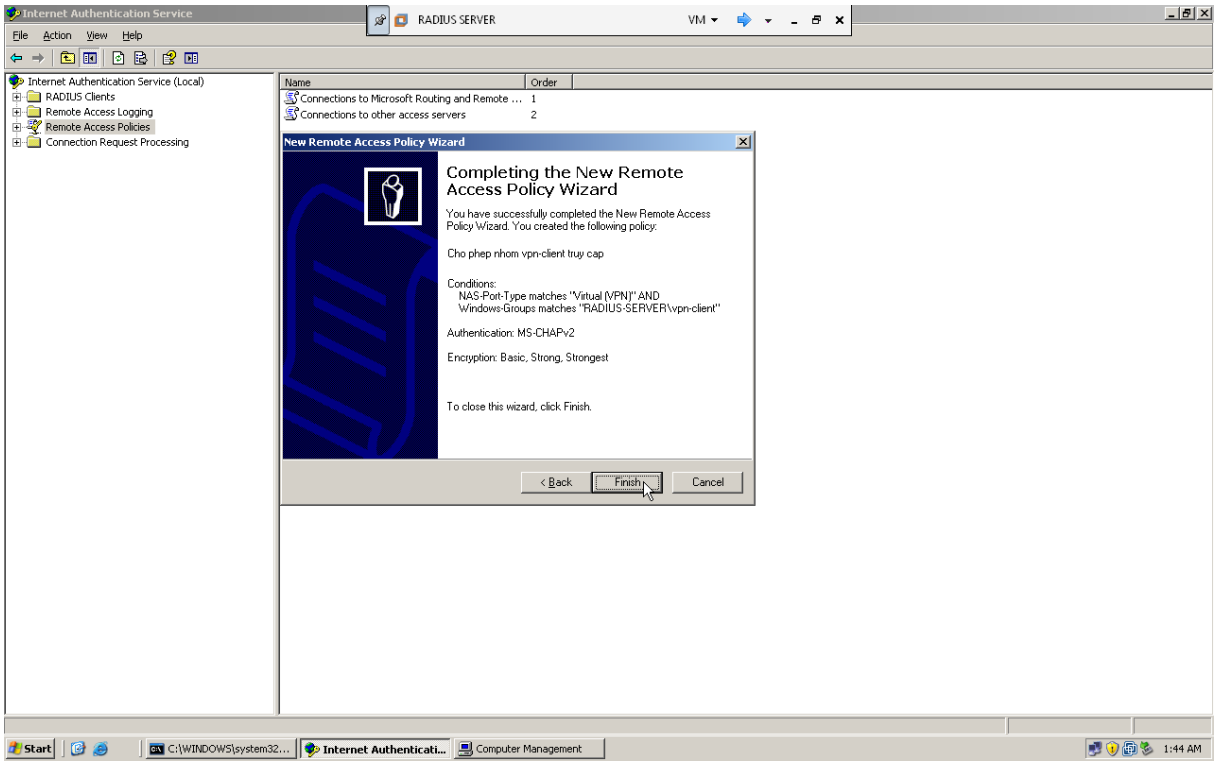
Sau đó nhấn **Next**:



Để mặc định các tùy chọn cấp độ mã hóa, nhấn **Next**:

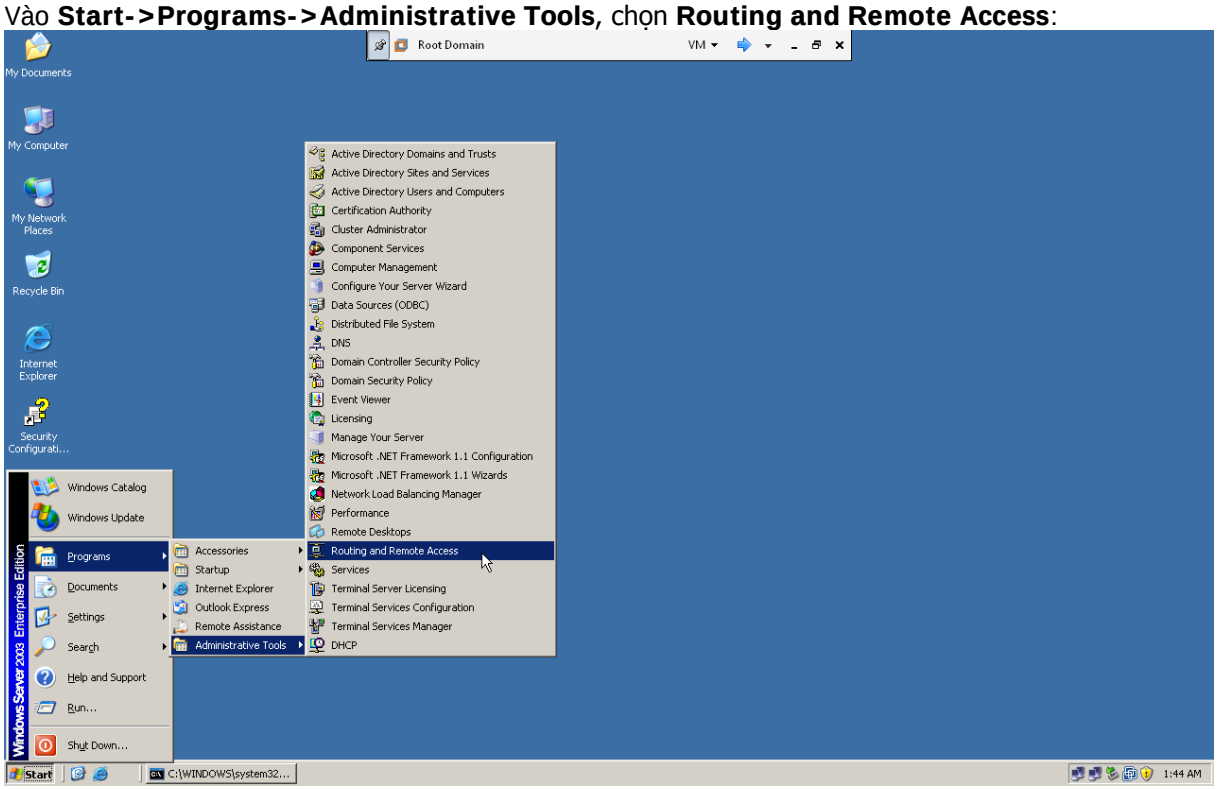


Nhấn **Finish** để hoàn thành quá trình cấu hình chính sách truy cập cho client thông qua Radius Server:

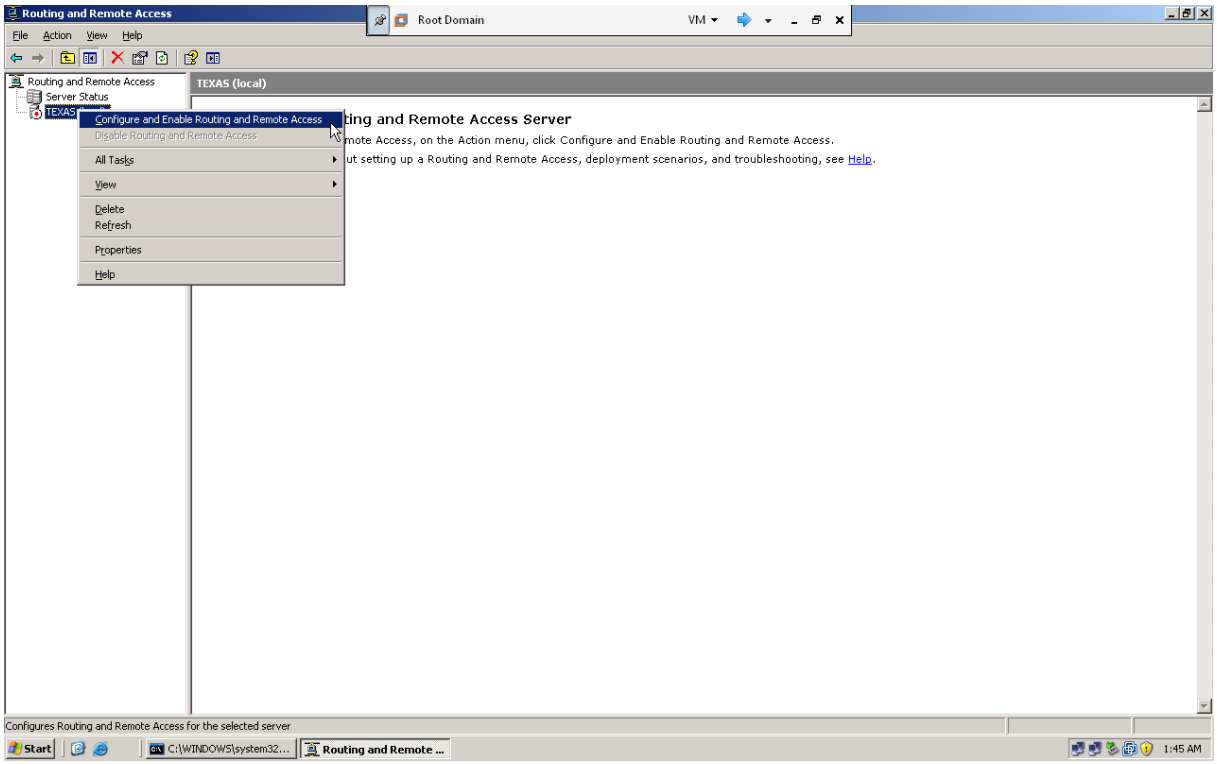


- **Trên máy Root Domain**:

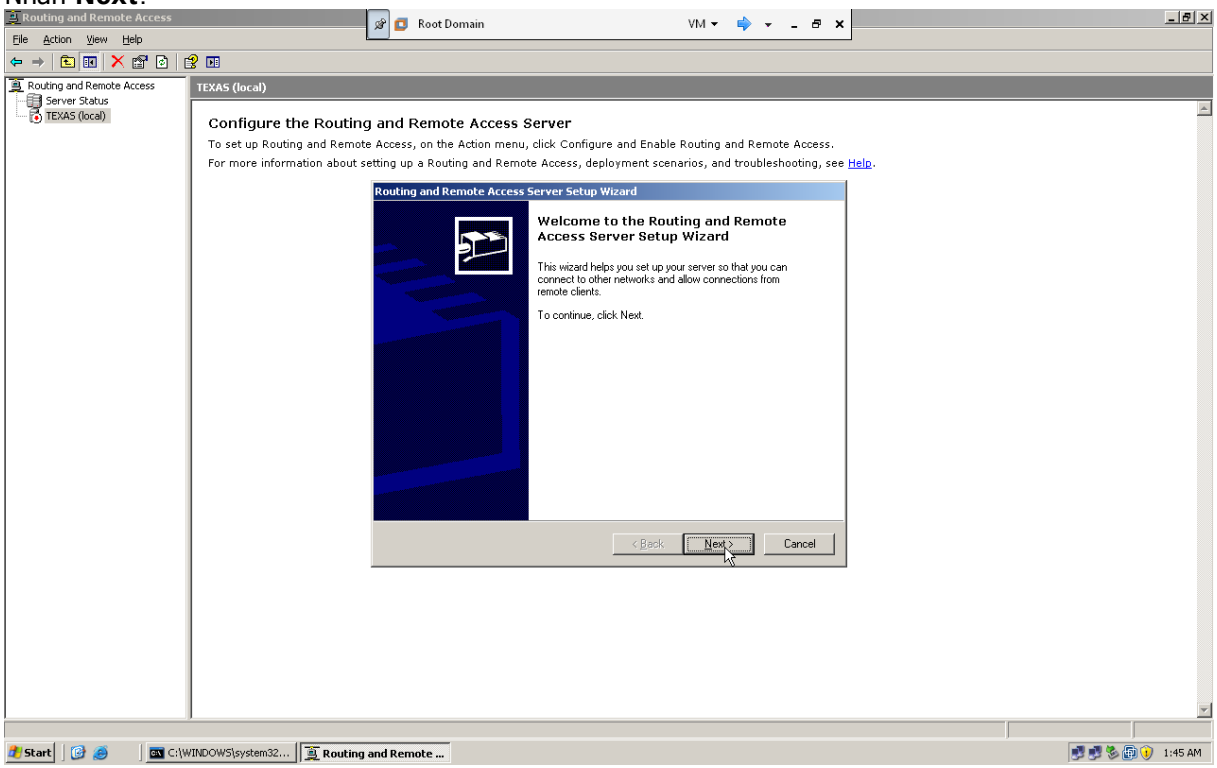
Vào **Start->Programs->Administrative Tools**, chọn **Routing and Remote Access**:



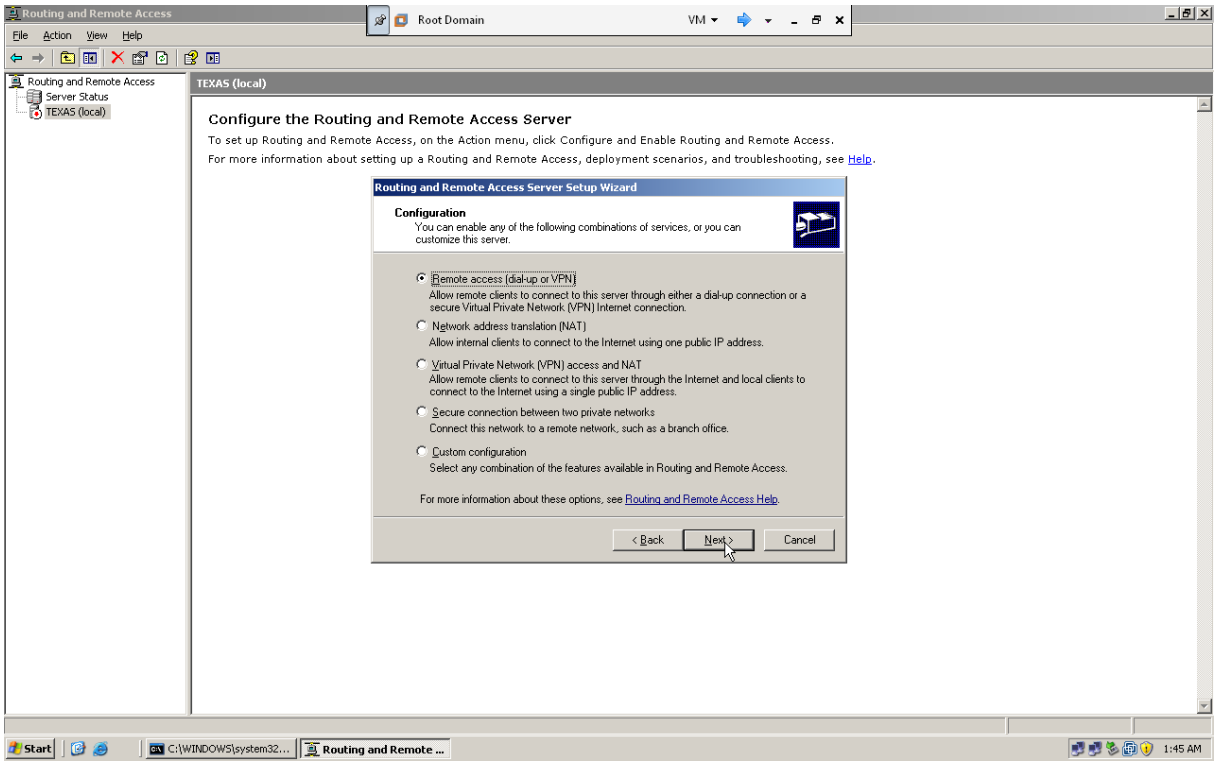
Chọn tên máy, nhấn chuột phải và chọn **Configure and Enable Routing and Remote Access**:



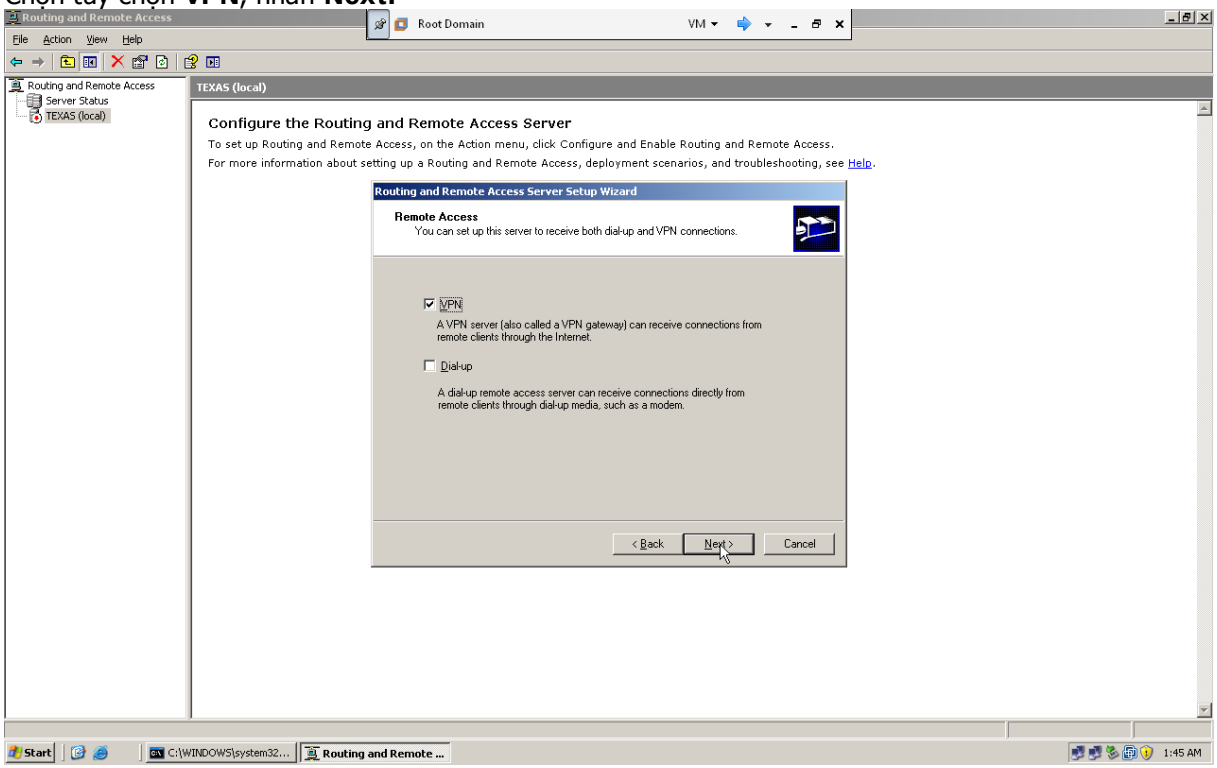
Nhấn **Next**:



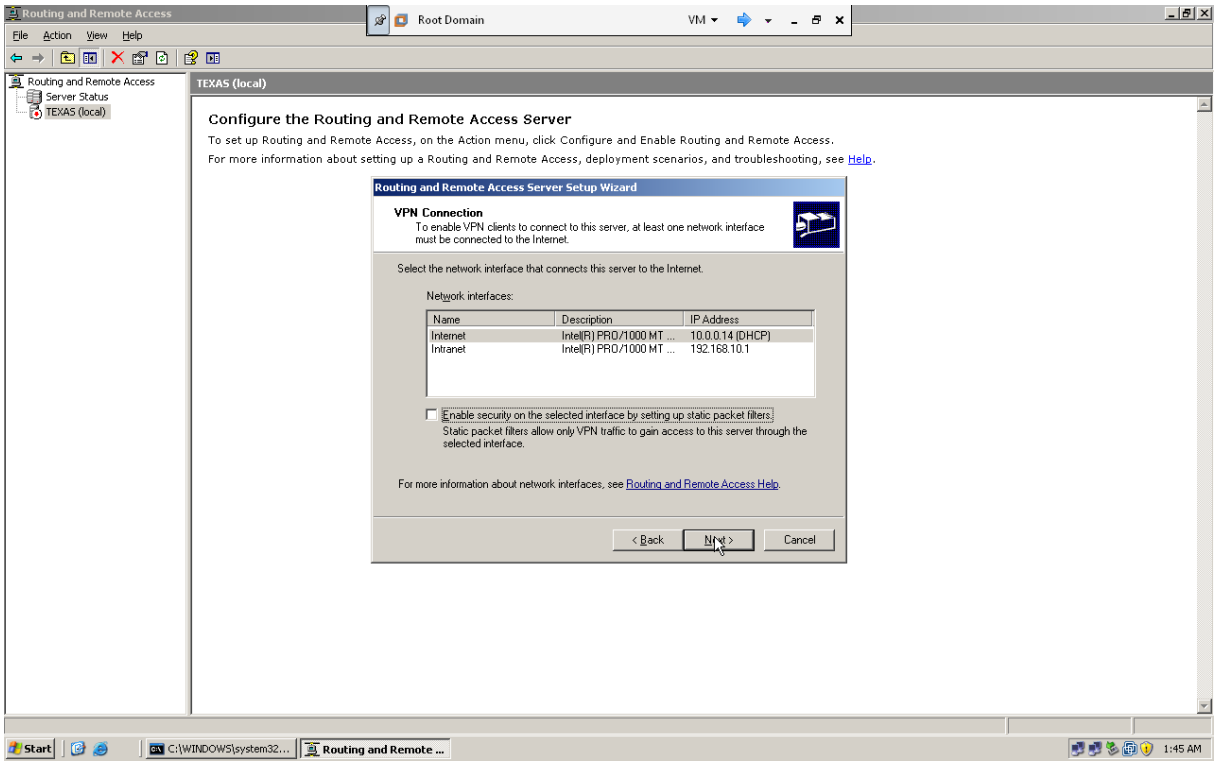
Chọn **Remote access (dial-up or VPN)**, nhấn **Next**:



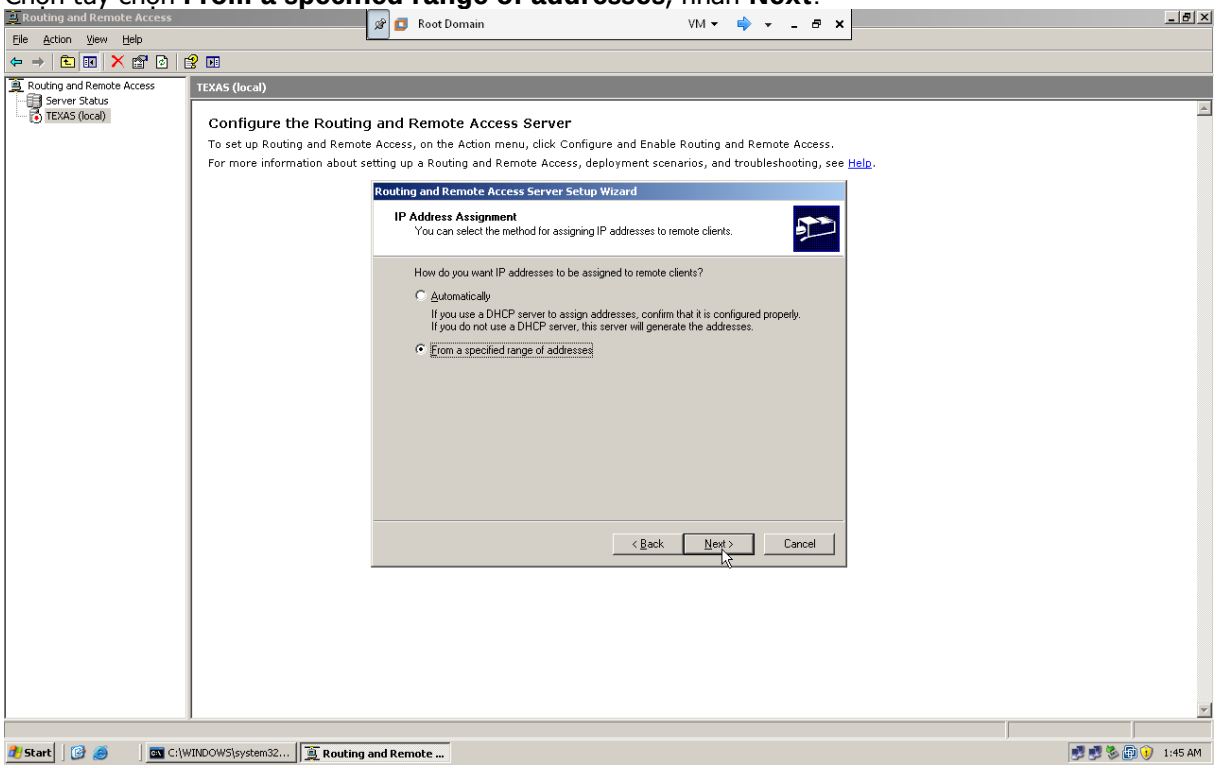
Chọn tùy chọn **VPN**, nhấn **Next:**



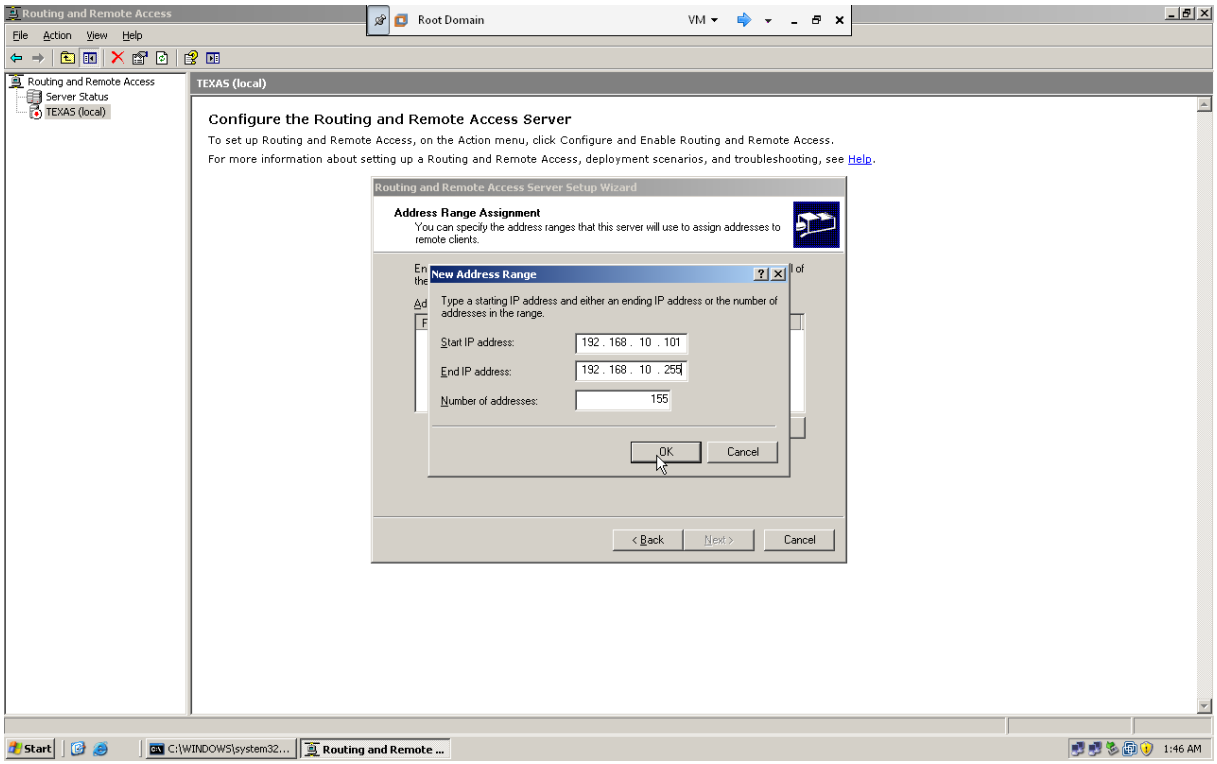
Chọn card mạng **Internet**, bỏ tùy chọn **Enable security on the selected interface by setting up static packet filters** sau đó nhấn **Next**:



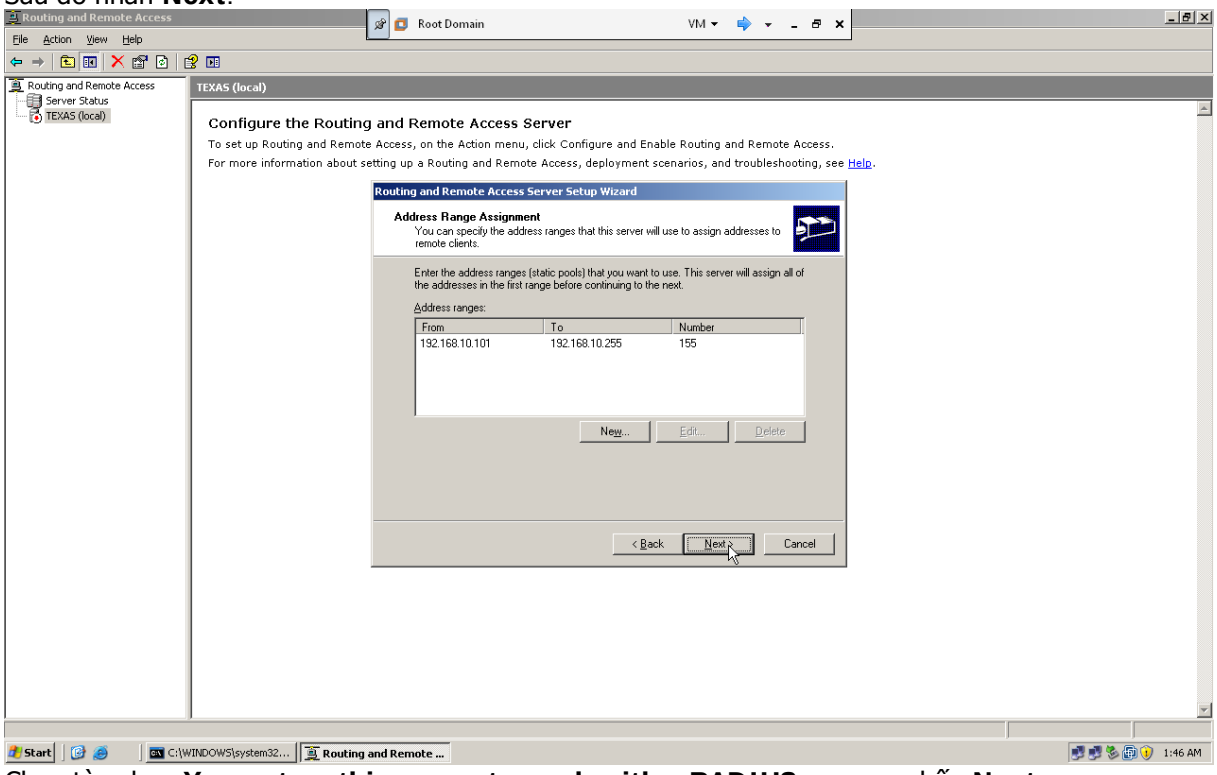
Chọn tùy chọn **From a specified range of addresses**, nhấn **Next**:



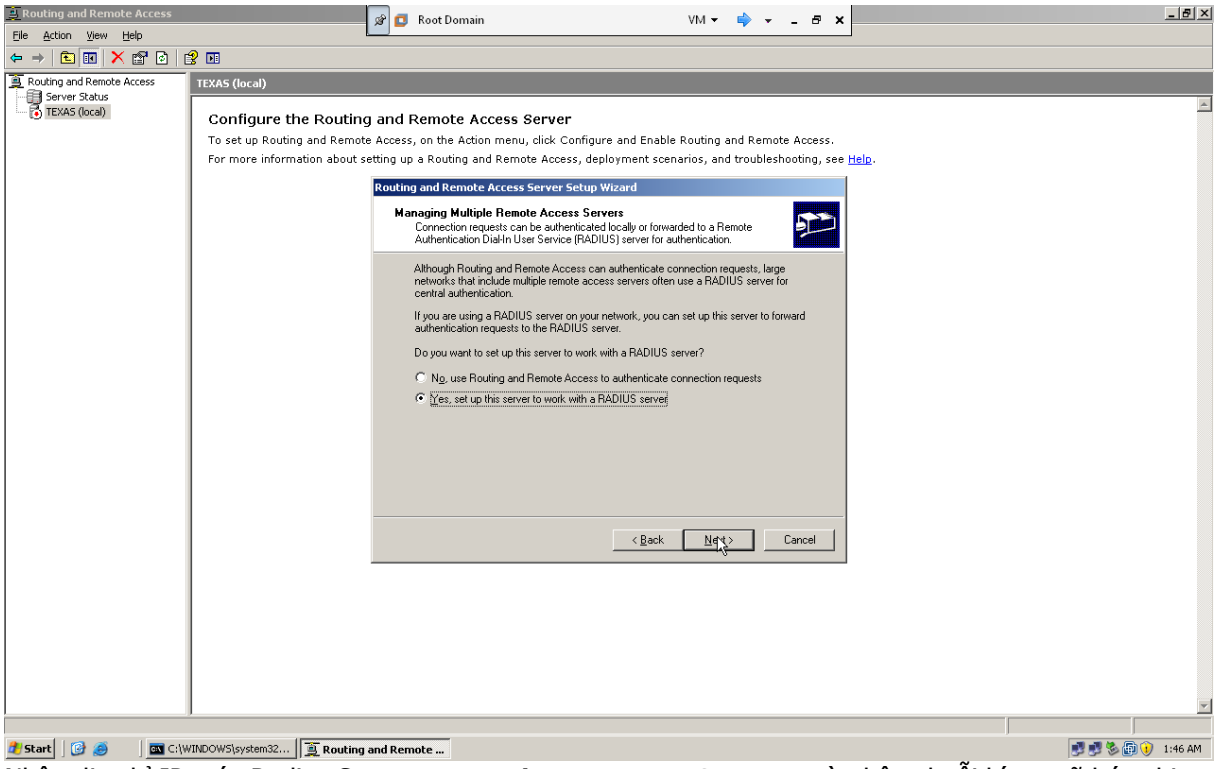
Tạo một dãy địa chỉ IP cho người dùng truy cập tài nguyên máy chủ thông qua kết nối VPN:



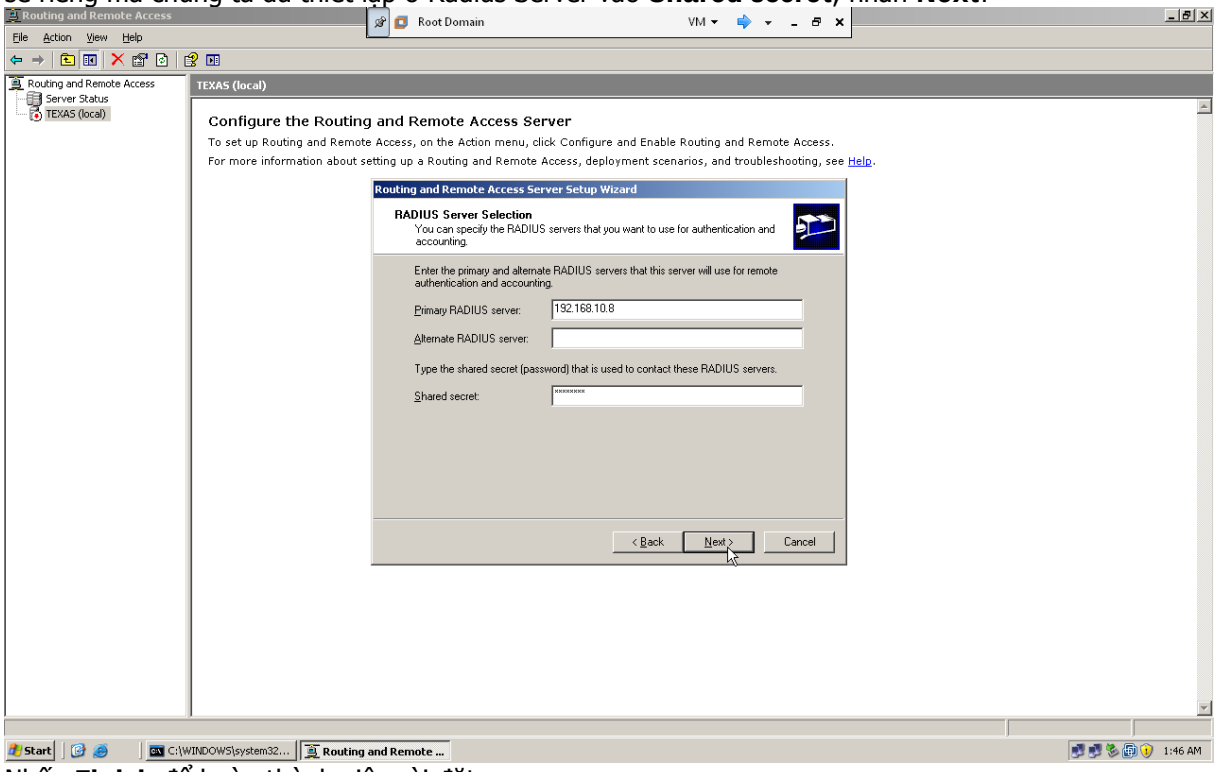
Sau đó nhấn **Next**:



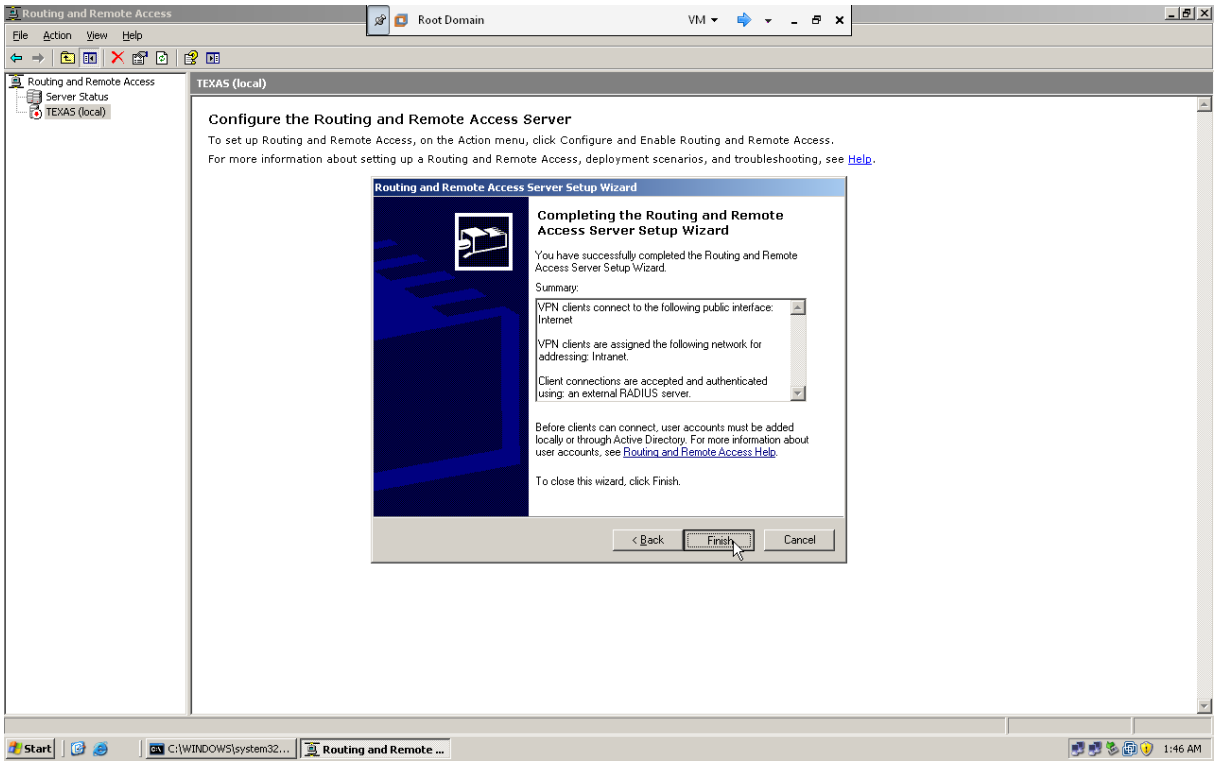
Chọn tùy chọn **Yes, set up this server to work with a RADIUS server**, nhấn **Next**:



Nhập địa chỉ IP máy Radius Server trong **Primary RADIUS server** và nhập chuỗi kí tự mã hóa chia sẽ riêng mà chúng ta đã thiết lập ở Radius Server vào **Shared secret**, nhấn **Next**:

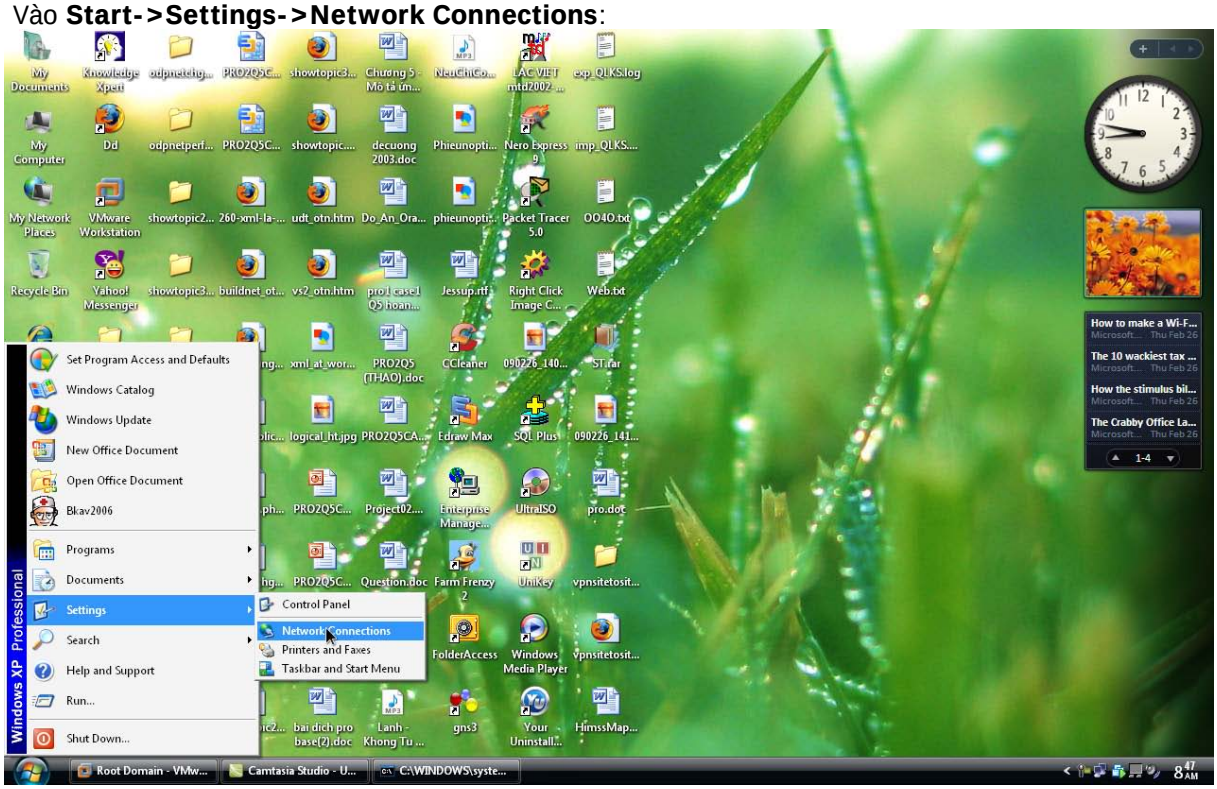


Nhấn **Finish** để hoàn thành việc cài đặt:

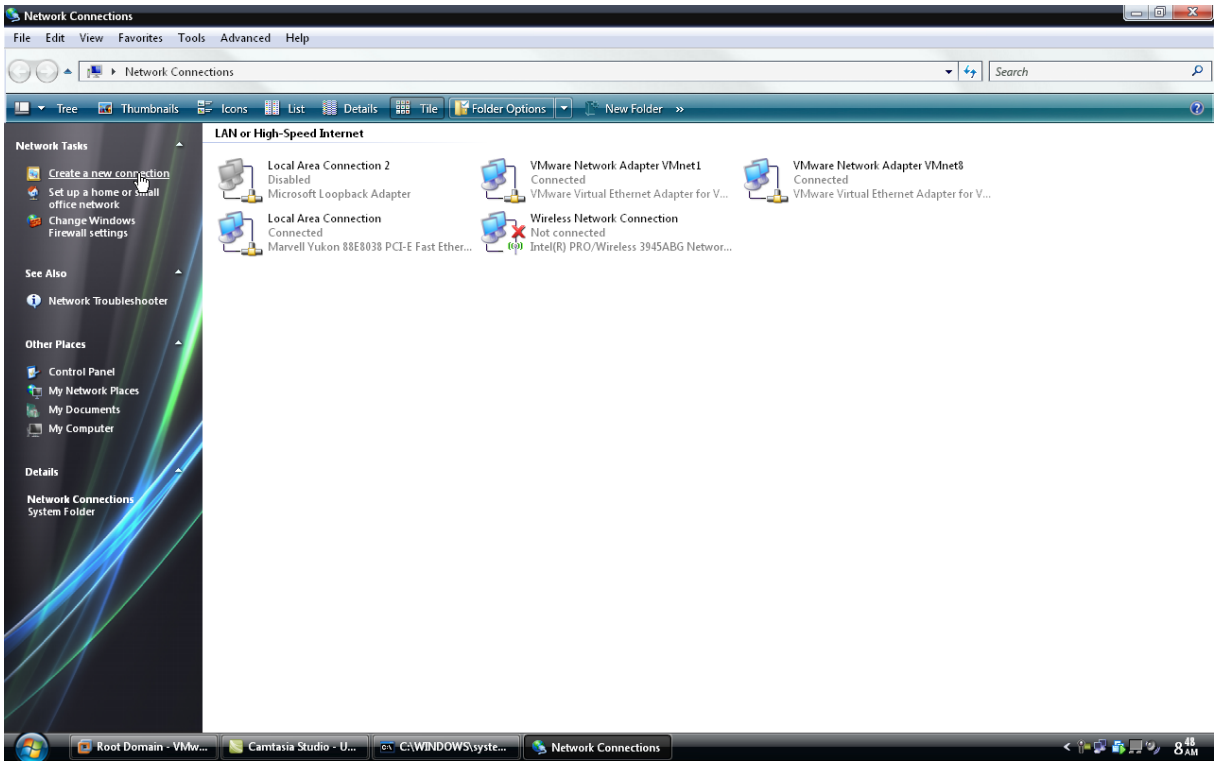


- **Trên máy Client:**

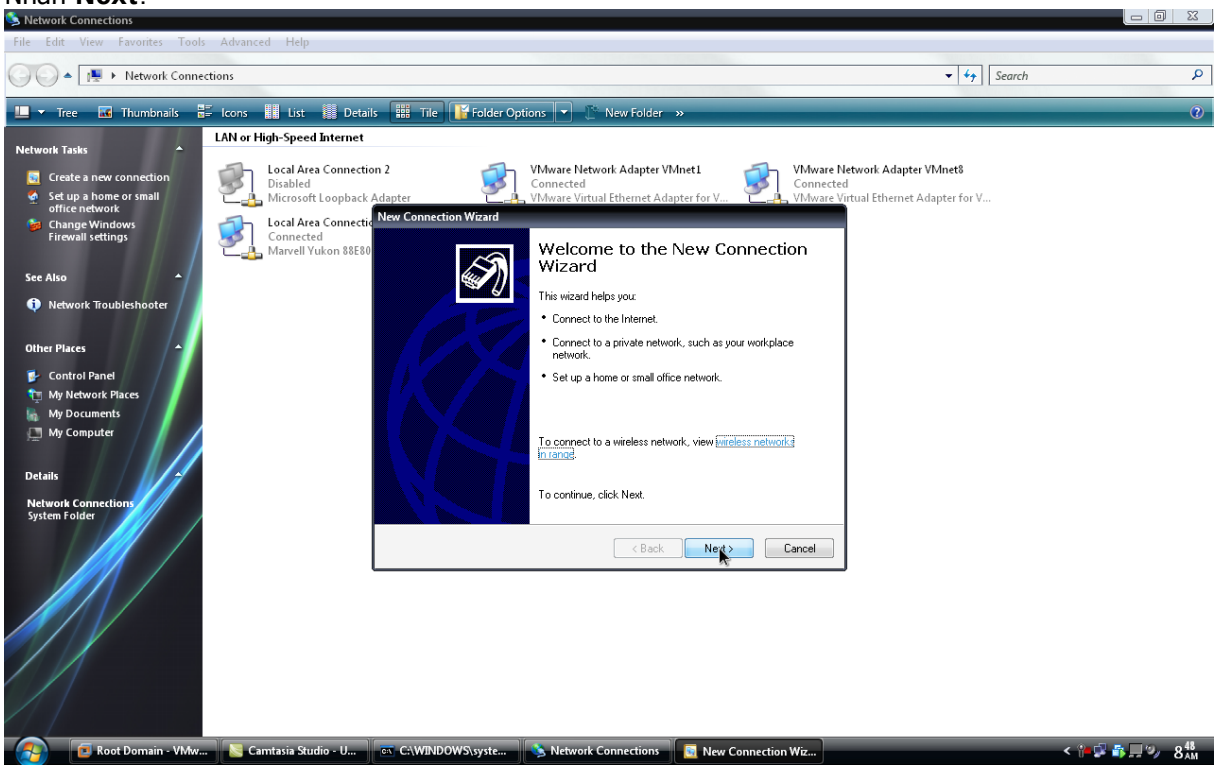
Vào **Start->Settings->Network Connections**:



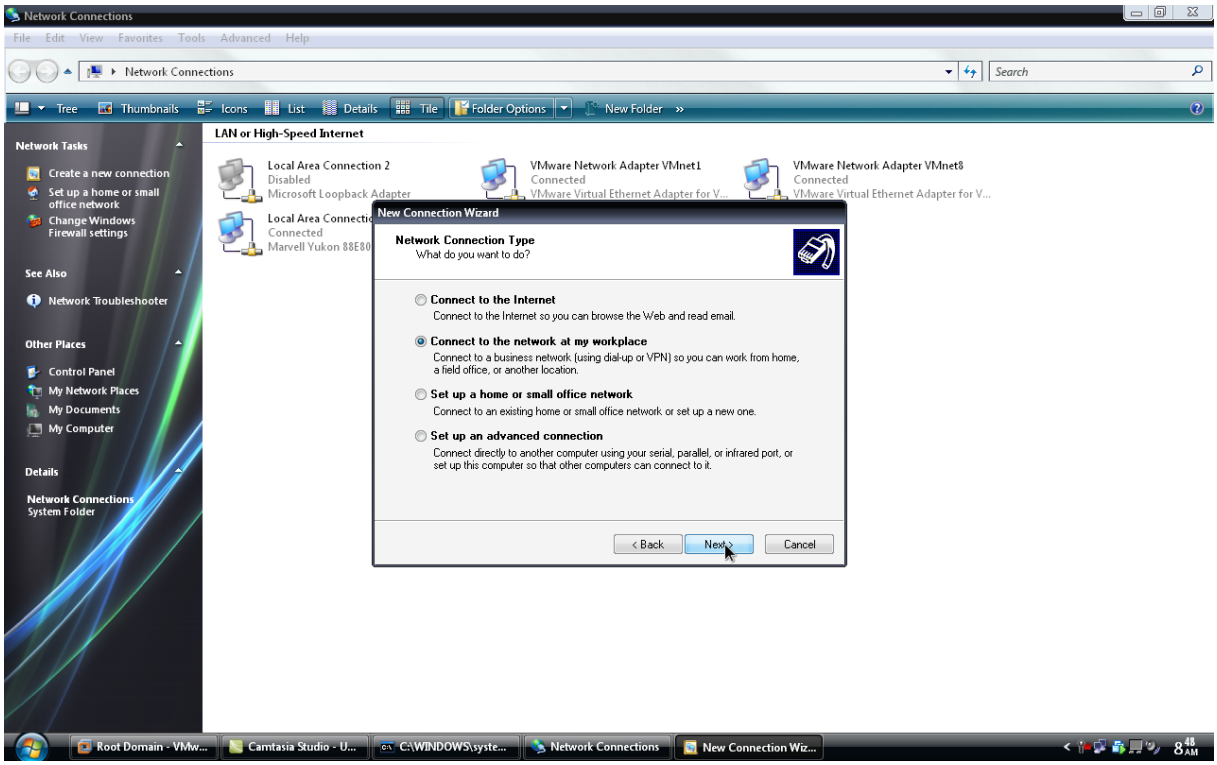
Tạo một kết nối mới bằng cách nhấn **Create new a connection**:



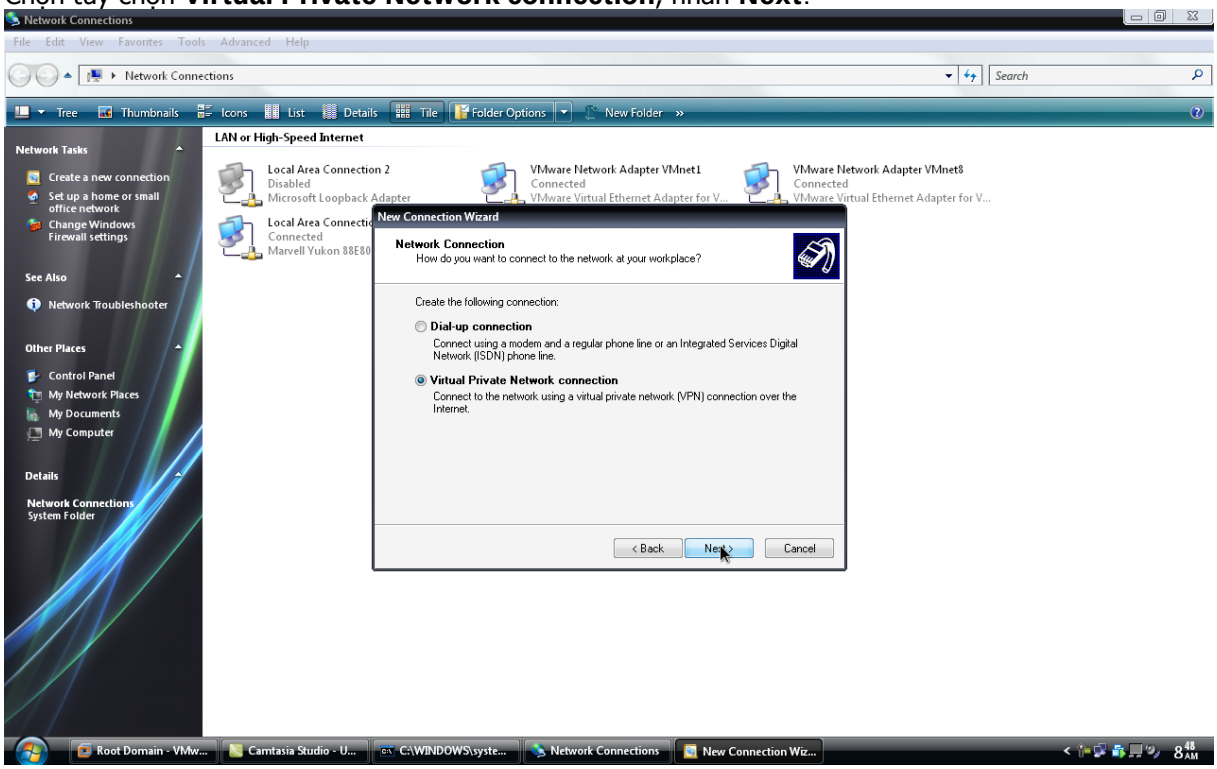
Nhấn **Next**:



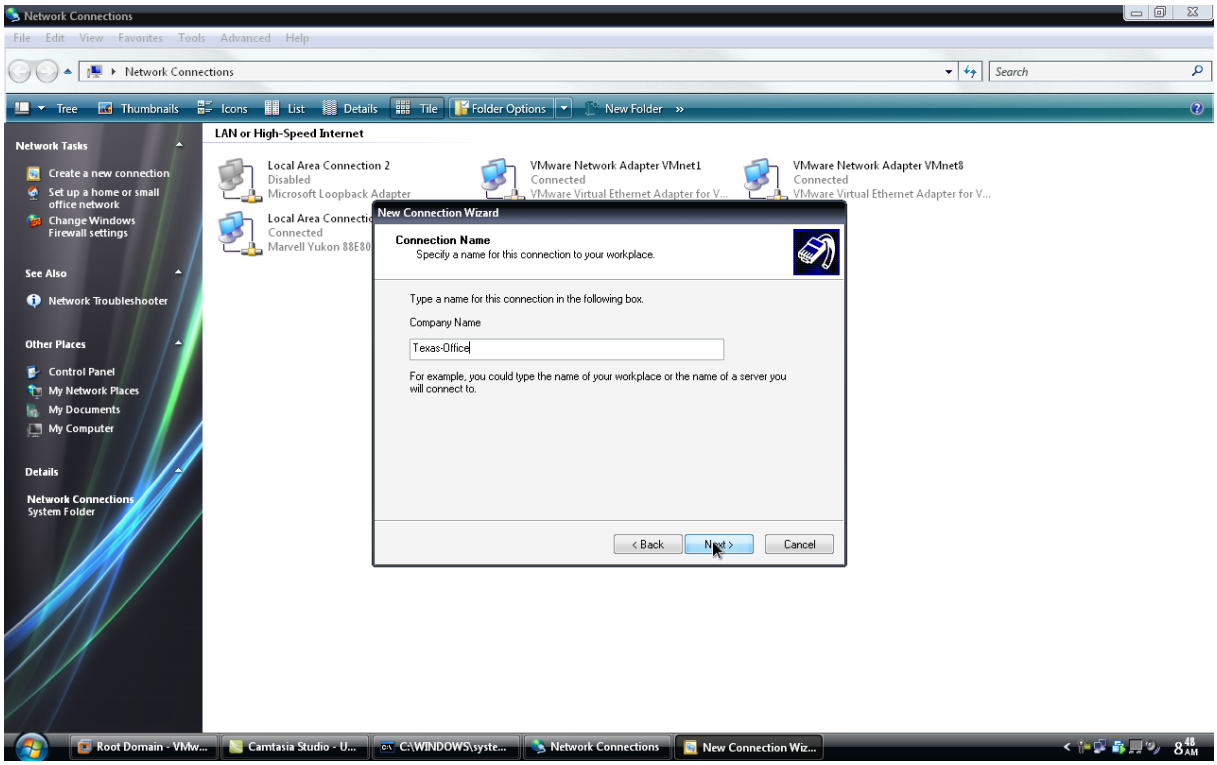
Chọn tùy chọn **Connect to the network at my workplace**, nhấn **Next**:



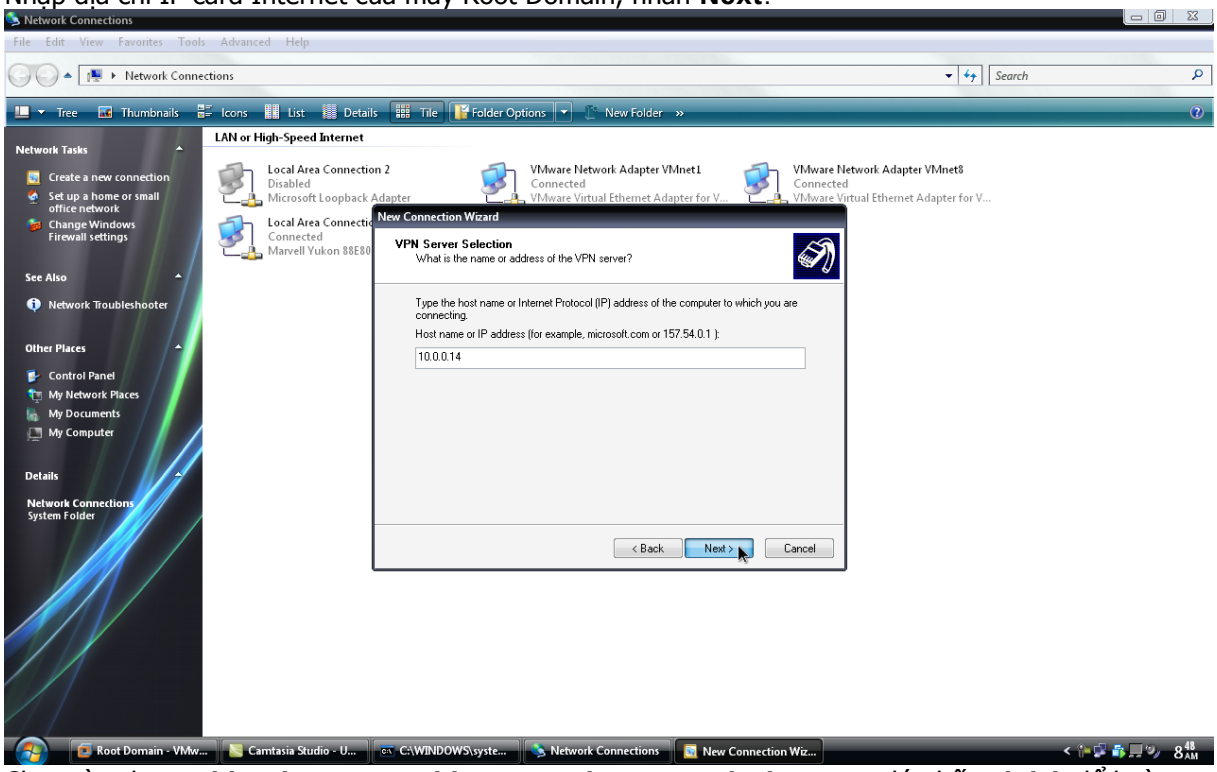
Chọn tùy chọn **Virtual Private Network connection**, nhấn **Next**:



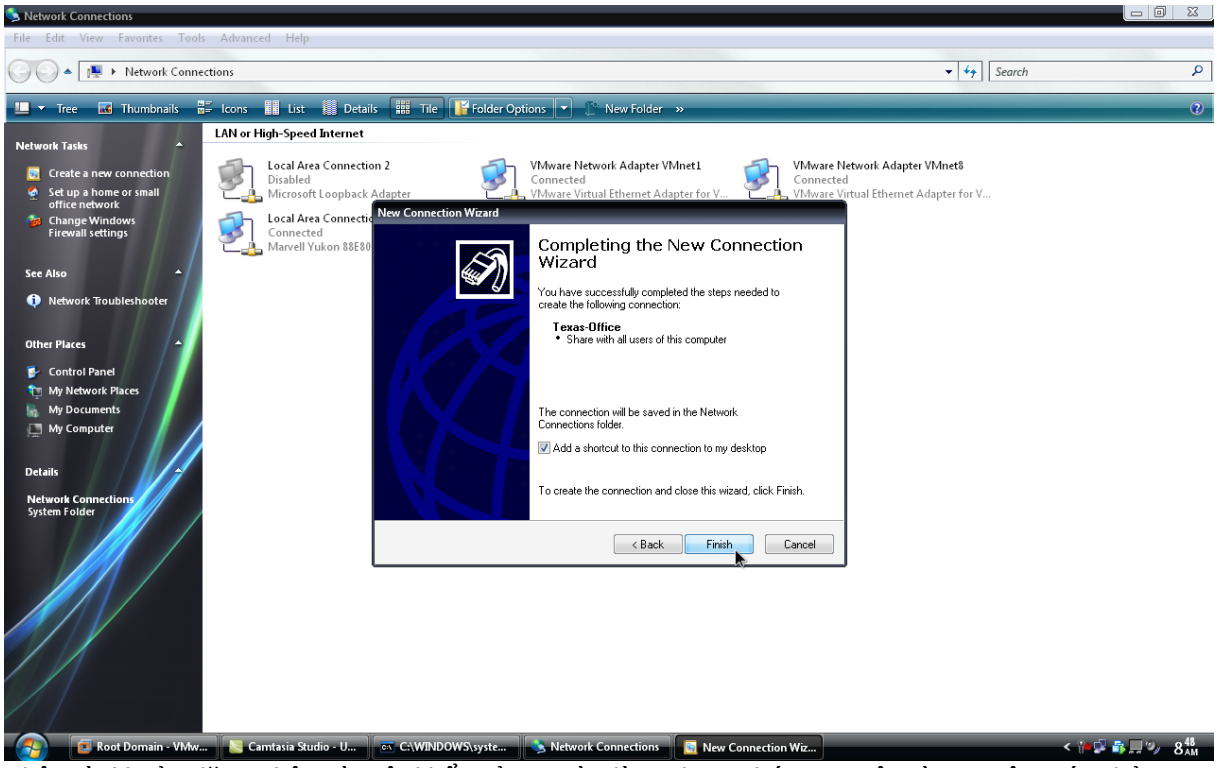
Nhập tên công ty cần kết nối truy cập tài nguyên thông qua VPN, nhấn **Next**:



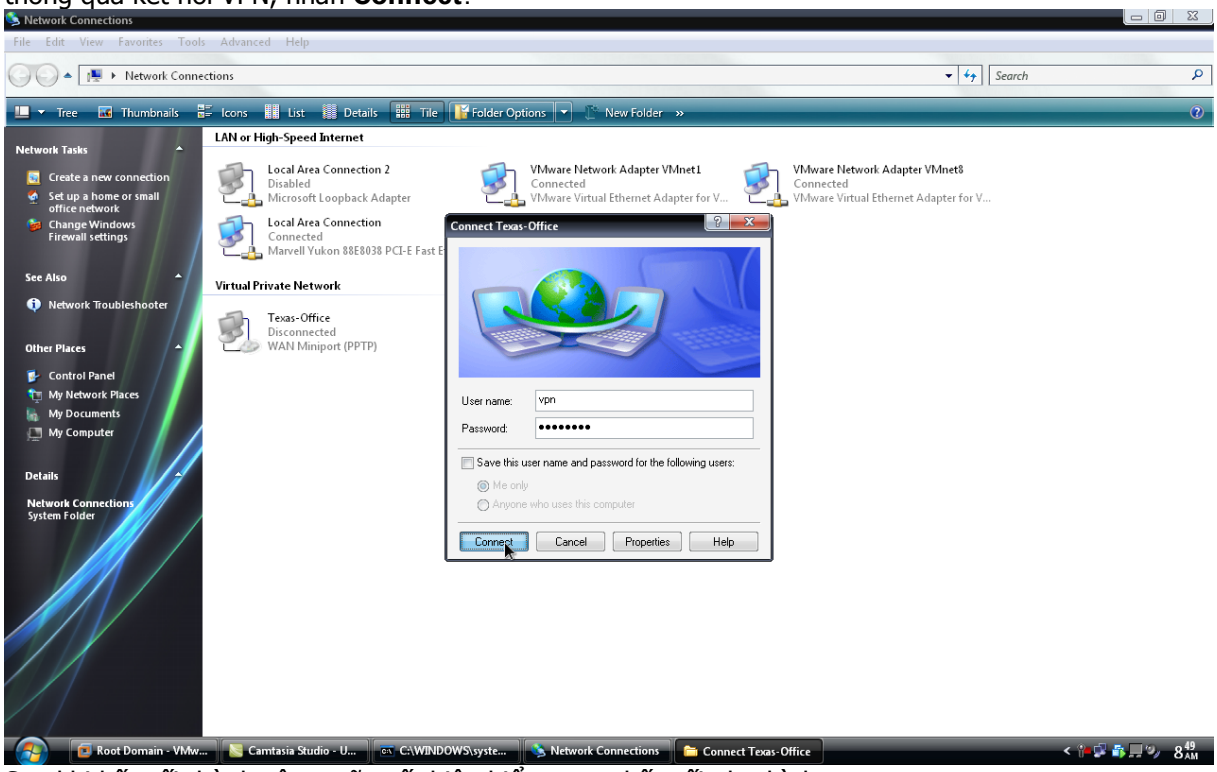
Nhập địa chỉ IP card Internet của máy Root Domain, nhấn **Next**:



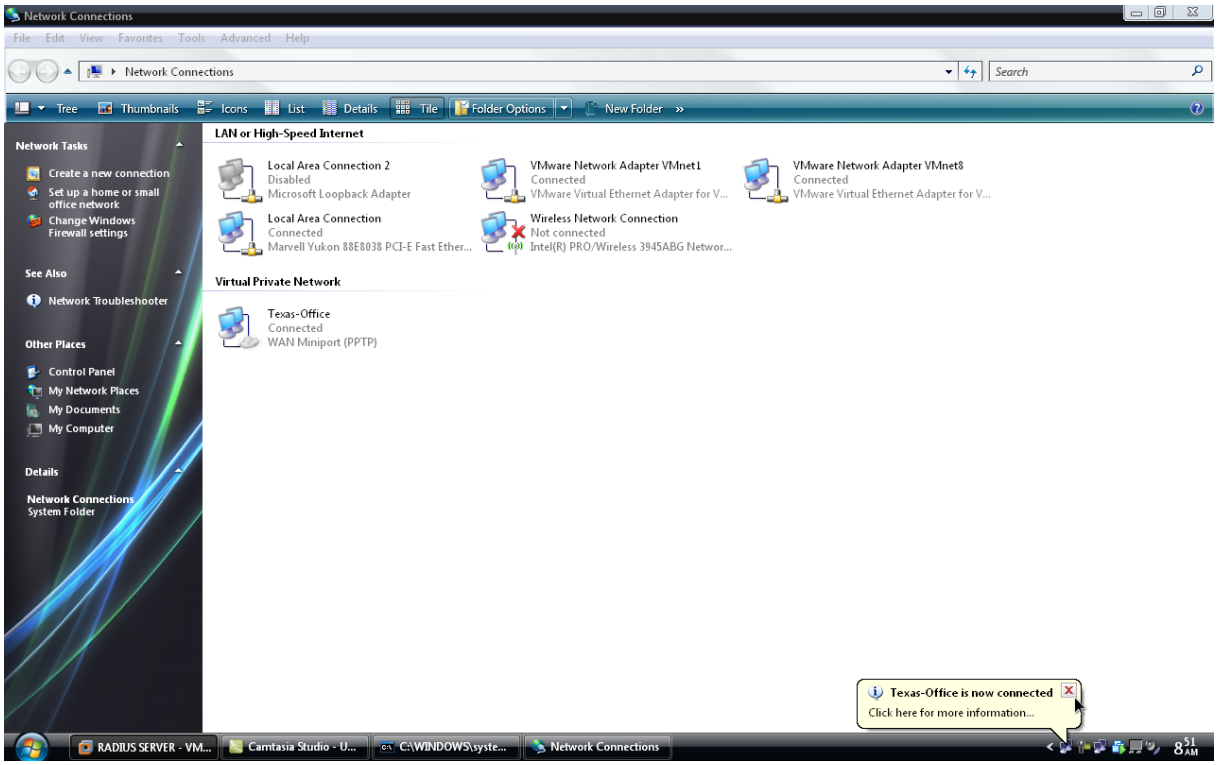
Chọn tùy chọn **Add a shortcut to this connection to my desktop** sau đó nhấn **Finish** để hoàn thành việc cài đặt một kết nối VPN:



Nhập tài khoản đăng nhập và mật khẩu của người dùng được phép truy cập tài nguyên máy chủ thông qua kết nối VPN, nhấn **Connect**:



Sau khi kết nối thành công, sẽ xuất hiện biểu tượng kết nối như hình sau:


Network Connections
File Edit View Favorites Tools Advanced Help
Network Connections
Search
Tree Thumbnails Icons List Details Tile Folder Options New Folder
Network Tasks
Create a new connection
Set up a home or small office network
Change Windows Firewall settings
See Also
Network Troubleshooter
Other Places
Control Panel
My Network Places
My Documents
My Computer
Details
Network Connections
System Folder
LAN or High-Speed Internet
Local Area Connection 2
Disabled
Microsoft Loopback Adapter
VMware Network Adapter VMnet1
Connected
VMware Virtual Ethernet Adapter for V...
VMware Network Adapter VMnet8
Connected
VMware Virtual Ethernet Adapter for V...
Local Area Connection
Connected
Marvell Yukon 88E8038 PCI-E Fast Ether...
Wireless Network Connection
Not connected
Intel(R) PRO/Wireless 3945ABG Networ...
Virtual Private Network
Texas-Office
Connected
WAN Miniport (PPTP)
Texas-Office is now connected
Click here for more information...
RADIUS SERVER - VM...
Camtasia Studio - U...
C:\WINDOWS\syste...
Network Connections
8:51 AM

Bài 7: ISA Server 2006

Mục tiêu bài học

Trong bài học này, chúng ta sẽ:

- Định nghĩa Firewall.
- Chức năng của Firewall.
- Cấu trúc của Firewall.
- Các thành phần của Firewall.
- Những hạn chế của Firewall.
- Cài đặt và cấu hình ISA 2006.

Khái niệm về Firewall

Bức tường lửa (Firewall) là hệ thống ngăn chặn việc truy nhập trái phép từ bên ngoài vào mạng.Hệ thống tường lửa thường bao gồm cả phần cứng và phần mềm.Tường lửa thực hiện việc lọc bỏ những địa chỉ không hợp lệ dựa theo các quy tắc hay chỉ tiêu định trước gọi là các luật.

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.

Chức năng cơ bản của Firewall

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.Cụ thể là:

- Cấm hoặc cho phép các dịch vụ mạng từ trong ra ngoài (từ Intranet ra Internet) hay từ ngoài cào trong (Internet ra Intranet).
- Kiểm soát địa chỉ và các cổng truy cập.
- Nó có khả năng kiểm soát được người sử dụng truy nhập thông qua các tệp tin xác thực
- Firewall hiện đại cho phép kiểm tra nội dung của gói tin trao đổi giữa mạng bên trong và mạng bên ngoài.
- Firewall có thể ngăn chặn được một phần tấn công từ bên ngoài vào mạng nội bộ.

Cấu tạo Firewall

Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

- Bộ lọc packet (packet-filtering router).
- Cổng ứng dụng (application-level gateway hay proxy server).
- Cổng mạch (circuite level gateway).

Bộ lọc packet (Packet filtering router)

a. 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 TCI/IP.Vì giao thức này làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ 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.Đó là:

- Địa chỉ IP nơi xuất phát (IP Source address)
- Địa chỉ IP nơi nhận (IP Destination address)
- Những giao thức 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...) đợc phép mới chạy đợc trên hệ thống mạng cục bộ.

b. 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 được bao gồm trong mỗi phần mềm router.Ngoài ra, bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng (vì nó hoạt động ở tầng IP), vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

c. Hạn chế

Việc định nghĩa các chế độ lọc package là một việc khá phức tạp; đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể có thể nhận trên mỗi trường.Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển. Do làm việc dựa trên header của các packet, rõ ràng là bộ lọc packet không kiểm soát được nôi dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

❖ **Cổng ứng dụng (Application-level Gateway)**

a. Nguyên lý

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng.Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service.Proxy service là các bộ code đặc biệt cài đặt trên gateway cho từng ứng dụng.Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua Firewall. Ngoài ra, proxy code có thể được lập cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Một cổng ứng dụng thường được coi như là một pháo đài (bastion host), bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài.Những biện pháp đảm bảo an ninh của một bastion host là:

- Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (Operating system).Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào Operating System, cũng như là đảm bảo sự tích hợp Firewall.
- Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.
- Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ như user password hay smart card.
- Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một sồ các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.
- Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

Mỗi proxy đều độc lập với các proxies khác trên bastion host.Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ môt proxy đang có vấn để.

b. Ưu điểm

Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.
Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.
Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.
Luật lệ lọc filltering cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

c. Hạn chế

Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy.Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phải là một bước thôi.Tuy nhiên, cũng đã có một số phần mềm client cho

phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phải cổng ứng dụng trên lệnh Telnet.

❖ **Cổng vòng (circuit-Level Gateway)**

Cổng vòng là một chức năng đặc biệt có thể thực hiện đợc bởi một cổng ứng dụng.Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

Cổng vòng đơn giản chuyển tiếp kết nối telnet qua Firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục Telnet nào.Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection).Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống Firewall, nó che dấu thông tin về mạng nội bộ.

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các quản trị mạng thật sự tin tưởng những ngời dùng bên trong.Ưu điểm lớn nhất là một bastion host có thể đợc cấu hình như là một hỗn hợp cung cấp Cổng ứng dụng cho những kết nối đến, và cổng vòng cho các kết nối đi.Điều này làm cho hệ thống bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp chức năng bức tường lửa để bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

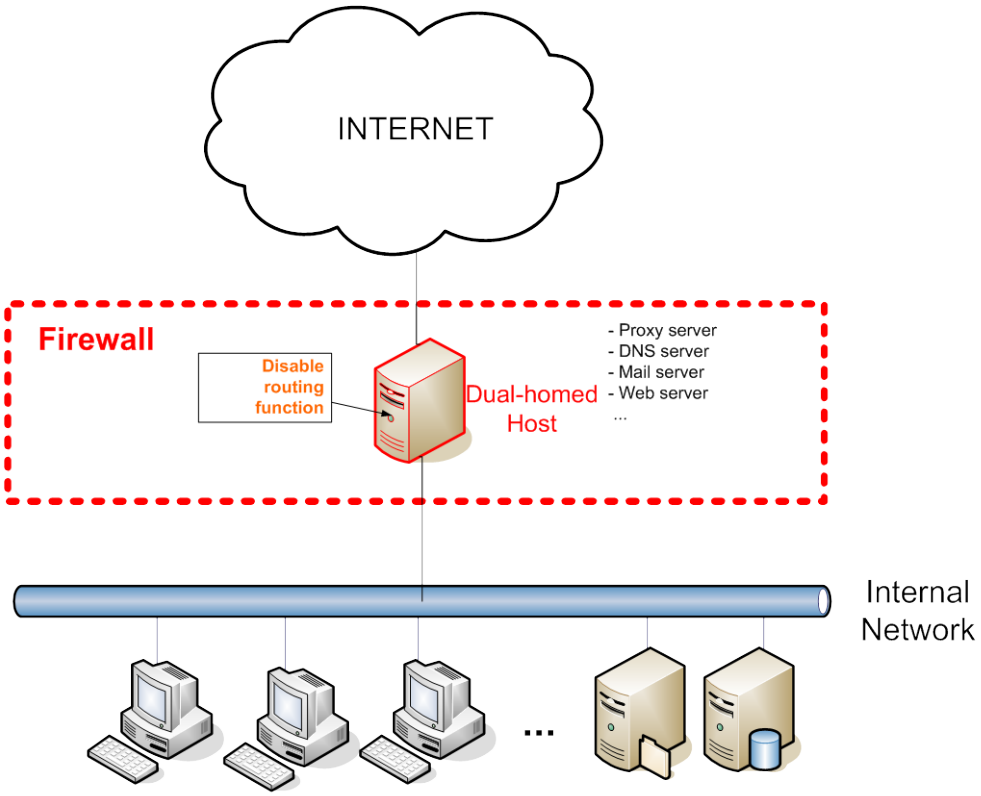
Kiến trúc của Firewall

1. Dual-Homed Host

Firewall kiến trúc kiểu Dual-homed host được xây dựng dựa trên máy tính dual-homed host. Một máy tính được gọi là dual-homed host nếu nó có ít nhất hai network interfaces, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau và như thế máy tính này đóng vai trò là Router mềm. Kiến trúc dual-homed host rất đơn giản. Dual-homed host ở giữa, một bên được kết nối với Internet và bên còn lại nối với mạng nội bộ (LAN).

Dual-homed host chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (proxy) chúng hoặc cho phép users đăng nhập trực tiếp vào dual-homed host. Mọi giao tiếp từ một host trong mạng nội bộ và host bên ngoài đều bị cấm, dual-homed host là nơi giao tiếp duy nhất.

- Phải disable chức năng routing của dual-homed host để cấm hoàn toàn lưu thông IP từ ngoài vào.
- Các hệ thống bên trong và bên ngoài dual-homed host chỉ có thể liên lạc với dual-homed host mà chúng không liên lạc trực tiếp được với nhau.
- Dual-homed host cung cấp dịch vụ thông qua proxy server hoặc login trực tiếp vào dual-homed host.

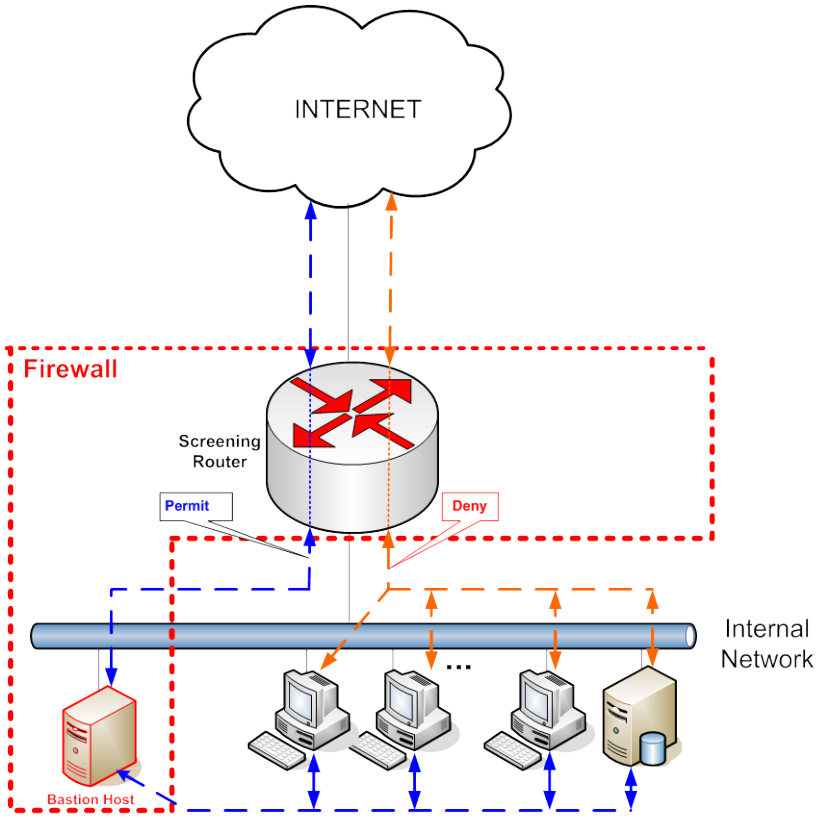


2. Screened Host

Screened Host có cấu trúc ngược lại với cấu trúc Dual-homed host.Kiến trúc này cung cấp các dịch vụ từ một host bên trong mạng nội bộ, dùng một Router tách rời với mạng bên ngoài.Trong kiểu kiến trúc này, bảo mật chính là phương pháp **Packet Filtering**.Bastion host được đặt bên trong mạng nội bộ.Packet Filtering được cài trên Router.Theo cách này, Bastion host là hệ thống duy nhất trong mạng nội bộ mà những host trên Internet có thể kết nối tới.
Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong Bastion host) mới được cho phép kết nối.Bất kỳ một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới host này.Vì thế Bastion host là host cần phải được duy trì ở chế độ bảo mật cao.Packet filtering cũng cho phép bastion host có thể mở kết nối ra bên ngoài.Cấu hình của packet filtering trên screening router như sau:
- Cho phép tất cả các host bên trong mở kết nối tới host bên ngoài thông qua một số dịch vụ cố định.
- Không cho phép tất cả các kết nối từ các host bên trong (cấm những host này sử dụng dịch proxy thông qua bastion host).
- Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau.
- Một số dịch vụ được phép đi vào trực tiếp qua packet filtering.
- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua proxy.

Bởi vì kiến trúc này cho phép các packet đi từ bên ngoài vào mạng bên trong, nó dường như là nguy hiểm hơn kiến trúc Dual-homed host, vì thế nó được thiết kế để không một packet nào có thể tới được mạng bên trong.Tuy nhiên trên thực tế thì kiến trúc dual-homed host đôi khi cũng có lỗi mà cho phép các packet thật sự đi từ bên ngoài vào bên trong (bởi vì những lỗi này hoàn toàn không biết trước, nó hầu như không được bảo vệ để chống lại những kiểu tấn công này.Hơn nữa, kiến trúc dualhomed host thì dễ dàng bảo vệ Router (là máy cung cấp rất ít các dịch vụ) hơn là bảo vệ các hostbên trong mạng.
Xét về toàn diện thì kiến trúc **Screened host** cung cấp độ tin cậy cao hơn và an toàn hơn kiến trúc **Dual-homed host**.
So sánh với một số kiến trúc khác, chẳng hạn như kiến trúc **Screened subnet** thì kiến trúc **Screened host** có một số bất lợi.Bất lợi chính là nếu kẻ tấn công tìm cách xâm nhập **Bastion Host** thì không có cách nào để ngăn tách giữa **Bastion Host** và các host còn lại bên trong mạng nội bộ.Router cũng có một số điểm yếu là nếu Router bị tổn thương, toàn bộ mạng sẽ bị tấn công.Vì lý do này mà **Sceened subnet** trở thành kiến trúc phổ biến nhất.

- Trong kiến trúc này chức năng bảo mật chính được cung cấp bởi chức năng packet filtering tại screening router.
- Packet filtering trên screening router được setup sao cho bastion host là máy duy nhất trong internal network mà các host trên internet có thể mở kết nối đến. Packet filtering cũng cho phép bastion host mở các kết nối (hợp pháp) ra bên ngòai (external network).
- Thường Packet filtering thực hiện các công việc như sau:
  [1]. Cho phép các internal hosts mở kết nối đến các host trên internet đối với 1 số dịch vụ được phép.
  [2]. Cấm tất cả kết nối từ các internal hosts
- Khi hacker đã tấn công được vào bastion host thì không còn một rào chắn nào cho các internal hosts.

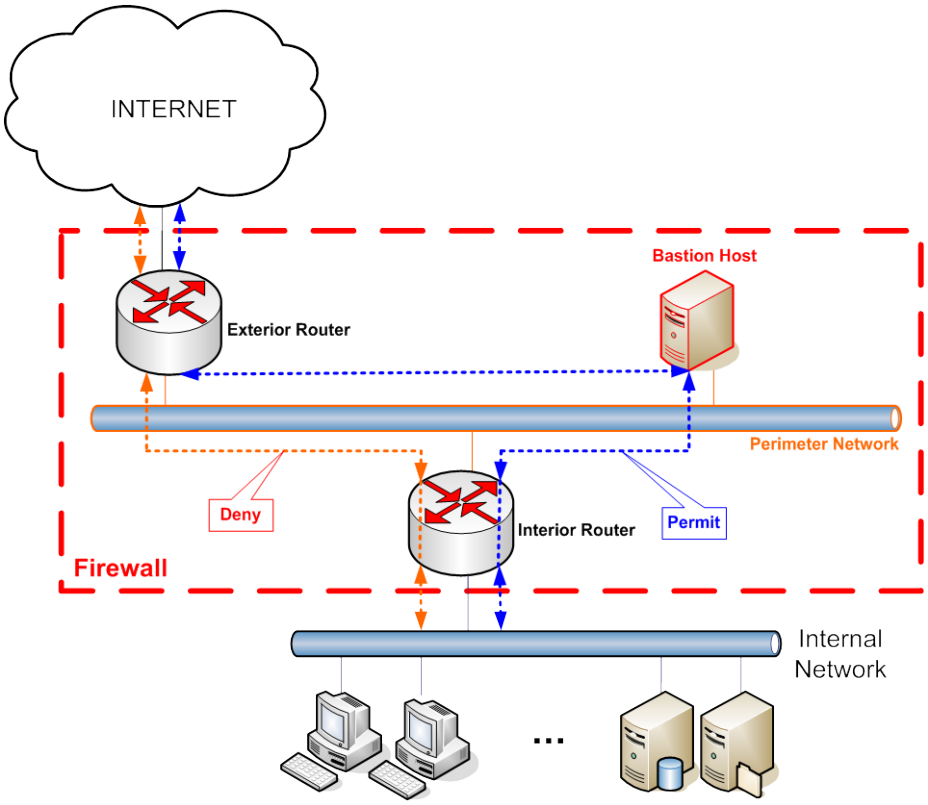


3. Screened Subnet

Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn *cho* **bastion host**, tách bastion host khỏi các host khác, phần nào tránh lây lan một khi bastion host bị tổn thương, người ta đưa ra kiến trúc firewall có tên là Sreened Subnet.
Kiến trúc **Screened subnet** dẫn xuất từ kiến trúc screened host bằng cách thêm vào phần an toàn: mạng ngoại vi (perimeter network) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách bastion host ra khỏi các host thông thường khác.Kiểu screened subnet đơn giản bao gồm hai screened router:
Router ngoài (External router còn gọi là access router): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (bastion host, interior router).Nó cho phép hầu hết những gì outbound từ mạng ngoại vi.Một số qui tắc packet filtering đặc biệt được cài đặt ở mức cần thiết đủ để bảo vệ bastion host và interior router vì bastion host còn là host được cài đặt an toàn ở mức cao.Ngoài các qui tắc đó, các qui tắc khác cần giống nhau giữa hai Router.
Interior Router (còn gọi là choke router): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi.Nó không thực hiện hết các qui tắc packet filtering của toàn bộ firewall.Các dịch vụ mà interior router cho phép giữa bastion host và mạng nội bộ, giữa bên ngoài và mạng nội bộ không nhất thiết phải giống nhau.Giới hạn dịch vụ giữa bastion host và mạng nội bộ nhằm giảm số lượng máy (số lượng dịch vụ trên các máy này) có thể bị tấn công khi bastion host bị tổn thương và thoả hiệp với bên ngoài.Chẳng hạn nên giới hạn các dịch vụ được phép giữa bastion host và mạng nội bộ như SMTP khi có Email từ bên ngoài vào, có lẽ chỉ giới hạn kết nối SMTP giữa bastion host và Email Server bên trong.

- Thêm 1 perimeter network để cô lập internal network với internet.Như vậy dù hacker đã tấn công được vào bastion host vẫn còn 1 rào chắn nữa phải vượt qua là interior router.Các lưu thông trong internal network được bảo vệ an toàn cho dù bastion đã bị "chiếm".
- Các dịch vụ nào ít tin cậy và có khả năng dễ bị tấn công thì nên để ở perimeter network.
- Bastion host là điểm liên lạc cho các kết nối từ ngoài vào như: SMTP; FTP; DNS.Còn đối với việc truy cập các dịch vụ từ internal clients đến các server trên internet thì được điều khiển như sau:
  +. Set up packet filtering trên cả hai exterior và interior router để cho phép internal clients truy cập các servers bên ngoài 1 cách trực tiếp.
  +. Set up proxy server trên bastion host để cho phép internal clients truy cập các servers bên ngoài 1 cách gián tiếp.

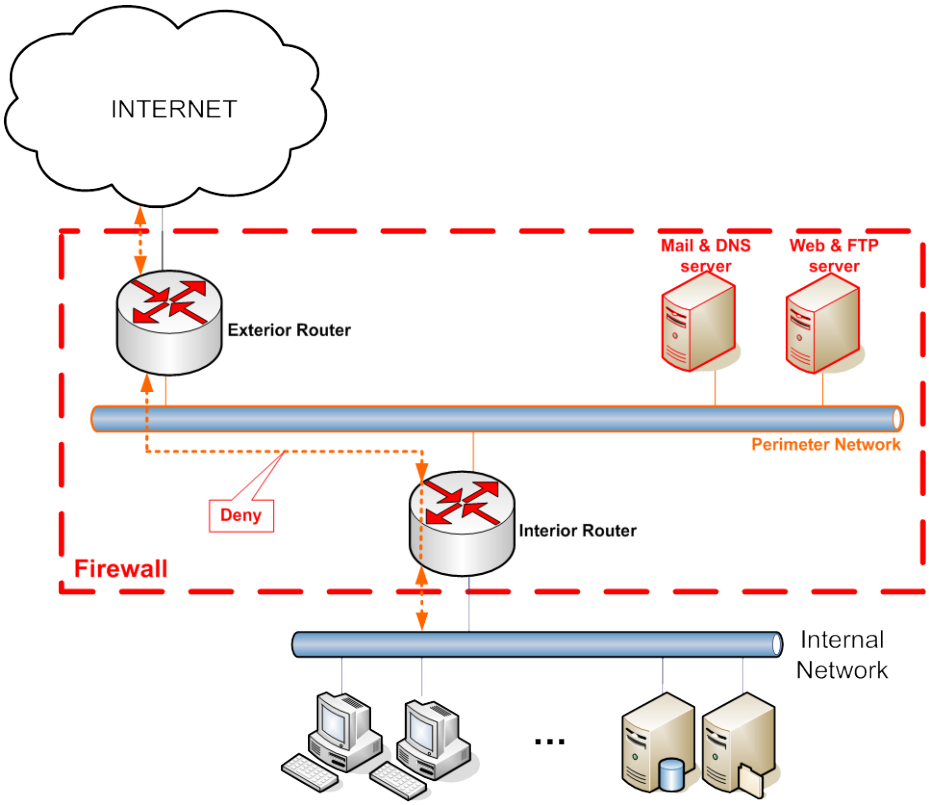
- Nên hạn chế các dịch vụ mà interior router cho phép giữa bastion host và internal net để giảm đi số máy có nguy cơ bị tấn công tiếp theo khi bastion đã bị "chiếm".
- Exterior router cho phép tất cả lưu thông từ perimeter net ra internet.Các packet filtering rules thiết yếu để bảo vệ cho các internal hosts là giống nhau trên tại exterior router và interior router.Thường exterior router thực hiện packet filtering rules tổng quát, chung chung, ít chi tiết hơn so với interior router (ngoại trừ những packet filtering rules thật thiết yếu thì giống nhau).Việc phát hiện và ngăn cấm sự giả mạo địa chỉ được thực hiện tại exterior router.



❖ **<u>Một số lưu ý về các kiến trúc firewall :</u>**

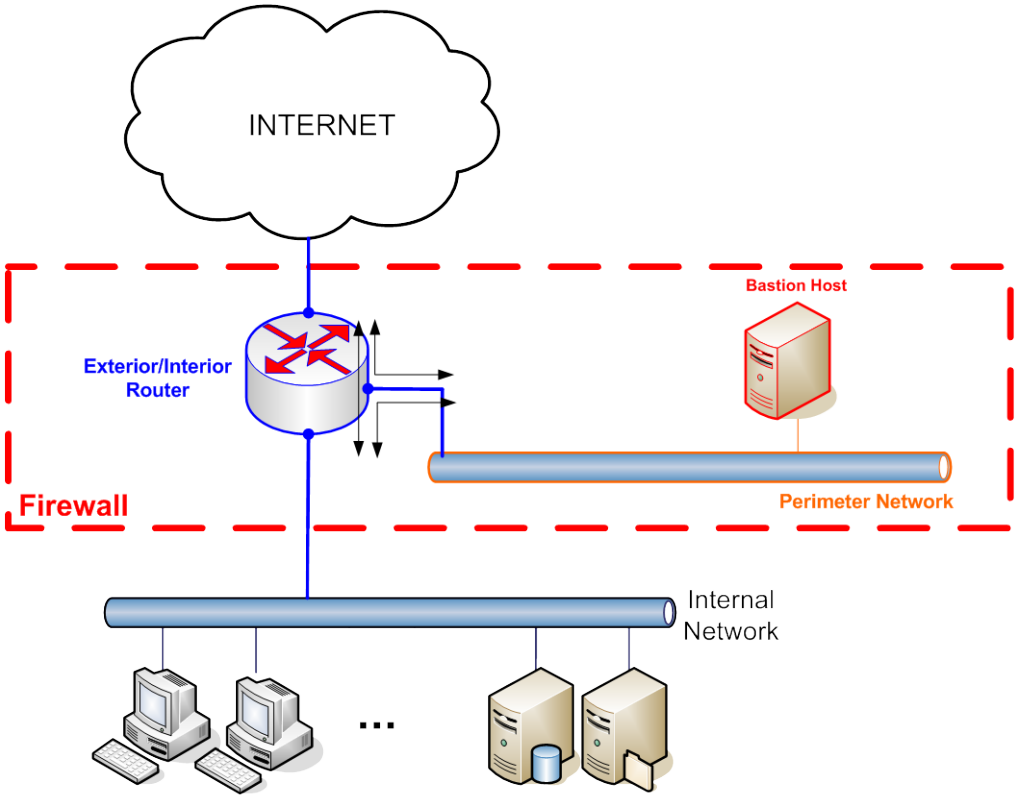
- **Các dạng kiến trúc firewall khác có thể dùng**

1. **Dùng nhiều Bastion Hosts**
   Để tăng performance, redundancy và tách biệt các servers và dữ liệu



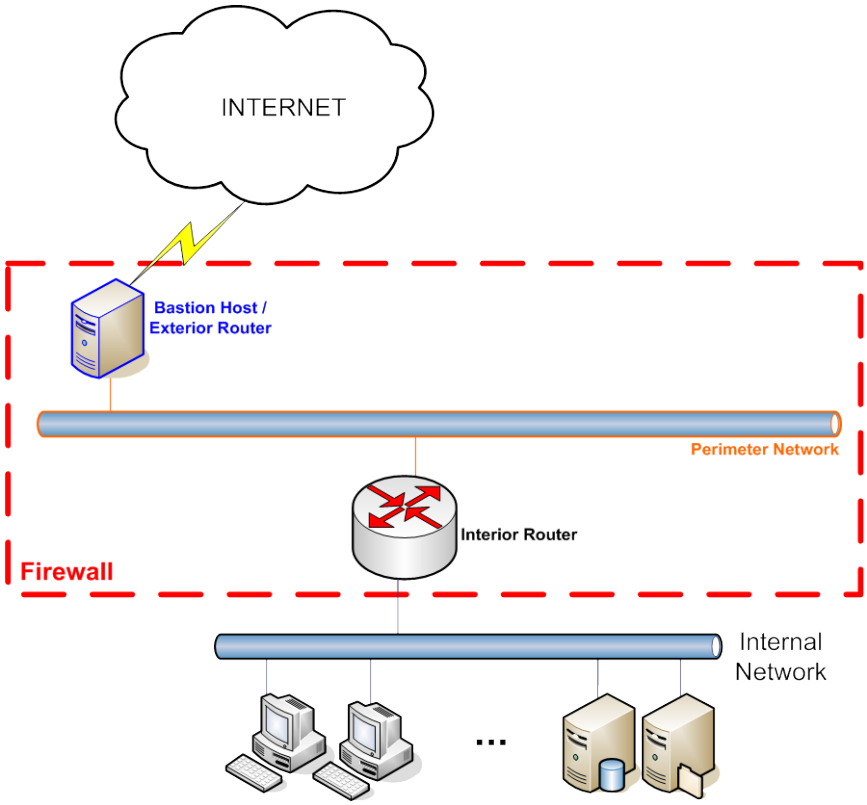
2. Ghép Interior Router với Exterior Router

- Router phải cho phép áp dụng các luật cho dòng packet đi vô và đi ra trên mỗi interface.

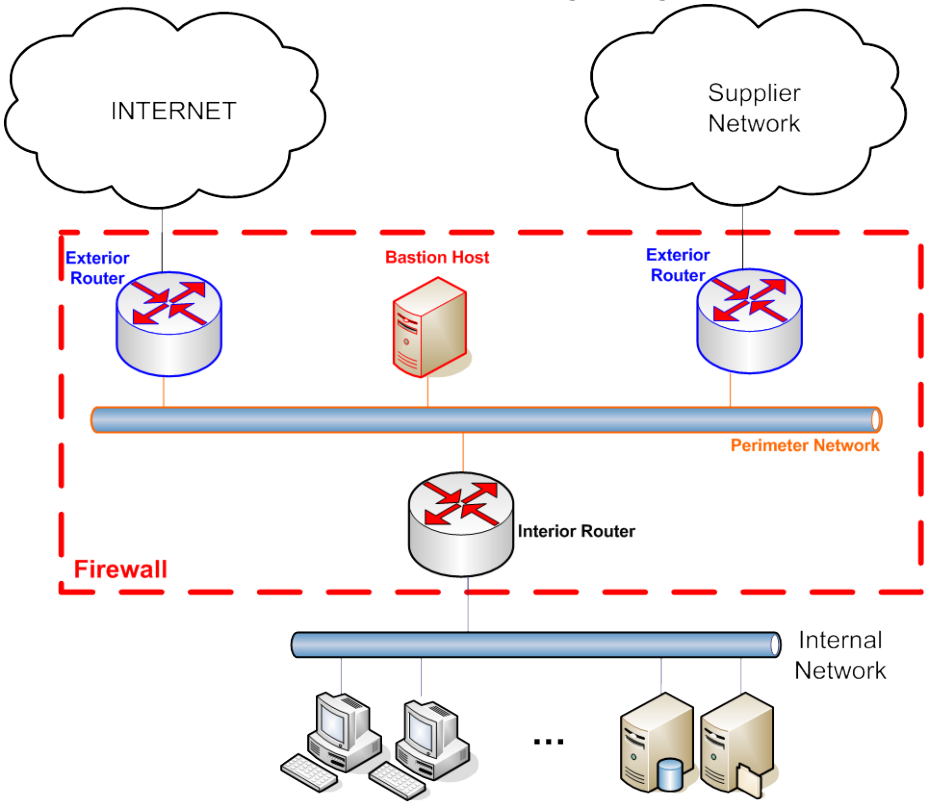


3. Ghép Bastion Host và Exterior Router

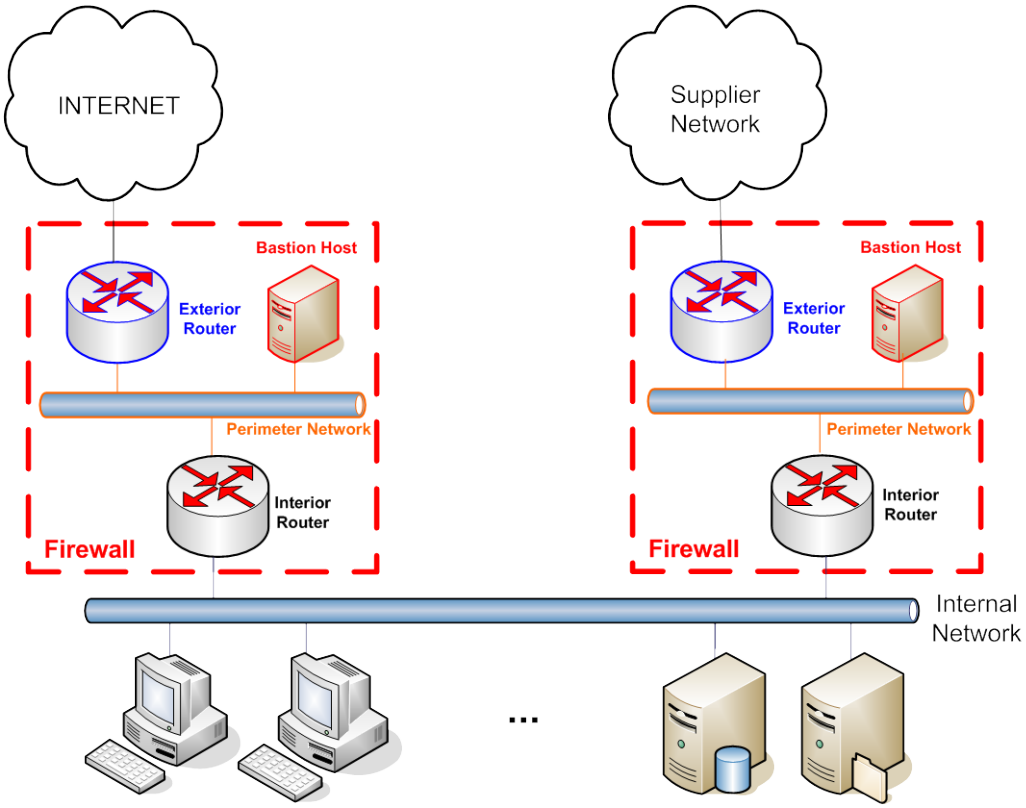
Thường được dùng trong trường hợp dùng kết nối PPP lên internet



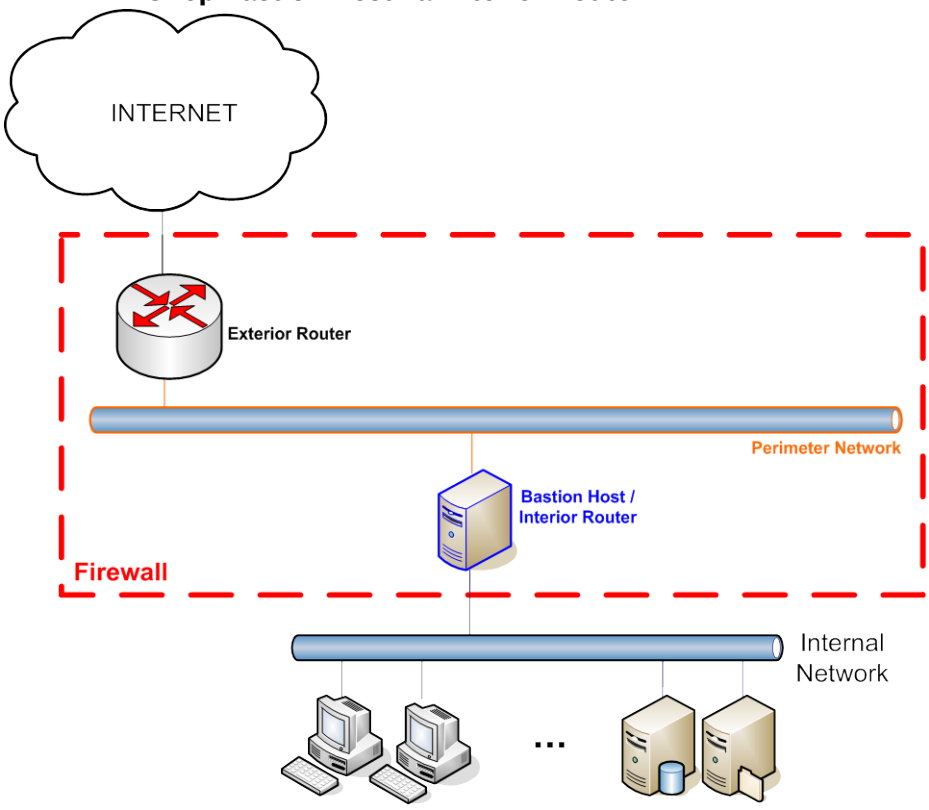
4. **Dùng nhiều Exterior Routers**
   Trong trường hợp có nhiều kết nối lên internet hoặc trường hợp 1 kết nối lên internet và các kết nối đến các mạng bên ngòai khác.



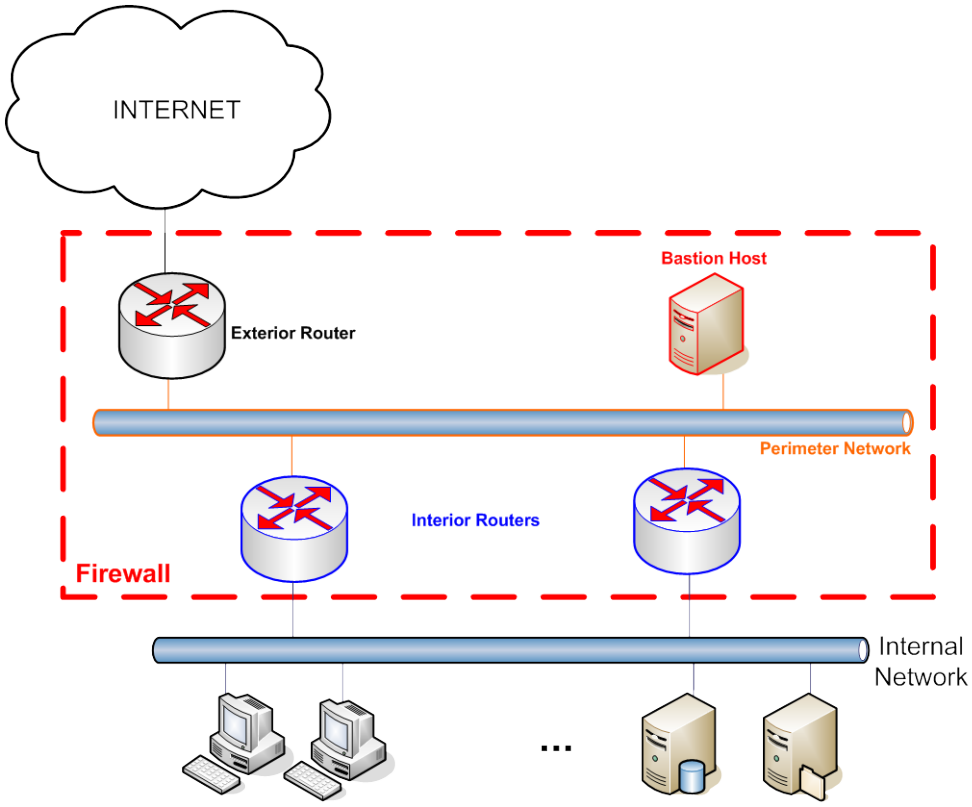
5. **Dùng nhiều Perimeter Networks**
   Dùng nhiều perimeter net để cung cấp đặc tính dư thừa (redundancy) cho hệ thống.



- **Các kiến trúc không nên dùng**
  1. **Ghép Bastion Host và Interior Router**



  2. **Dùng nhiều Interior Routers**



❖ **Một số lưu ý đối với máy giữ vai trò Bastion Host :**

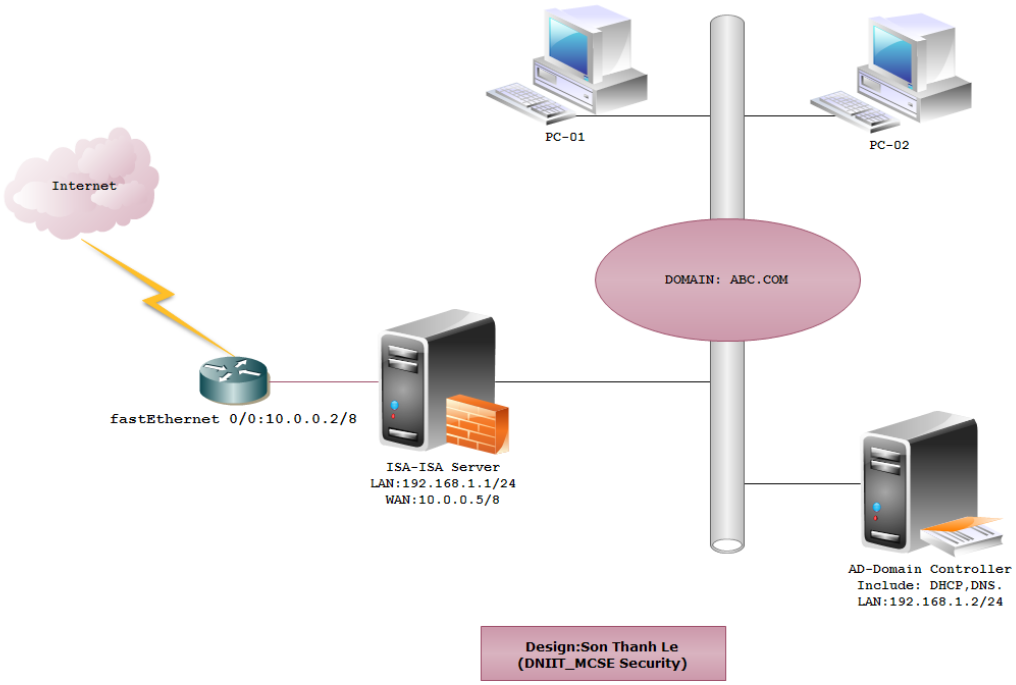
1. Cấm các user accounts
2. Tắt bỏ các dịch vụ không cần thiết
3. Cài đặt phiên bản hệ điều hành "gọn gàng & sạch sẽ" nhất có thể được
4. Sửa tất cả các lỗi hệ thống
5. System logs
6. Tắt bỏ chức năng routing

Giới thiệu ISA Server

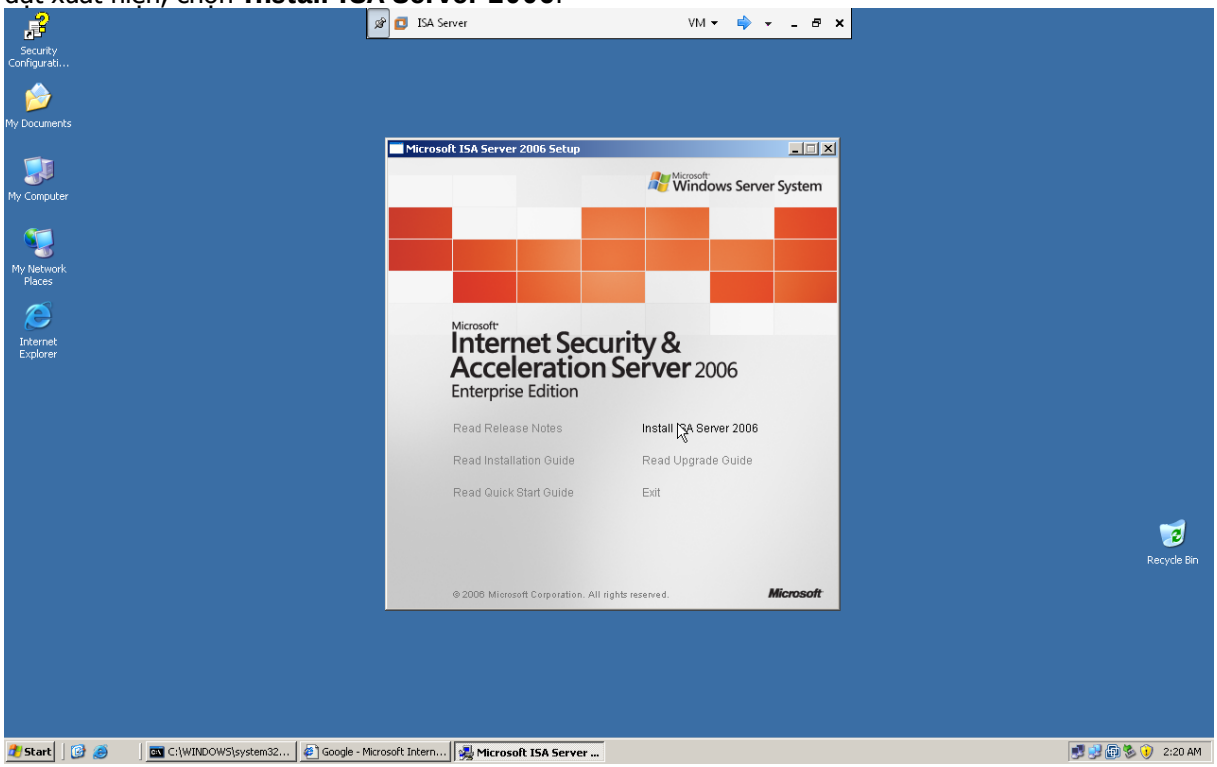
Microsoft Internet Security and Acceleration Sever (ISA Server) là phần mềm share internet của hãng phần mềm nổi tiếng Microsoft, là bản nâng cấp duy nhất (tính đến thời điểm này) từ phần mềm MS Proxy Server 2.0.Có thể nói đây là một phần mềm share internet khá hiệu quả, ổn định, dễ cấu hình, firewall tốt, nhiều tính năng cho phép bạn cấu hình sao cho tương thích với mạng LAN của bạn.Tốc độ nhanh nhờ chế độ cache thông minh, với tính năng lưu Cache vào RAM (Random Access Memory), giúp bạn truy xuất thông tin nhanh hơn, và tính năng Schedule Cache (Lập lịch cho tự động download thông tin trên các WebServer lưu vào Cache và máy con chỉ cần lấy thông tin trên các Webserver đó bằng mạng LAN).

Cài đặt và quản trị ISA Server 2006

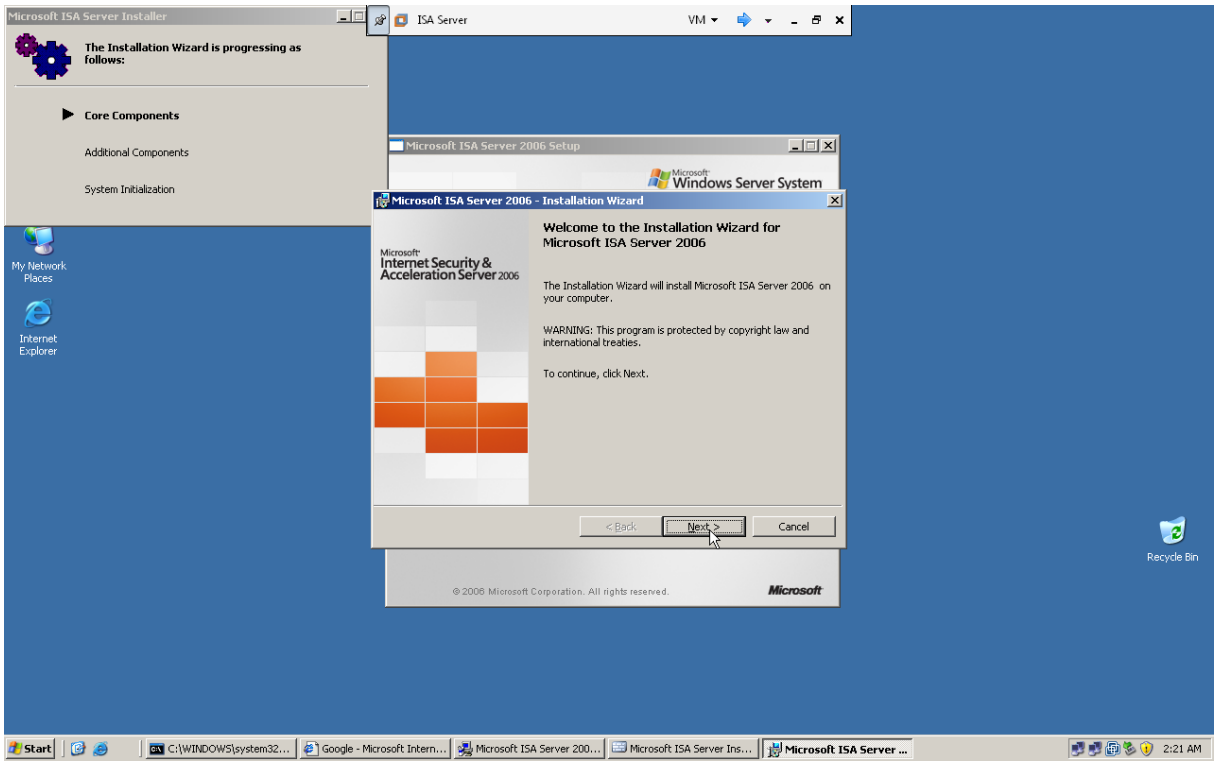
Mô hình triển khai ISA Server 2006 như sau:



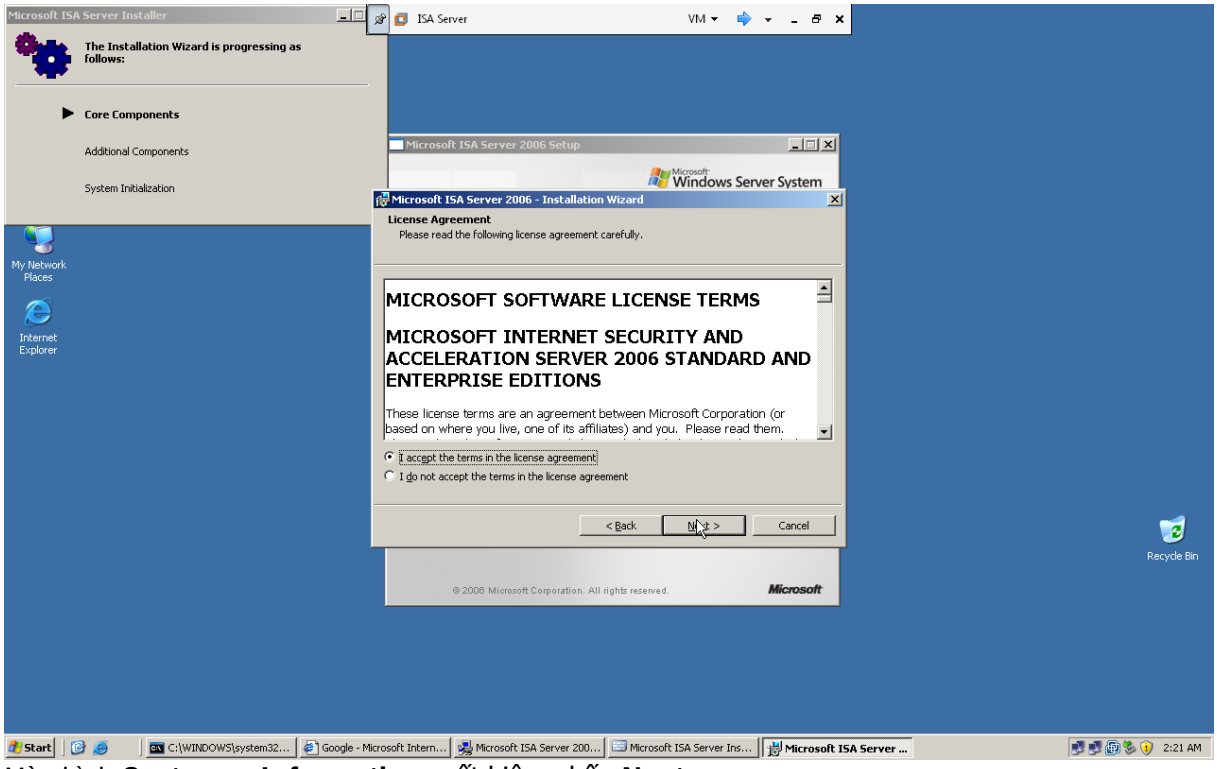
Bỏ đĩa cài đặt Microsoft ISA Server 2006 Enterprise Edition vào, chạy tập tin Setup.exe, màn hình cài đặt xuất hiện, chọn **Install ISA Server 2006**.



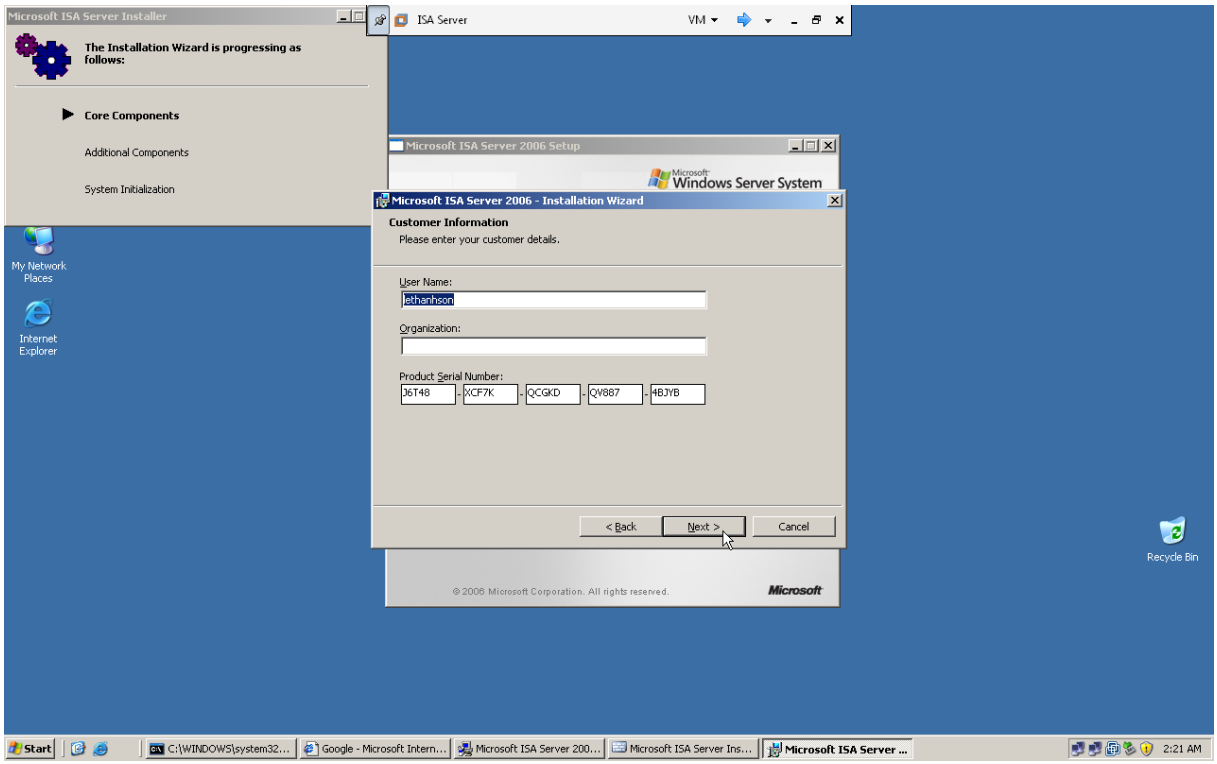
Màn hình **Microsoft ISA Server 2006-Installation Wizard** xuất hiện, nhấn **Next**:



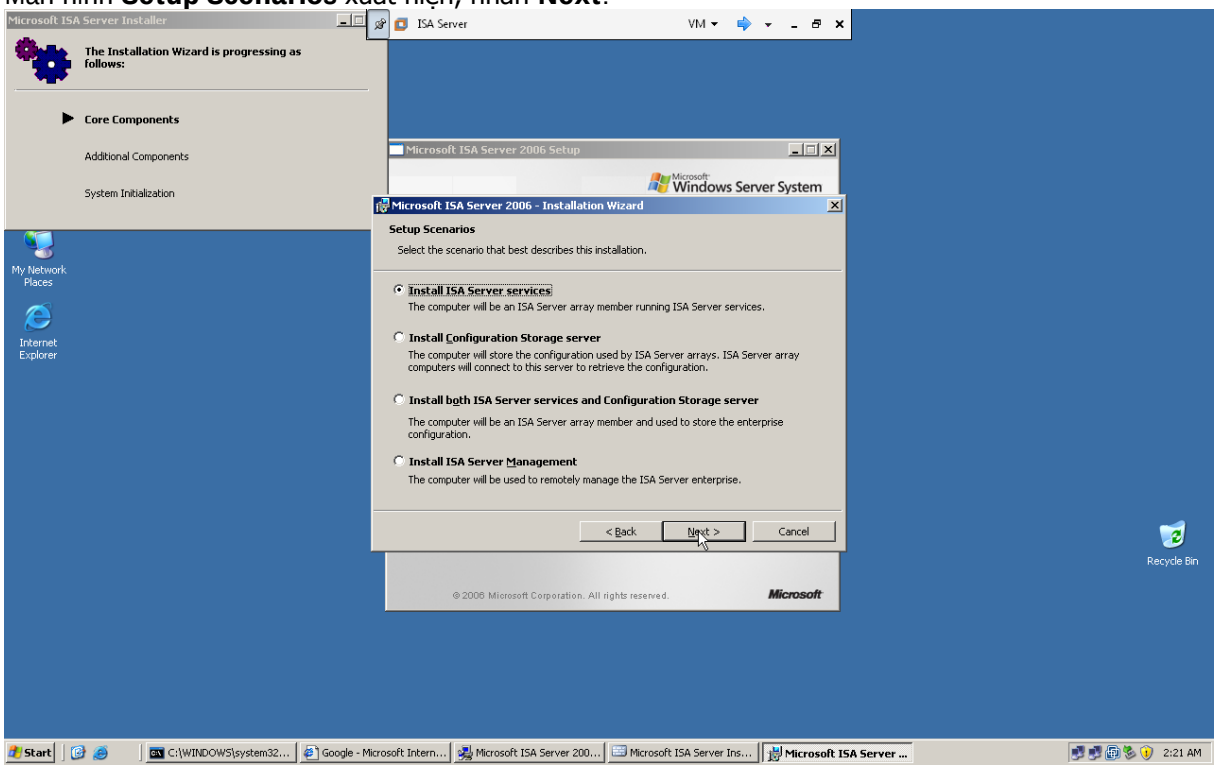
Màn hình **License Agreement** xuất hiện, chọn **I accept the items in the license agreement**, nhấn **Next**:



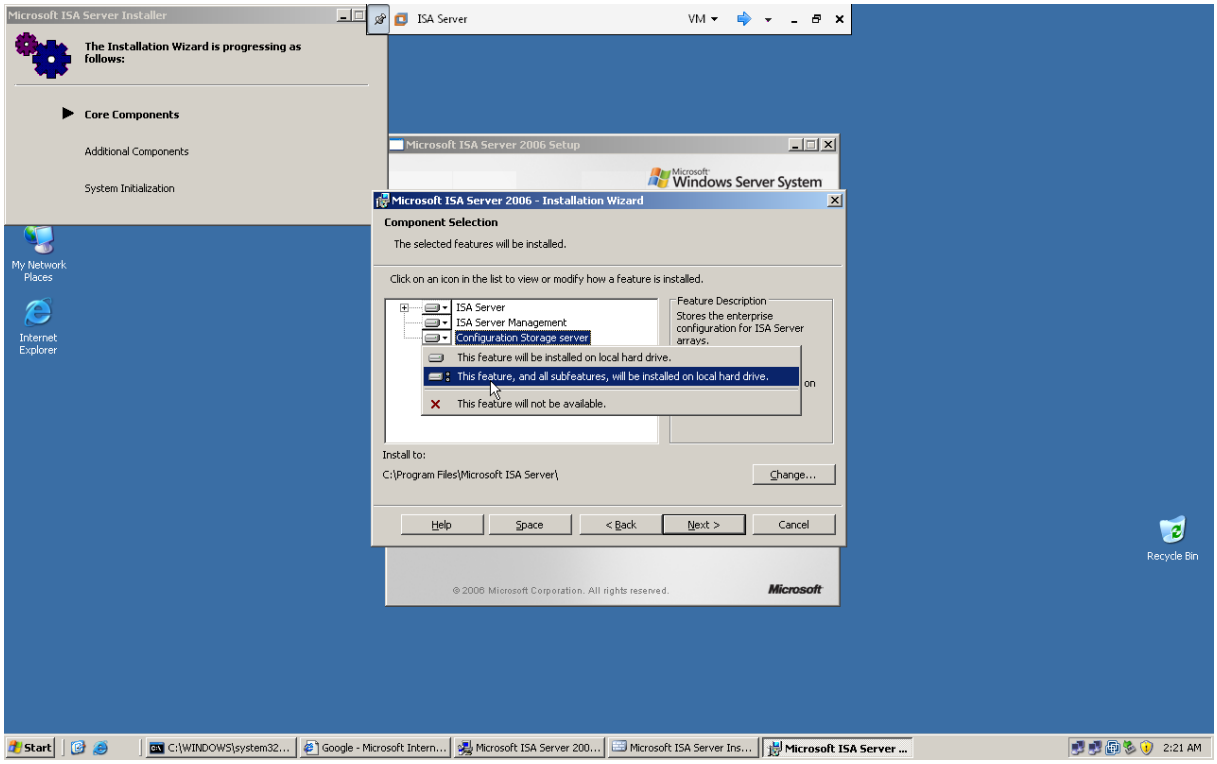
Màn hình **Customer Information** xuất hiện, nhấn **Next**:



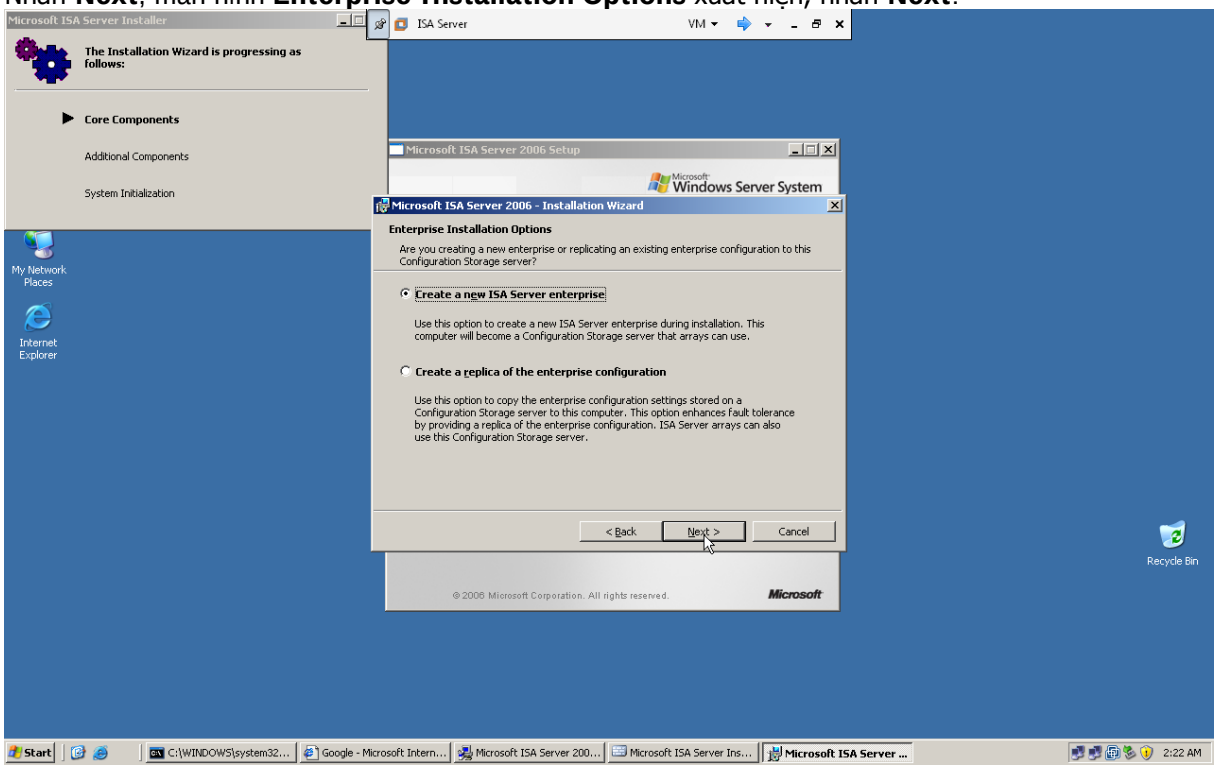
Màn hình **Setup Scenarios** xuất hiện, nhấn **Next**:



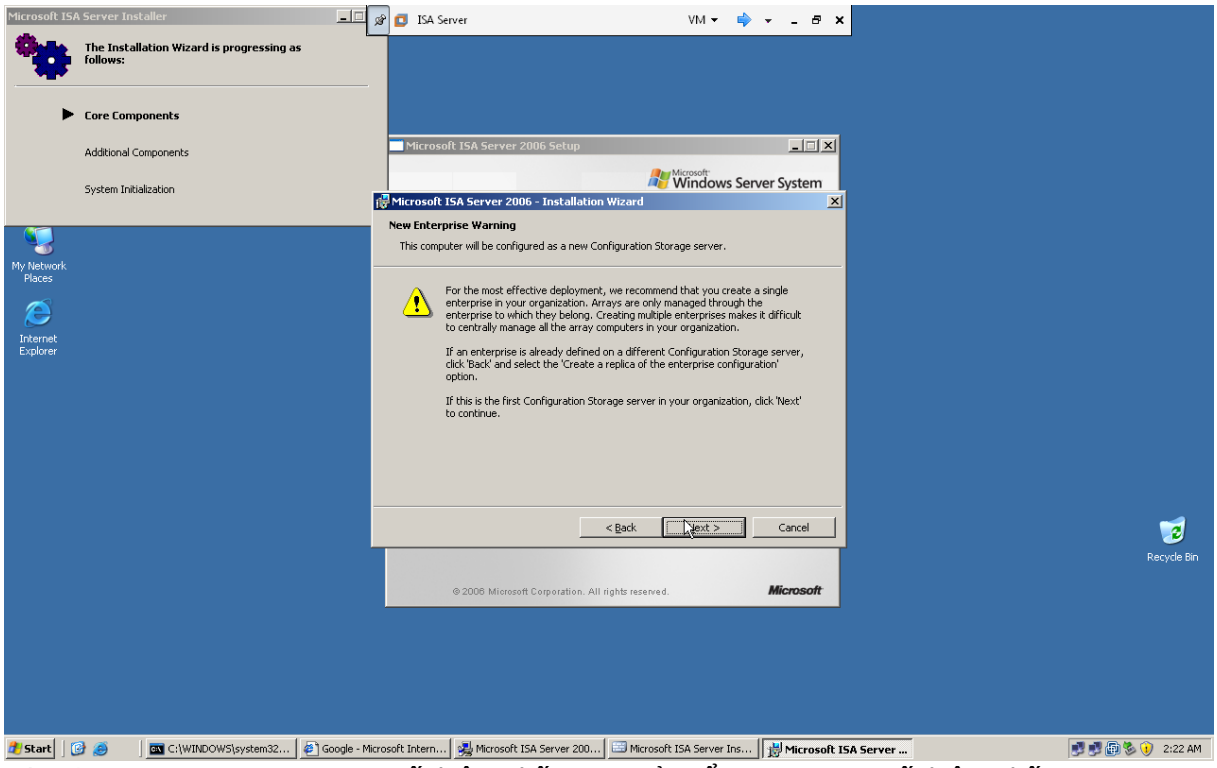
Màn hình **Component Selection** xuất hiện, chọn **Configuration Storage server->This feature, and all subfeatures, will be installed on local hard drive**:



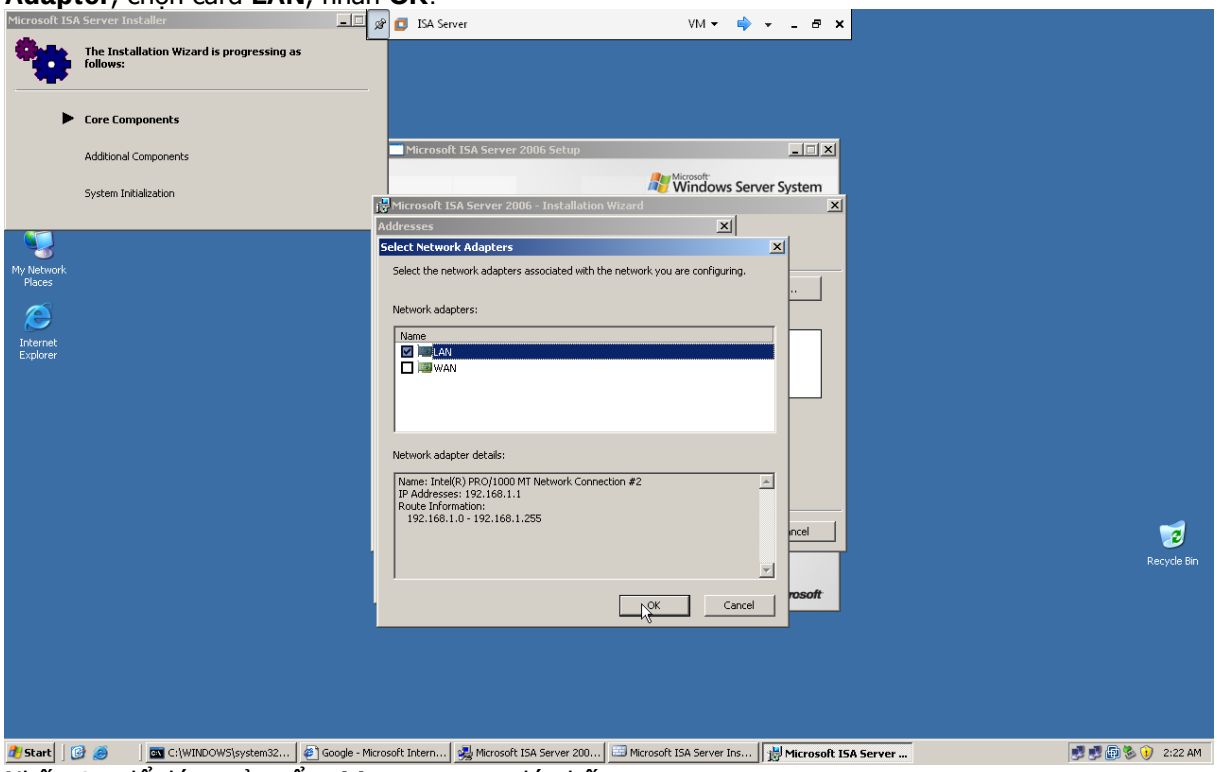
Nhấn **Next**, màn hình **Enterprise Installation Options** xuất hiện, nhấn **Next**:



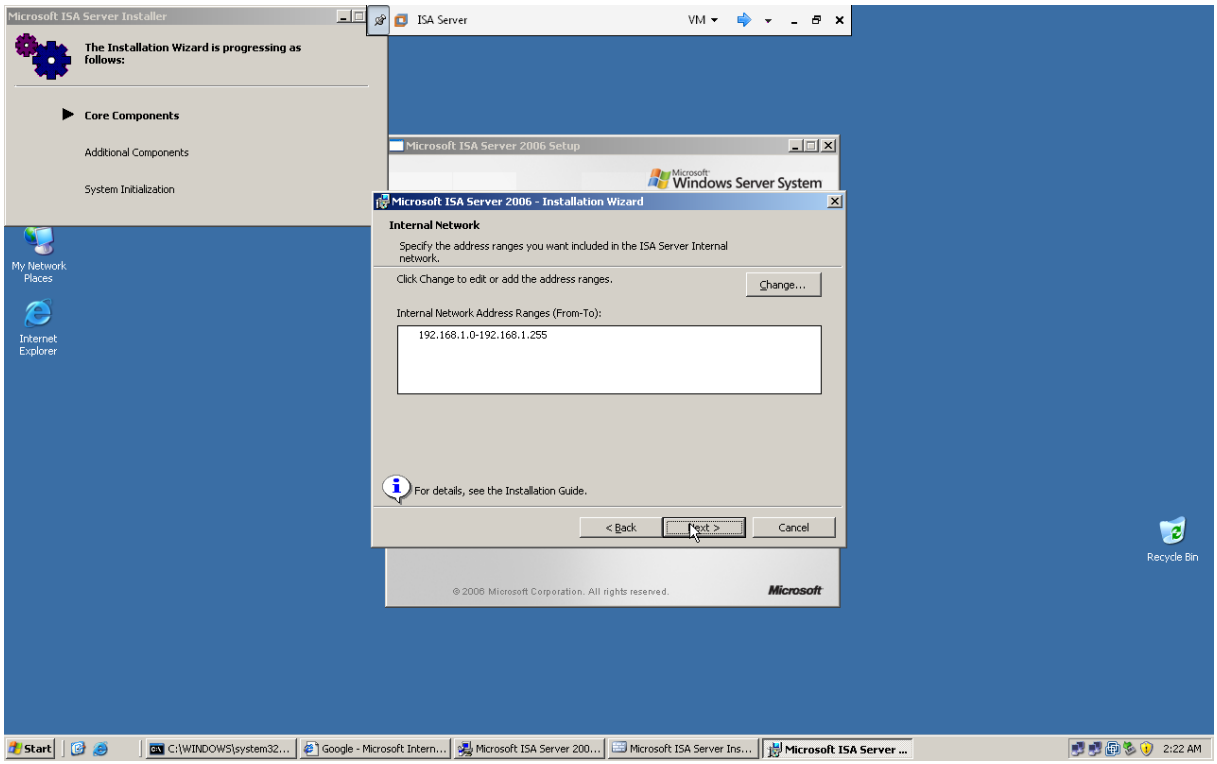
Màn hình **New Enterprise Warning** xuất hiện, nhấn **Next**:



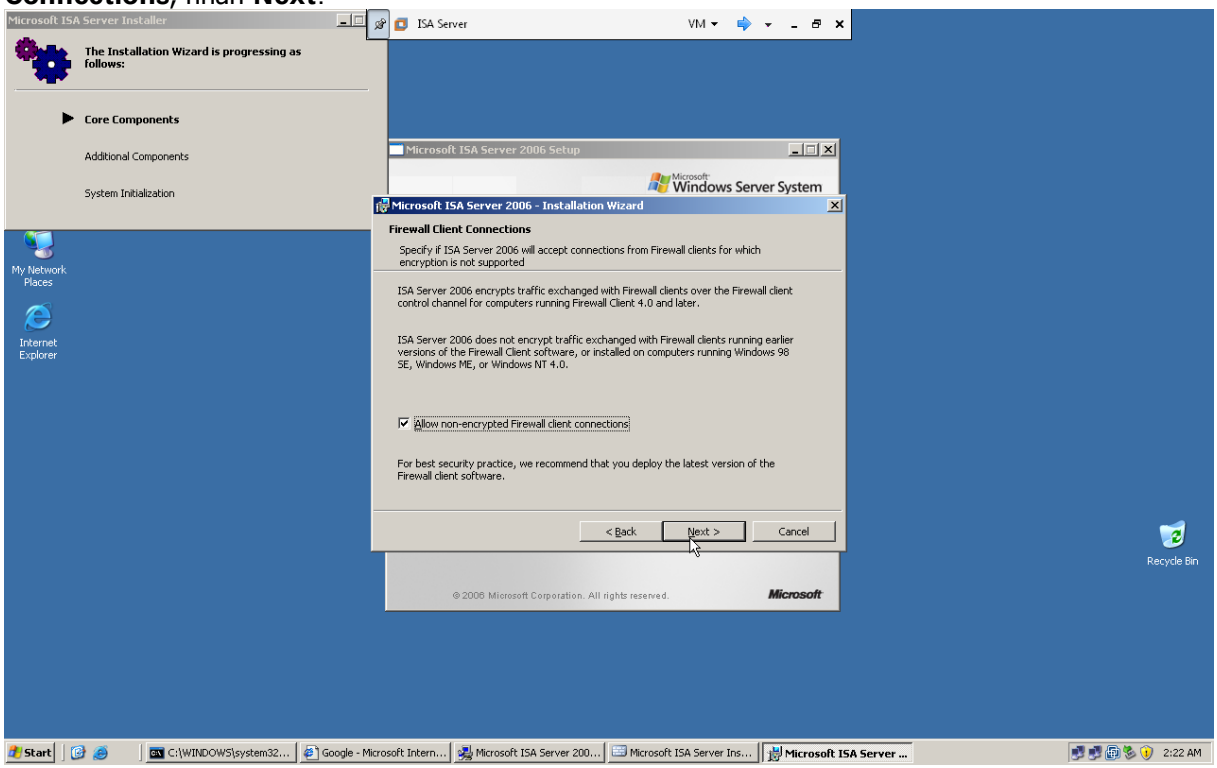
Màn hình **Internal Nextwork** xuất hiện, nhấn **Add**, cửa sổ **Addresses** xuất hiện, nhấn **Add Adapter**, chọn card **LAN**, nhấn **OK**:



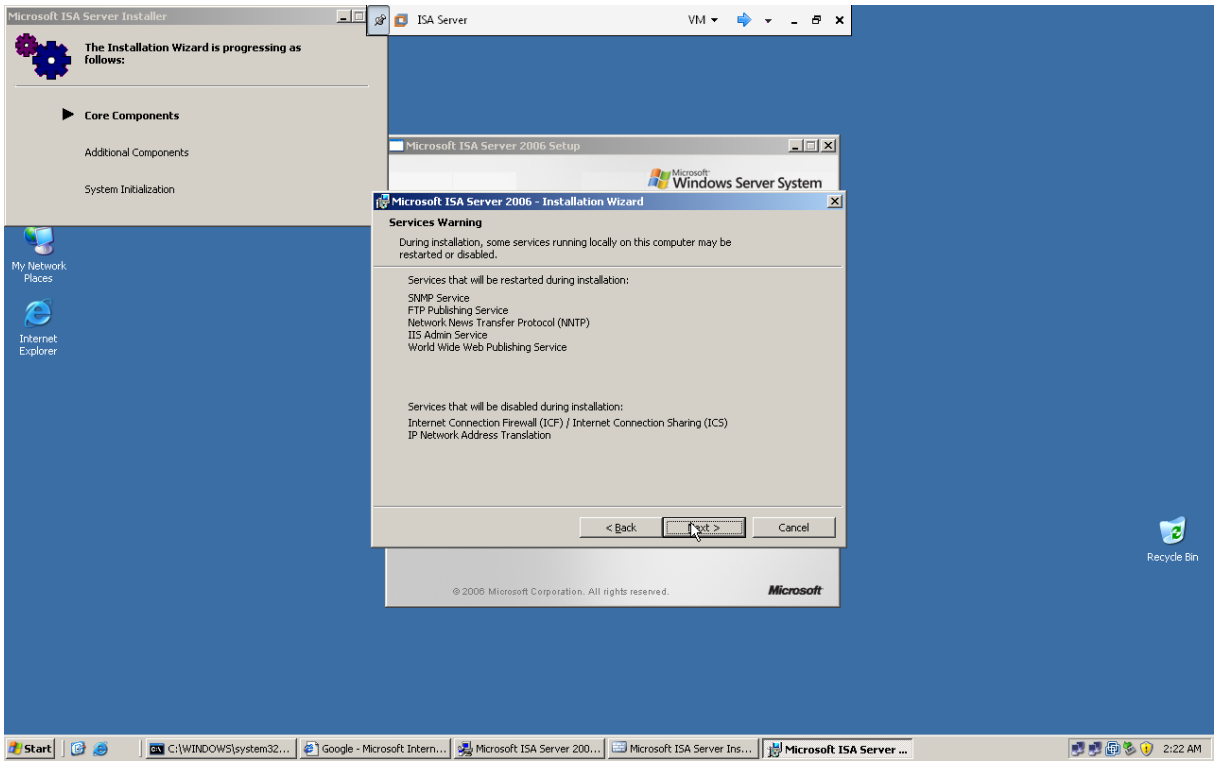
Nhấn **OK** để đóng cửa sổ **Addresses**, sau đó nhấn **Next**:



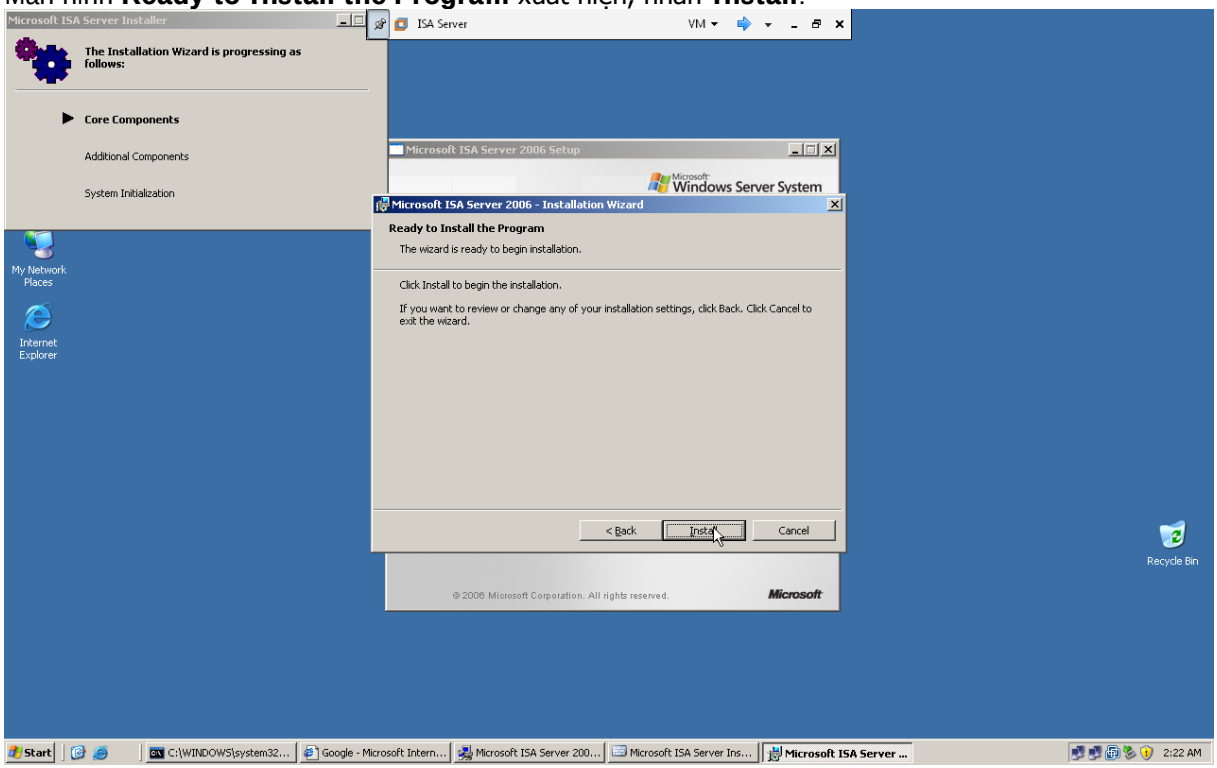
Màn hình **Firewall Client Connections** xuất hiện, chọn **Allow non-encrypted Firewall client Connections**, nhấn **Next**:



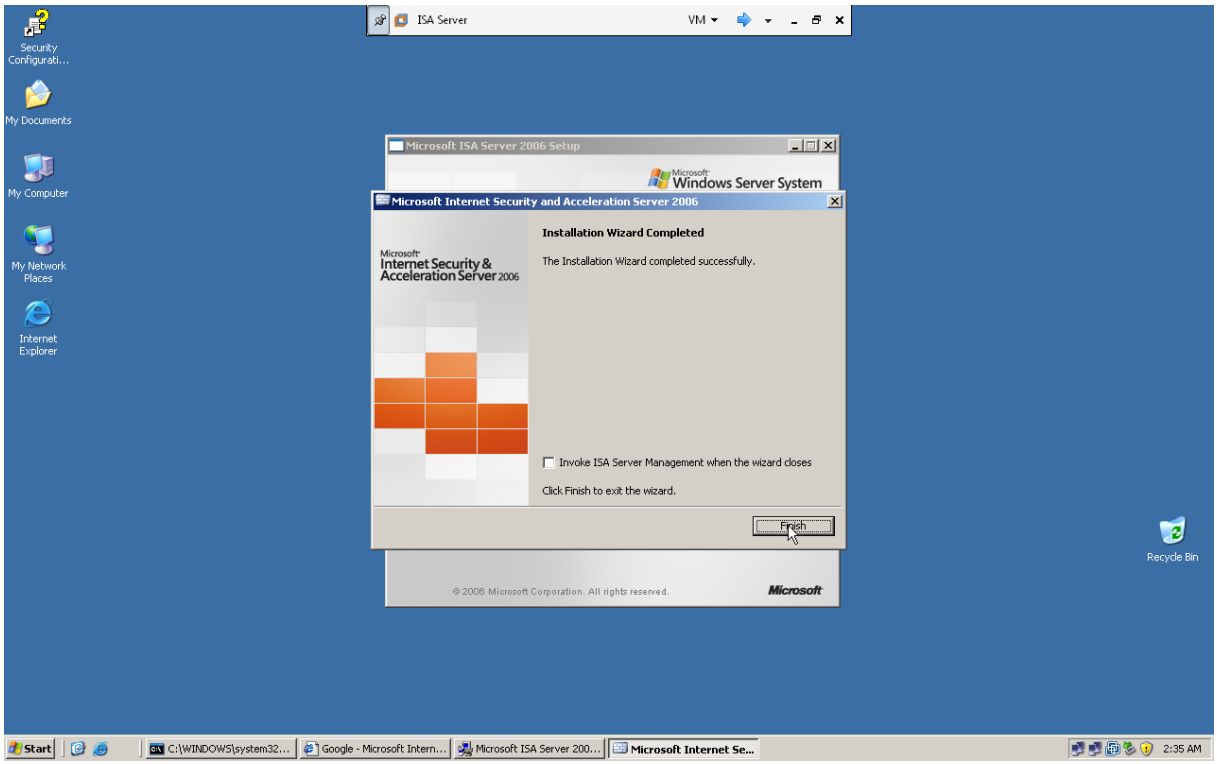
Màn hình **Service Warning** xuất hiện, nhấn **Next**:



Màn hình **Ready to Install the Program** xuất hiện, nhấn **Install**:



Qúa trình cài đặt bắt đầu cho đến khi màn hình **Installation Wizard Completed** xuất hiện, nhấn **Finish**:



- ✓ **Quản trị ISA Server 2006(xem Lab)**