Bài toán thực tế

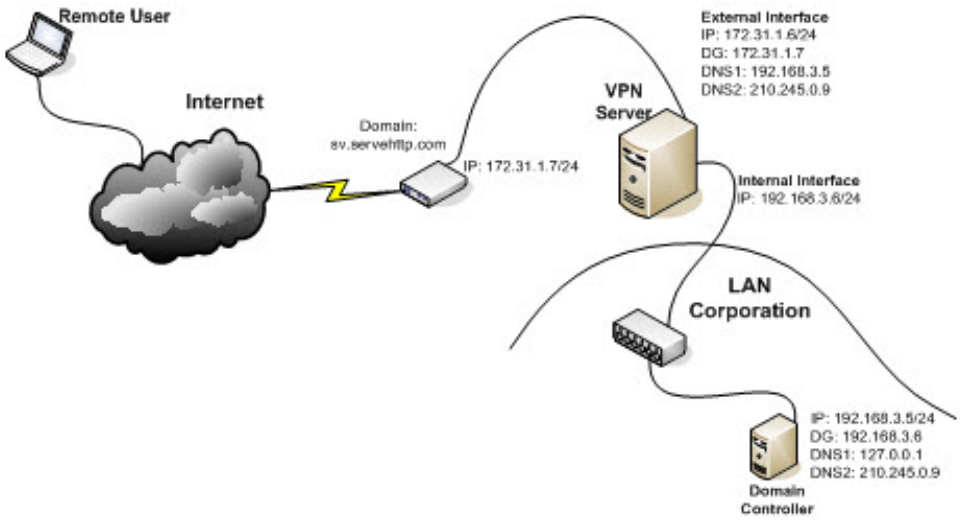
Bởi:

Khoa CNTT ĐHSP KT Hưng Yên

Bài toán

Xây dựng hệ thống VPN cho phép các thầy, cô và các bạn sinh viên truy cập vào hệ thống mạng nội bộ của khoa CNTT khi đang đi công tác xa hoặc làm việc tại nhà.

Sơ đồ hệ thống



Các bước cấu hình hệ thống

ISA Server 2004 firewall có thể được cấu hình trở thành môt VPN server. Khi bật chức năng VPN server nó có thể chấp nhận các kết nối vào từ VPN clients -incoming VPN client , nếu kết nối thành công, VPN client computer sẽ là thành viên cua Mạng được bảo vệ, không khác gì so với các Client bên trong LAN. VPN servers truyền thống cho phép VPN clients đầy đủ quyền truy cập vào Mạng khi đã được kết nối.

Ngược lại với ISA Server 2004 VPN server có khả năng cho phép chúng ta điều khiển những protocols nào và những servers nào mà VPN clients có thể kết nối đến dựa trên đặc quyền mà Client đã khai báo khi thiết lập kết nối-credentials đến VPN server.

Có thể dùng Microsoft Internet Security and Acceleration Server 2004 management console để quản lý tất cả cấu hình liên quan đến VPN server . Firewall sẽ quản lý danh sách các IP addresses được cấp phát cho VPN clients và bố trí các IP này trên một VPN clients network được chỉ định. Điều khiển truy cập sau đó có thể được bố trí dựa trên chiều giao tiếp, thông qua kiểm soát của các Access Rules : Đến hay từ VPN clients network.

Theo các bước sau tiến hành enable ISA Server 2004 VPN server:

- Enable VPN Server
- Tạo một Access Rule cho phép VPN clients truy cập vào Internal network
- Kiểm tra các kết nối VPN.

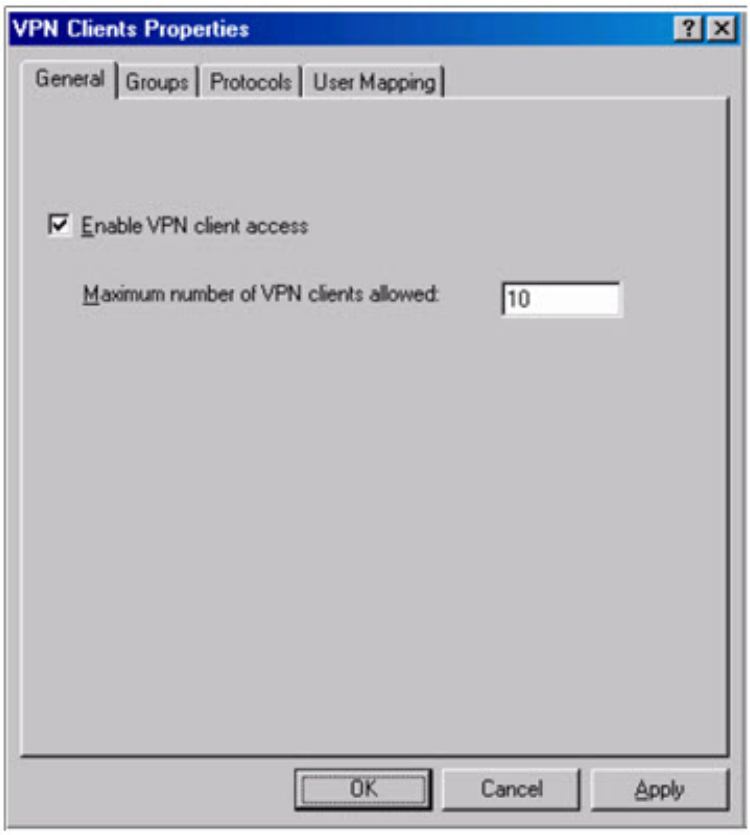
Enable VPN Server

Theo mặc định, thành phần VPN server trên ISA Server bị disabled. Bước đầu tiên là enable tính năng VPN server và cấu hình các thành phần VPN server.

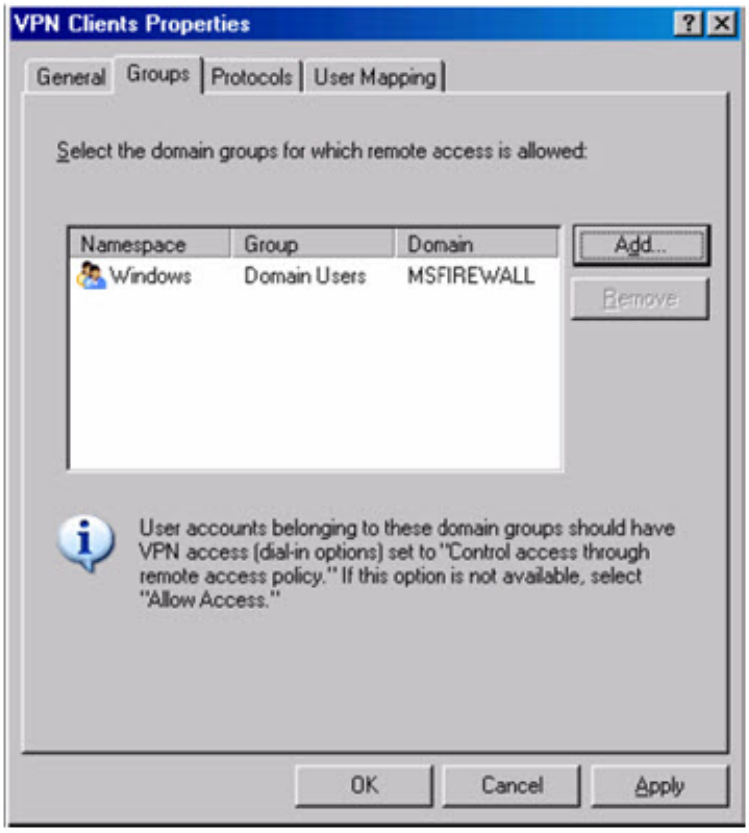
Tiến hành các bước sau để enable và cấu hình ISA Server 2004 VPN Server:

1. Mở Microsoft Internet Security and Acceleration Server 2004 management console , mở rộng server name. Click trên Virtual Private Networks (VPN) node.
2. Click trên Tasks tab trong Task Pane. Click Enable VPN Client Access.

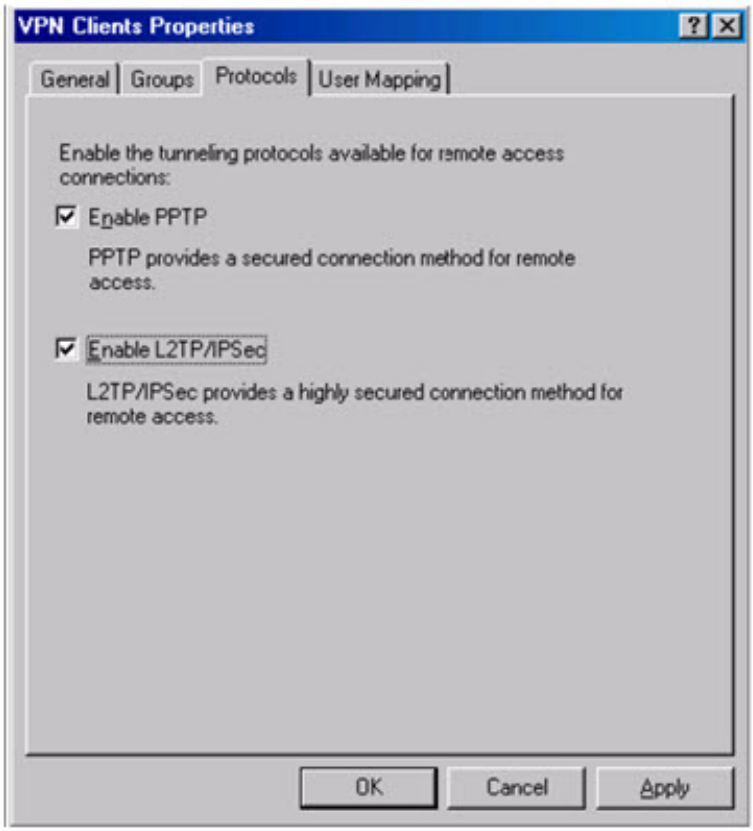
1. Click Apply để lưu những thay đổi và cập nhật firewall policy.
2. Click OK trong Apply New Configuration dialog box.
3. Click Configure VPN Client Access.
4. Trên General tab, thay đổi giá trị là Maximum number of VPN clients allowed
5. Từ 5 đến 10.



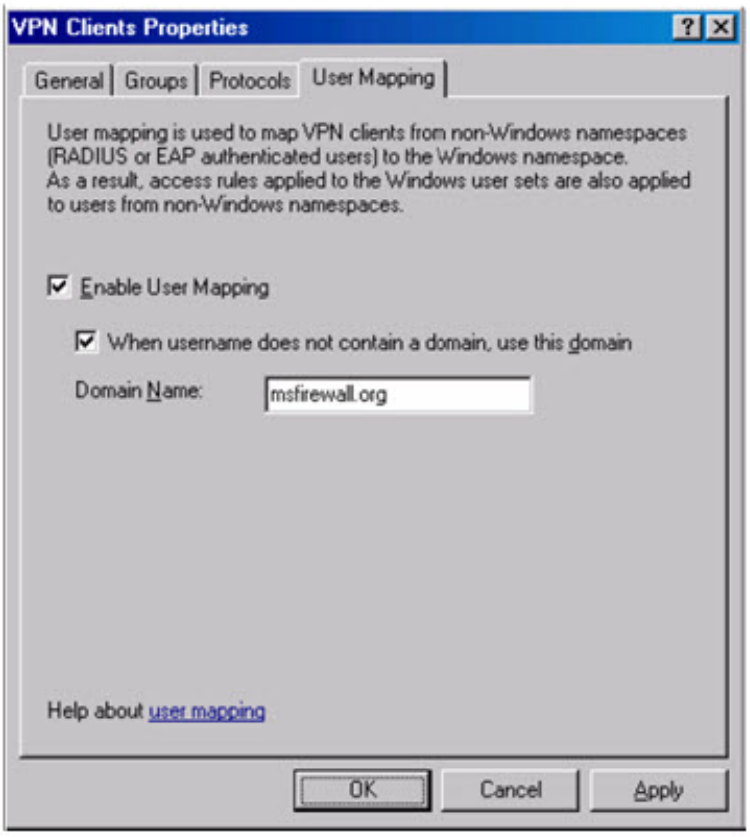
1. Click trên Groups tab. Trên Groups tab, click Add button.
2. Trong Select Groups dialog box, click Locations button. trong Locations dialog box, click msfirewall.org entry và click OK.
3. Trong Select Group dialog box, điền Domain Users trong Enter the object names to select text box. Click Check Names button. group name này sẽ có gạch dưới khi nó được tìm thấy trong Active Directory. Click OK.



1. Click Protocols tab. Trên Protocols tab, đánh dấu check vào Enable L2TP/ IPSec check box.



1. Click User Mapping tab. Đánh dấu check vào Enable User Mapping check box.
2. Đánh dấu check vào When username does not contain a domain, use this domain check box. Điền vào msfirewall.org trong Domain Name text box.



1. Click Apply trong VPN Clients Properties dialog box.
2. Click OK Microsoft ISA 2004

Dialog box nhận được thông báo rằng phải restart lại ISA Server firewall trước khi các xác lập có hiệu lực. Click OK.

1. Click Apply lưu lại những thay đổi và cập nhật cho firewall policy.
2. Click OK trong Apply New Configuration dialog box.
3. Restart ISA Server 2004 firewall.
4. Tạo một Access Rule cho phép VPN Clients truy cập vào Internal Network

Tại thời điểm này, VPN clients có thể kết nối đến VPN server. Tuy nhiên, VPN clients không thể truy cập đến bất cứ tài nguyên nào trên Internal network. Trước hết, bạn phải tạo một Access Rule cho phép các thành viên thuộc VPN clients network truy cập vào Internal network. Trong vd này, chúng ta sẽ tạo một Access Rule nhằm cho phép tất cả các lưu thông từ VPN clients network được vào Internal network. Trong môi trường thực tế, bạn có thể tạo ra access rules hạn chế hơn nhằm chặt chẽ việc Users trên VPN clients network chỉ có thể truy cập đến các tài nguyên mà họ có nhu

Tiến hành các bước sau để tạo VPN clients Access Rule:

1. Trong Microsoft Internet Security and Acceleration Server 2004 management console, mở rộng server name và click Firewall Policy node. Right click Firewall Policy node, chọn New và click Access Rule.
2. Trong Welcome to the New Access Rule Wizard page, đặt tên cho rule trong Access Rule name text box. Trong vd này, chúng ta sẽ đặt tên cho rule là VPN Client to Internal. Click Next.
3. Trên Rule Action page, chọn Allow và click Next.
4. Trên Protocols page, chọn All outbound protocols từ danh sách This rule applies to. Click Next.
5. Trên Access Rule Sources page, click Add. Trong Add Network Entities dialog box, click Networks folder và double click trên VPN Clients. Click Close.

1. Click Next trên Access Rule Sources page.
2. Trên Access Rule Destinations page, click Add. Trên Add Network Entities dialog box, click Networks folder và double click trên Internal. Click Close.
3. Trên User Sets page, chấp nhận xác lập mặc định là, All Users, và click Next.
4. Click Finish trên Completing the New Access Rule Wizard page.
5. Click Apply để lưu những thay đổi và cập nhật firewall policy.
6. Click OK trong Apply New Configuration dialog box.

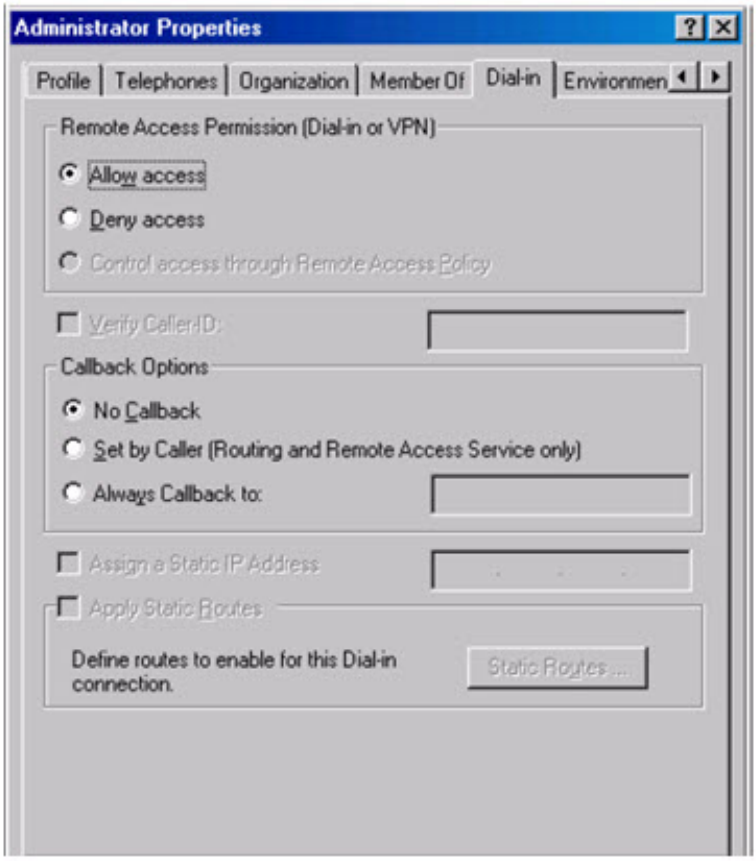
Enable truy cập quay số -Dial-in Access cho Administrator Account

Trong Active Directory domains không phải ở chế độ native mode (Native mode: Ở chế độ này tất cả các Domain Controllers trong domain ấy phải là Windows Server 2000/ 2003), Tất cả các tài khoản User đều bị disabled quyền quay số truy cập theo mặc định- dial-in access by default. Trong tình huống này, bạn phải enable dial-in access trên mỗi tài khoản

cơ bản. Ngược lại, thì Active Directory domains ở chế độ native mode có dial-in access được tập trung điều khiển bởi Remote Access Policy trong RRAS Server. Windows NT 4.0 dial-in access luôn được điều khiển căn cứ trên từng User account Trong ví dụ này, Active Directory ở dạng Windows Server 2003 mixed mode, và vì thế cần thay đổi thủ công các xác lập quyền quay số trên user account.

Tiến hành các bước sau trên domain controller để enable Dial-in access cho riêng Administrator account:

1. Click Start và chọn Administrative Tools. Click Active Directory Users and Computers.
2. Trong Active Directory Users and Computers console, click trên Users node trong khung trái. Double click trên Administrator account trong khung phải.
3. Click trên Dial-in tab. Trong khung Remote Access Permission (Dial-in or VPN), chọn Allow access. Click Apply và click OK.



1. Đóng Active Directory Users and Computers console.
2. Kiểm tra kết nối VPN ISA Server 2004 VPN server giờ đây đã chấp nhận các kết nối VPN client.

Tiến hành các bước sau để kiểm tra VPN Server:

1. Trên Windows 2000 external client, right click My Network Places icon trên desktop và click Properties.
2. Double click Make New Connection icon trong Network and Dial-up Connections window.
3. Click Next trên Welcome to the Network Connection Wizard page.
4. Trên Network Connection Type page, chọn Connect to a private network through the Internet option và click Next.
5. Trên Destination Address page, điền IP address 192.168.1.70 trong Host name or IP address text box. Click Next.
6. Trên Connection Availability page, chọn For all users option và click Next.

Không thay đổi trên Internet Connection Sharing page. và click Next.

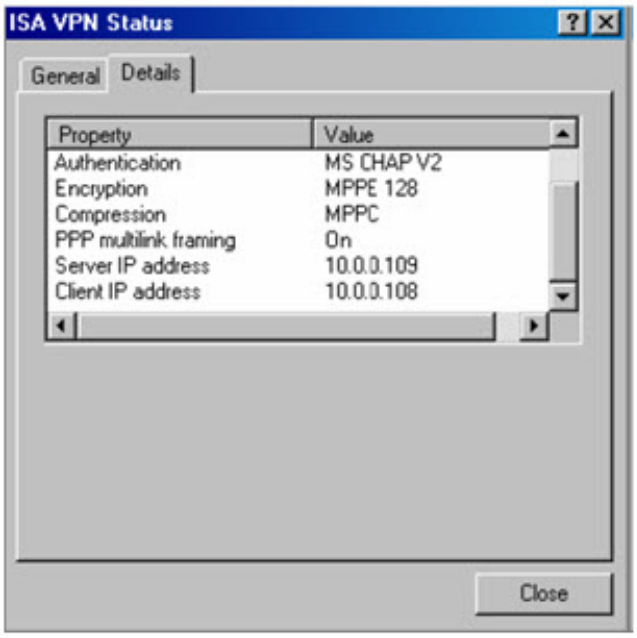
Trên Completing the Network Connection Wizard page, điền vào tên của VPN connection trong Type the name you want to use for this connection text box.

Trong vd này, chúng ta sẽ đặt tên kết nối là ISA VPN. Click Finish.

Trong Connect ISA VPN dialog box, điền vào user name

MSFIREWALL\administrator và password của administrator user account. Click Connect.

1. VPN client sẽ thiết lập một kết nối với ISA Server 2004 VPN server. Click OK
2. trong Connection Complete dialog box nhận được thông báo rằng kết nối đã được thiết lập.
3. Double click trên Connection icon trong system tray và click Details tab. Bạn có thể thấy chế độ mã hóa 128 bits dùng giao thức MPPE- MPPE 128 encryption được sử dụng để bảo vệ data và thấy IP address được cấp phát cho VPN client.



1. Click Start và Run command. Trong Run dialog box, điền vào \\EXCHANGE2003BE trong Open text box, và click OK. Các folder shares trên domain controller xuất hiện.
2. Right click Connection icon trong system tray và click Disconnect.