

## **Truy cập máy khách VPN từ xa qua VPN Site to Site**

**Trong bài này chúng tôi sẽ giới thiệu cho các bạn cách kích hoạt các kết nối VPN máy khách để truy cập từ xa qua VPN Site to Site cho các mạng văn phòng chi nhánh.**

Trong một số bài được giới thiệu trước đây về ISA Server, chúng tôi đã giới thiệu cho các bạn khá nhiều kiến thức về cơ sở hạ tầng VPN Site to Site. Chính vì vậy mà trong bài này, chúng tôi muốn giới thiệu cho các bạn một vấn đề nâng cao trong kỹ thuật này, đó là kích hoạt các kết nối VPN máy khách để truy cập từ xa qua VPN Site to Site cho các mạng văn phòng chi nhánh.

Vấn đề có thể đơn giản với những ai đó đã làm việc nhiều với ISA Firewall. Tuy nhiên với đại đa số thì đây vẫn là một vấn đề phức tạp. Tuy nhiên trong quá trình sử dụng, chúng tôi có thể đưa ra các vấn đề chính ở đây là các định

nghĩa của ISA Firewall Networks và các Network Rules dùng để kết nối với ISA Firewall Networks đã được định nghĩa đó.

Khi bạn cài đặt ISA Firewall lần đầu, một số ISA Firewall Networks mặc định sẽ được tạo. Những thứ có thể nói là quan trọng cần đề cập đến ở đây là:

- **Local Host Network** – Mạng được định nghĩa bởi tất cả các địa chỉ IP đường biên cho bất cứ giao diện nào trên ISA.
- **Default Internal Network** – Đây là một ISA Firewall Network mà bạn có thể định nghĩa khi ISA Firewall được cài đặt. Điển hình nó chính là interface gần nhất cho các dịch vụ cơ sở hạ tầng mạng chính mà ISA Firewall phụ thuộc, chẳng hạn như Active Directory domain controller, DNS server, DHCP server và dịch vụ chứng chỉ.
- **Default External Network** – Default External Network được định nghĩa với tất cả các địa chỉ IP *không*

*bị gộp trong định nghĩa của bất kỳ ISA Firewall Network nào. Bạn không bao giờ cần add các địa chỉ IP vào Default External Network vì nó là một mạng tự xác định, gồm có các địa chỉ IP mà bạn không nhóm vào bất cứ một mạng ISA Firewall Network nào.*

- **VPN Clients Network** – VPN Clients Network là một ISA Firewall Network có chứa địa chỉ IP của máy khách VPN truy cập xa và các VPN gateway đang kết nối đến ISA Firewall. Định nghĩa ISA Firewall Network này mang tính động. Vì VPN client và gateway kết nối đến the ISA Firewall, các địa chỉ VPN interface của chúng sẽ tự động được add vào định nghĩa VPN Clients Network, và sẽ tự động bị xóa đi khi VPN client và gateway hủy kết nối với ISA Firewall.

Các ISA Firewall Network được gán với giao diện mạng (network interface) gần nhất với các địa chỉ được định nghĩa bởi ISA Firewall network. Trong đó, NIC là “root” của các ISA Firewall Network cụ thể.

Cho ví dụ, nếu các network ID là 192.168.1.0/24, 192.168.2.0/24 và 192.168.3.0/24 được đặt phía sau interface A (ý nói ở đây interface A gần nhất với các network ID này), thì interface A chính là root của ISA Firewall Network được định nghĩa cho ba network ID này. Điều này giúp ngăn chặn các tấn công giả mạo. Nếu ISA Firewall thấy một địa chỉ nguồn của một quá trình truyền thông gửi ra từ một host không thuộc về một trong các network ID này thì ISA Firewall sẽ chặn sự truyền thông đó vì địa chỉ IP này không nằm trong định nghĩa của ISA Firewall Network để được phép truyền thông.

Hình dưới đây thể hiện nơi bạn có thể tìm danh sách các ISA Firewall Network. Trong giao diện quản lý ISA Firewall, mở mảng (hoặc máy chủ Standard Edition), sau đó kích nút **Configuration**. Bên dưới nút **Configuration**, kích **Networks**. Kích tab trong vùng cửa sổ giữa, khi đó bạn sẽ thấy danh sách các ISA Firewall Network.



Hình 1

Để các host trên ISA Firewall Network có thể truyền thông với nhau, bạn cần phải tạo các nguyên tắc mạng Network Rule. Nếu không có Network Rule cho việc kết nối hai ISA Firewall Network với nhau, sẽ không có sự truyền thông giữa các host trên hai mạng này.

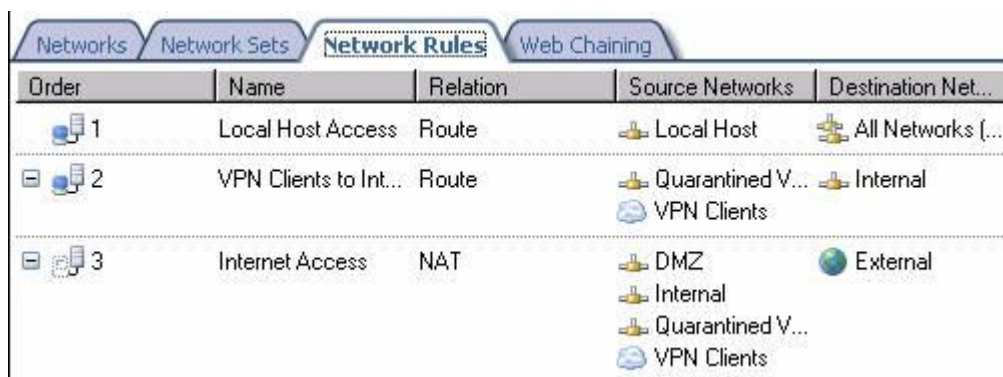
Network Rule có thể định nghĩa cách thức NAT hoặc mối quan hệ tuyến Route giữa mạng nguồn và mạng đích. Quan hệ Route sẽ cho phép các host phía này quan hệ có thể khởi tạo truyền thông với các host

phía bên kia bằng các nguyên tắc truy nhập Access Rules. Với mỗi quan hệ NAT, chỉ có các kết nối được NAT mới có thể khởi tạo kết nối thông qua Access Rule. Các kết nối gửi vào, hoặc được NAT ngược phụ thuộc vào các Web Publishing Rule hoặc Server Publishing Rule.

Bộ cài đặt ISA Firewall sẽ tạo các Network Rule cho bạn trong quá trình cài đặt ISA Firewall. Trong nút **Networks**, kích tab **Network Rules** ở phần giữa của giao diện điều khiển ISA Firewall. Ba Network Rule mặc định được hiển thị trong hình bên dưới (mặc dù vậy trong hình, các định nghĩa mặc định của các rule này đã được thay đổi). Các rule đó là:

- **Local Host Access** – định nghĩa mối quan hệ Route giữa Local Host Network và các mạng khác.
- **VPN Clients to Internal** – định nghĩa mối quan hệ Route giữa VPN Clients Network với các mạng Default Internal Network.

- **Internet Access** – định nghĩa mối quan hệ NAT cho quá trình truyền thông bắt nguồn từ Internal Network đến Default External Network.



Order	Name	Relation	Source Networks	Destination Net...
1	Local Host Access	Route	Local Host	All Networks (...)
2	VPN Clients to Int...	Route	Quarantined V... VPN Clients	Internal
3	Internet Access	NAT	DMZ Internal Quarantined V... VPN Clients	External

Hình 2

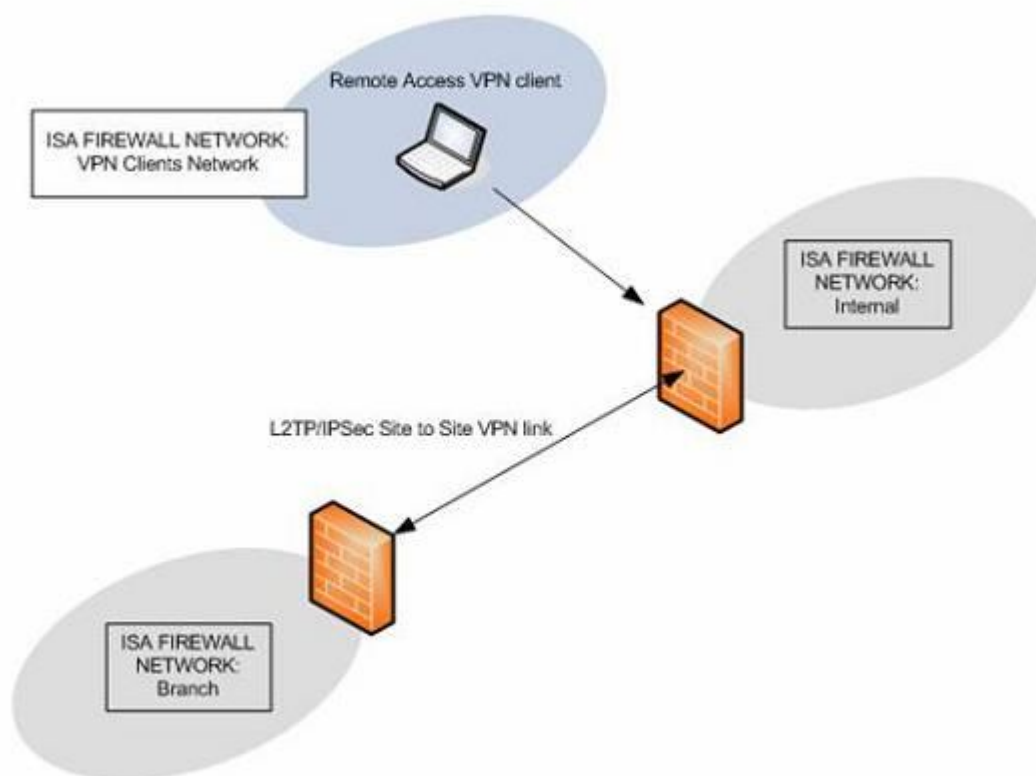
Hãy đi nghiên cứu tình huống mà ở đó chúng ta muốn cho phép các máy khách VPN từ xa có thể kết nối với các tài nguyên nằm tại văn phòng chi nhánh khi chúng thiết lập một kết nối đến văn phòng chi nhánh. Hình bên dưới cung cấp những phức tạp cơ bản về các ISA Firewall Network có liên quan trong sự truyền thông này:

- **VPN Clients Network** – Đây là mạng ISA Firewall Network có tất cả các máy khách VPN và gateway khi chúng kết nối với ISA Firewall.

- **Main office default Internal Network** – Đây là mạng nằm phía sau ISA Firewall văn phòng chính. Lưu ý rằng tên mạng (Network name) của ISA Firewall có liên quan với vị trí của máy khách đang kết nối với ISA Firewall Network này. Khi máy khách VPN truy cập từ xa kết nối với ISA Firewall văn phòng chi nhánh, đây sẽ là một Default Internal Network đối với các thành viên của VPN Clients Network. Mặc dù vậy, nếu một host tại văn phòng chi nhánh đã kết nối được với mạng này thì tên mạng sẽ cho thấy điều đó. Chúng ta sẽ đi xem xét một ví dụ cho vấn đề này sau.
- **Branch Remote ISA Firewall Network** – Các mạng Remote Network được định nghĩa khi bạn tạo các kết nối VPN site to site. Từ phía các host đang kết nối từ ISA Firewall văn phòng chính, các kết nối được tạo với mạng văn phòng chi nhánh sẽ được kết nối đến Branch Remote Network. Mặc dù vậy, nếu



một máy khách nào đó đã kết nối với ISA Firewall văn phòng chi nhánh, thì mạng mà các máy khách sẽ kết nối đến là gì? Đó chính là Default Internal Network vì trong kịch bản VPN site to site, tên của ISA Firewall Network đích có quan hệ với ISA Firewall mà máy khách VPN truy cập từ xa kết nối với nó.



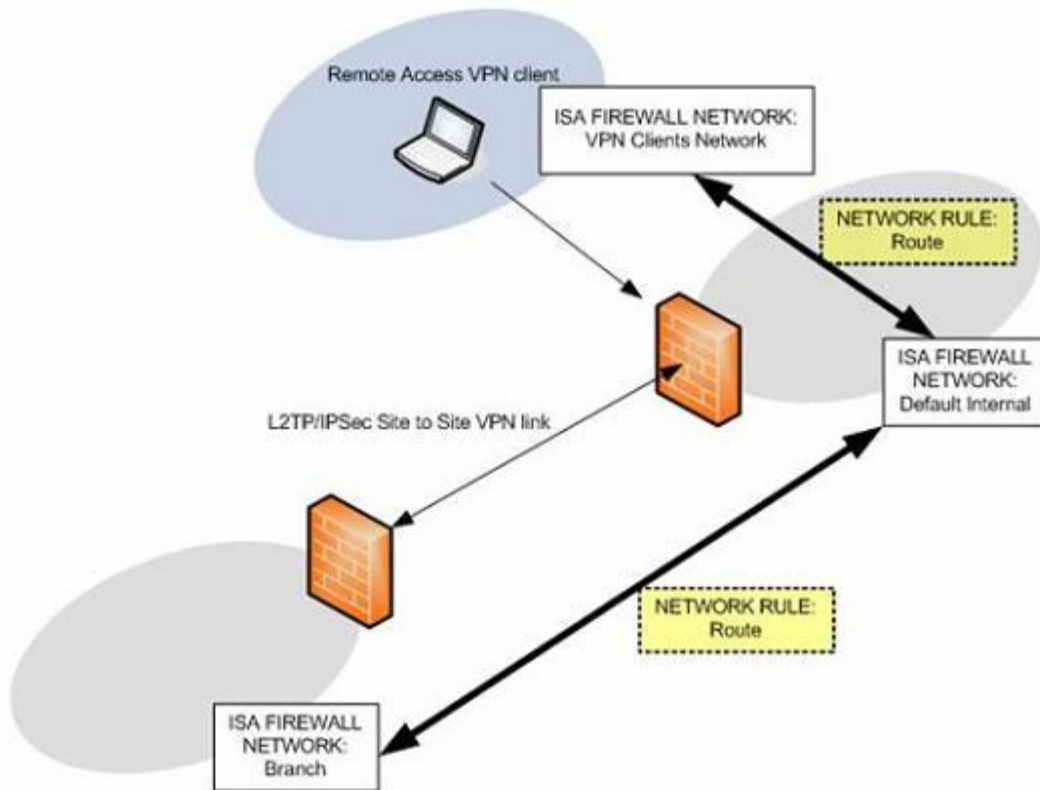
Hình 3

Hình bên dưới thể hiện mối quan hệ Route như đã định nghĩa bởi các Network Rule cho việc kết nối các mạng này với nhau:

- Có một Network Rule cho việc kết nối VPN Clients Network với default Internal Network. Network Rule này thiết lập mối quan hệ Route giữa các máy khách VPN và default Internal Network của văn phòng chính.
- Một Network Rule cho việc kết nối Default Internal Network của văn phòng chính với office ISA Firewall Network văn phòng chi nhánh. Network Rule này thiết lập mối quan hệ Route giữa các mạng này.

Các Network Rule này cho phép các máy khách VPN có thể kết nối với các tài nguyên trong mạng Default Internal Network của văn phòng chính, cho phép các thành viên của mạng Default Internal Network của văn phòng chính có thể kết nối đến tài nguyên nằm

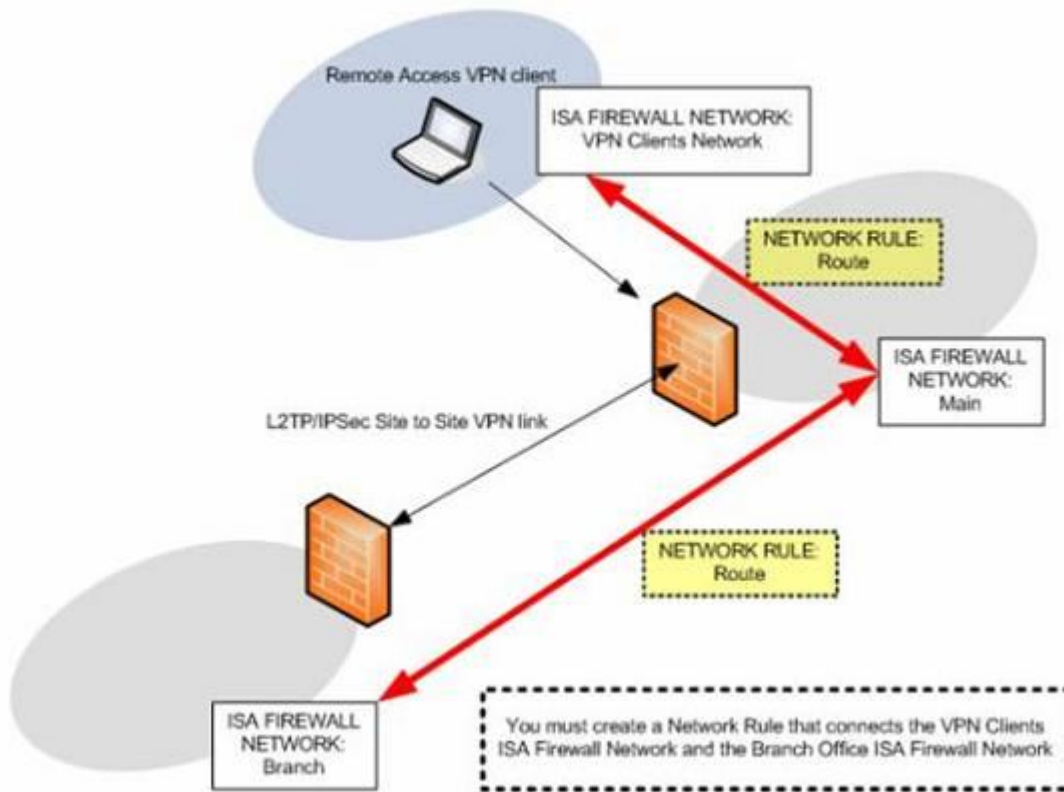
trong ISA Firewall Network của văn phòng chi nhánh. Mặc dù vậy, liệu có rule nào có thể cho phép các thành viên của mạng VPN Clients Network có thể kết nối với ISA Firewall Network văn phòng chi nhánh? Câu trả lời là không.



Hình 4

Hình bên dưới hiển thị những gì xảy ra khi chúng ta tạo một Network Rule mới để kết nối mạng VPN Client Network của văn phòng chính với mạng văn

phòng chi nhánh. Mũi tên đỏ cho thấy rằng chúng ta có một Network Rule định nghĩa mối quan hệ tuyến giữa hai mạng này. Hiện có một Network Rule cho việc kết nối VPN Clients Network của văn phòng chính và chúng ta có thể tạo các Access Rule để cho phép truyền thông giữa hai mạng này với nhau (VPN Client và mạng chi nhánh).

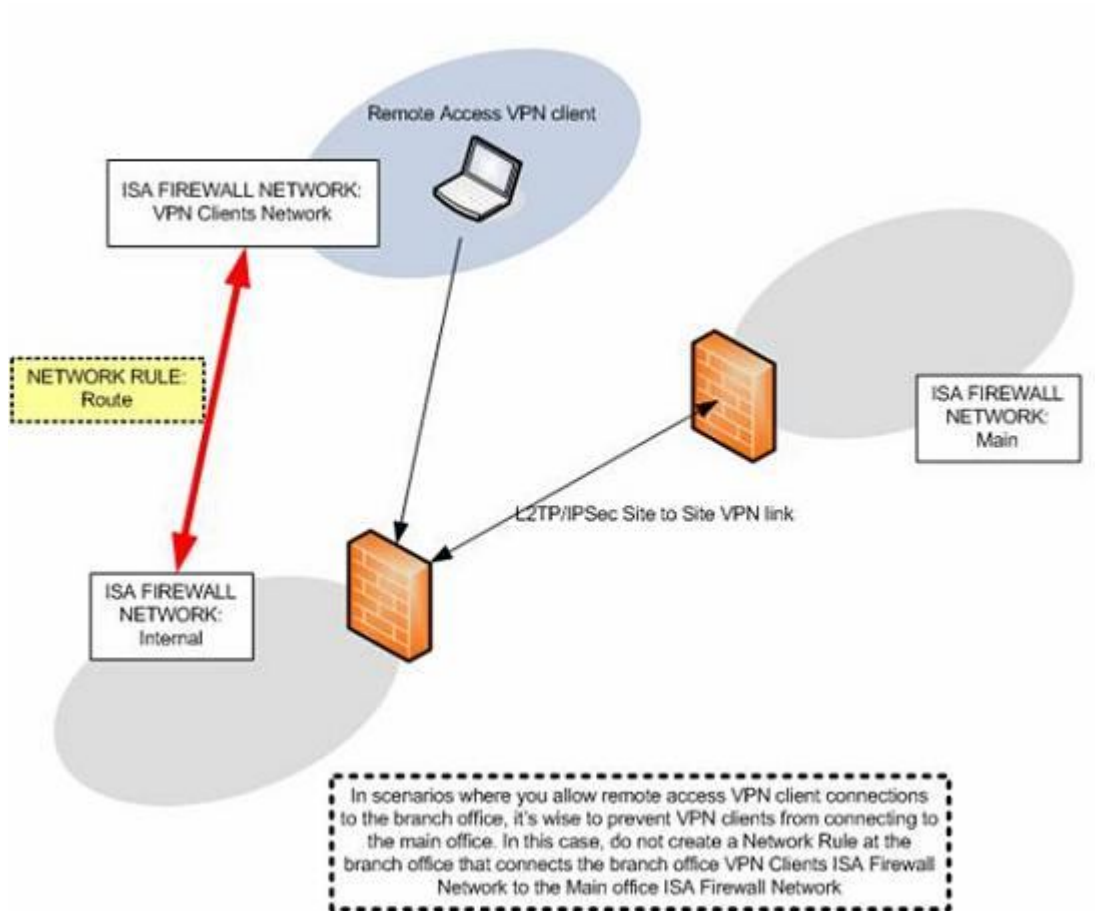


Hình 5

Hình bên dưới thể hiện một tình huống hơi khác so với những gì chúng ta nói ở trên: Giả sử bạn muốn cho phép các kết nối máy khách VPN từ xa đến ISA Firewall văn phòng chi nhánh. Trong trường hợp này, Network Rule yêu cầu kết nối VPN Clients Network văn phòng chi nhánh với Default Internal Network tại văn phòng chi nhánh. Bạn có thấy sự khác nhau dựa trên vị trí? Khi các máy khách VPN kết nối với ISA Firewall văn phòng chính, chúng phải kết nối với ISA Firewall Network văn phòng chi nhánh. Khi chúng đã kết nối với ISA Firewall văn phòng chi nhánh, chúng sẽ có khả năng kết nối đến Default Internal Network (cho ISA Firewall văn phòng chi nhánh).

Lưu ý rằng tên mạng sẽ thay đổi dựa vào phối cảnh của các host đang kết nối qua ISA Firewall văn phòng chi nhánh. Để kết nối tới văn phòng chính, các host đang kết nối từ ISA Firewall văn phòng chi

nhánh phải kết nối với Remote Site Network có phần tên “Main”.



Hình 6

Với cơ sở này, giờ đây bạn có thể chỉ ra tại sao một số quản trị viên ISA Firewall gặp phải vấn đề trong việc cho phép các máy khách VPN truy cập xa kết nối với ISA Firewall văn phòng chính để truy cập tài nguyên trên ISA Firewall Network văn phòng chi

nhánh: họ cần tạo một Network Rule để kết nối VPN Clients Network văn phòng chính với ISA Firewall Network văn phòng chi nhánh.

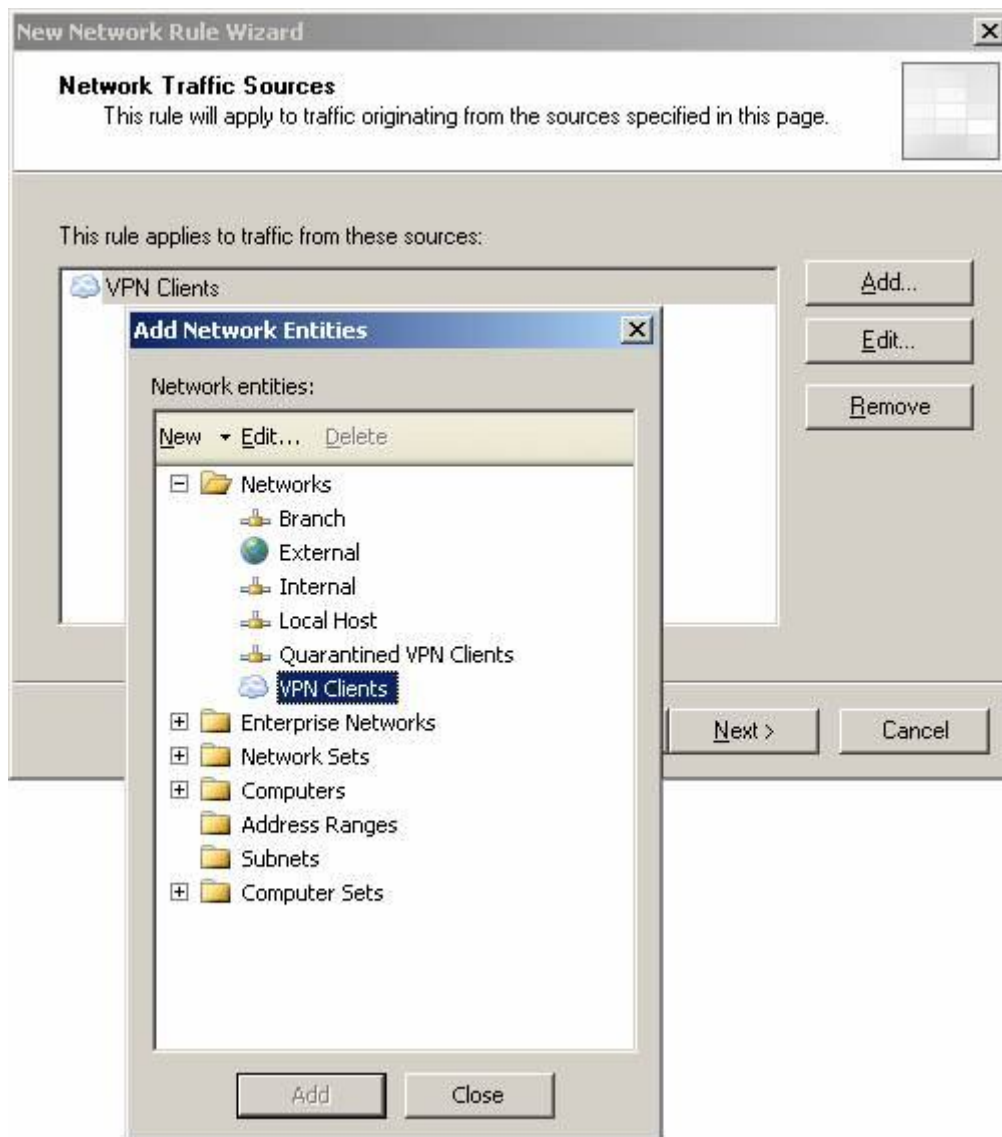
Quả thực, còn có một thứ khác cần phải thực hiện ở đây đó là tạo một Access Rule để cho phép truyền thông từ VPN Clients Network văn phòng chính đến mạng văn phòng chi nhánh. Mặc dù có một Network Rule kết nối các mạng với nhau nhưng vẫn cần phải có một Access Rule cho phép truyền thông giữa các mạng này.

Hãy sử dụng mạng VPN site to site mà chúng ta đã tạo trước đây để thể hiện cách thực hiện đó. Thực hiện các bước dưới đây để tạo một Network Rule:

1. Tại máy CSS, mở giao diện điều khiển ISA Firewall. Trong cửa sổ này, kích **Arrays** và kích mảng **Main**. Tiếp đó kích **Configuration** và **Networks**.

2. Trong nút **Networks**, kích tab **Network Rules** ở panel giữa. Trong tab **Tasks** trên Task Panel, kích liên kết **Create a Network Rule**.
3. Trong trang **Welcome to the New Network Rule Wizard**, nhập vào tên rule trong hộp thoại **Network Rule name**. Trong ví dụ này, chúng tôi đã sử dụng tên **VPN Clients to Branch** và kích **Next**.
4. Trong trang **Network Traffic Sources**, kích nút **Add**. Trong hộp thoại **Add Network Entities**, kích thư mục **Networks**, sau đó kích đúp vào mạng **VPN Clients**. Kích **Close**.



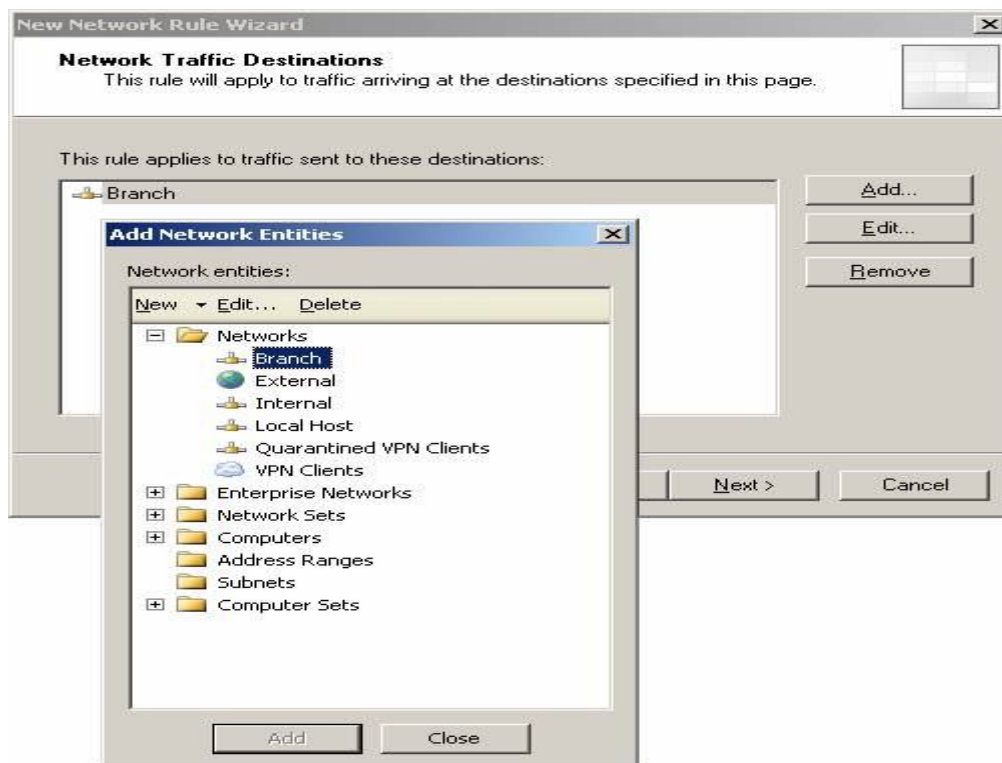


Hình 7

5. Kịch **Next** trong trang **Network Traffic Sources**.

6. Trong trang **Network Traffic Destinations**, kích nút **Add**. Trong hộp thoại **Add Network Entities**,

kích thư mục **Networks**, sau đó kích mạng **Branch**.  
Kích **Close**.



Hình 8

7. Trong trang **Network Relationship**, chọn tùy chọn **Route**. Có một vấn đề cần phải đề cập ở đây, từ quan điểm bảo mật trong việc sử dụng NAT cho kịch bản này, vì vậy chúng ta luôn phải chọn tùy chọn **Route**. Kích **Next**.



Hình 9

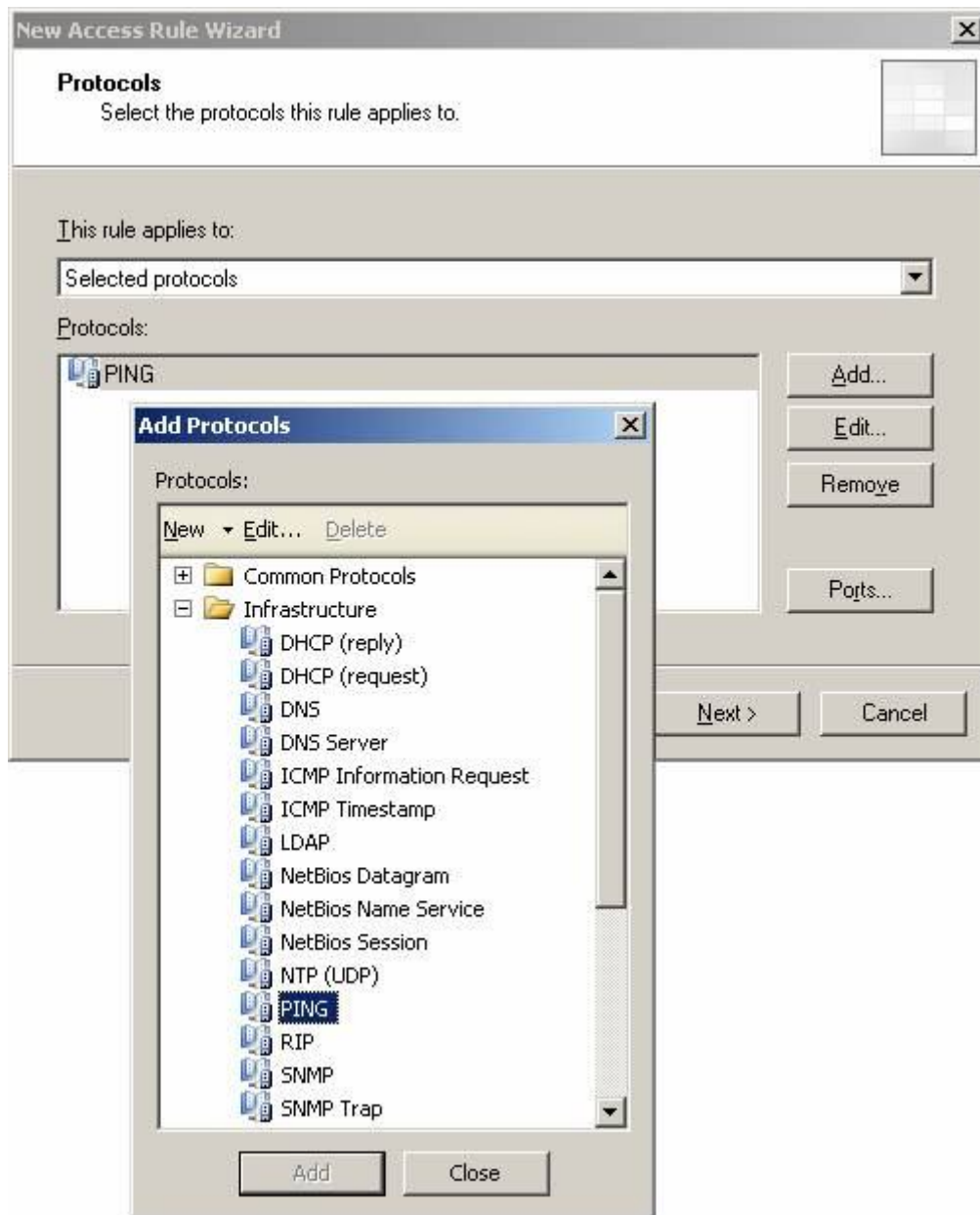
## 8. Kịch **Finish** trong trang **Completing the New Network Rule Wizard**

Lúc này chúng ta cần tạo hai Access Rule, một tại mảng ISA Firewall văn phòng chính và một tại văn phòng chi nhánh. Rule tại văn phòng chính sẽ cho phép PING từ VPN Clients Network đến được văn phòng chi nhánh, Access Rule tại văn phòng chi nhánh sẽ cho phép PING từ văn phòng chính đến Default Internal Network. Hãy tạo rule đầu tiên trên

mạng ISA Firewall văn phòng chính để cho phép ping từ VPN Clients Network đến mạng văn phòng chi nhánh:

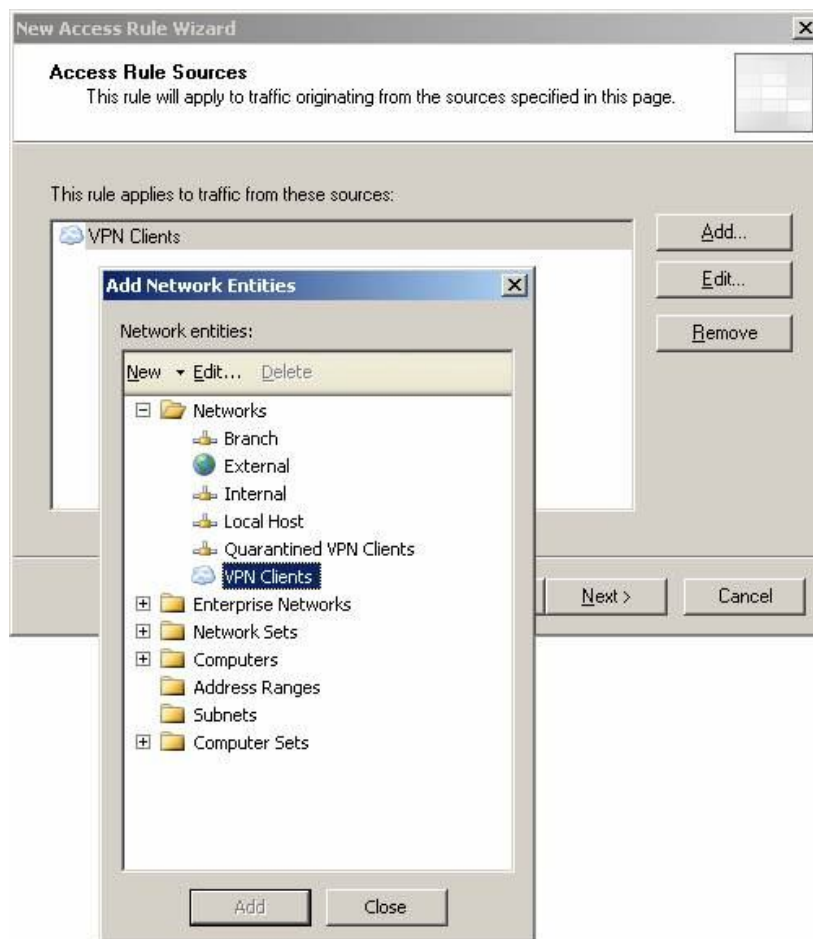
1. Tại máy tính CSS trong văn phòng chính, trong giao diện điều khiển ISA Firewall, kích **Firewall Policy (main)** trong phần panel trái của giao diện.
2. Trong tab **Tasks** của Task Pane, kích liên kết **Create Access Rule**.
3. Trên trang **Welcome to the New Access Rule Wizard**, nhập tên cho rule trong hộp **Access Rule name**. Trong ví dụ này, chúng tôi sử dụng tên **Ping VPN Clients to Branch** và kích **Next**.
4. Trong trang **Rule Action**, chọn tùy chọn **Allow** và kích **Next**.
5. Trong trang **Protocols**, chọn tùy chọn **Selected protocols** từ danh sách sổ xuống **This rule applies**. Kích nút **Add**. Trong hộp **Add Protocols**, kích thư

mục **Infrastructure**, sau đó kích đúp vào giao thức **PING**. Tiếp đó kích **Close**.



Hình 10

- Trong trang **Access Rule Sources**, kích nút **Add**. Trong hộp **Add Network Entities**, kích thư mục **Networks**, sau đó kích đúp mạng. Kích **Close**.



Hình 11

- Kích **Next** trong trang **Access Rule Sources**.
- Trong trang **Access Rule Destinations**, kích nút **Add**. Trong hộp **Add Network Entities**, kích thư

mục **Networks**, sau đó kích đúp mạng **Branch**. Kích **Close**.

9. Trong trang **User Sets**, chấp nhận thiết lập mặc định, **All Users**, và kích **Next**.

10. Kích **Finish** trong trang **Completing the New Access Rule Wizard**.

11. Kích **Apply** để lưu các thay đổi và cập nhật chính sách tường lửa. Kích **OK** trong hộp thoại **Apply New Configuration**.

Lúc này chúng ta hãy tạo rule thứ hai cho phép ping từ ISA Firewall Network văn phòng chính đến Default Internal Network văn phòng chi nhánh:

1. Tại máy tính CSS ở văn phòng chính, trong giao diện điều khiển ISA Firewall, kích nút **Firewall Policy (branch)** ở panel trái của giao diện điều khiển.

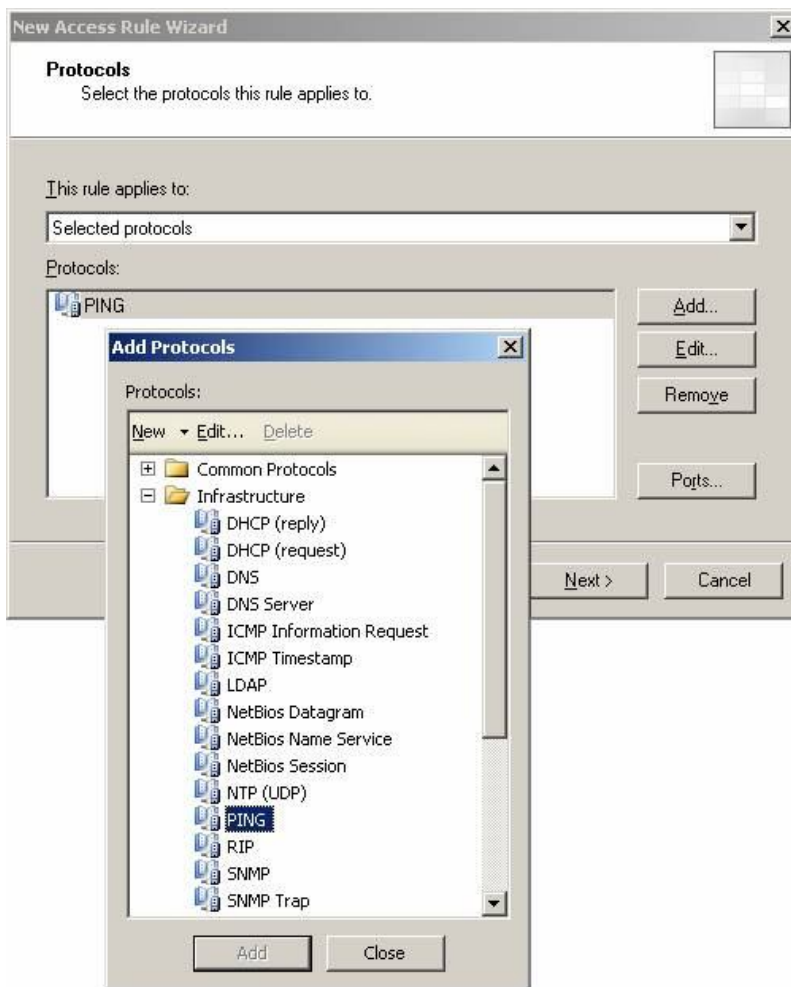
2. Trong tab **Tasks** trong Task Pane, kích liên kết **Create Access Rule**.

3. Trong trang **Welcome to the New Access Rule Wizard**, nhập vào tên rule trong hộp **Access Rule name**. Trong ví dụ này chúng tôi sử dụng tên **Ping Main to Branch** và kích **Next**.

4. Trong trang **Rule Action**, chọn tùy chọn **Allow** và kích **Next**.

5. Trong trang **Protocols**, chọn tùy chọn **Selected protocols** từ danh sách sổ xuống **This rule applies to**. Kích nút **Add**. Trong hộp thoại **Add Protocols**, kích thư mục **Infrastructure**, sau đó kích đúp giao thức **PING**. Kích **Close**.





Hình 12

6. Trong trang **Access Rule Sources**, kích nút **Add**. Trong hộp **Add Network Entities**, kích thư mục **Networks**, sau đó kích đúp mạng **Internal**. Kích **Close**.

7. Kích **Next** trong trang **Access Rule Sources**.

8. Trong trang **Access Rule Destinations**, kích nút **Add**. Trong hộp thoại **Add Network Entities**, kích thư mục **Networks**, sau đó kích mạng **Branch**. Kích **Close**.

9. Trong trang **User Sets**, chấp nhận thiết lập mặc định, **All Users**, và kích **Next**.

10. Kích **Finish** trong trang **Completing the New Access Rule Wizard**.

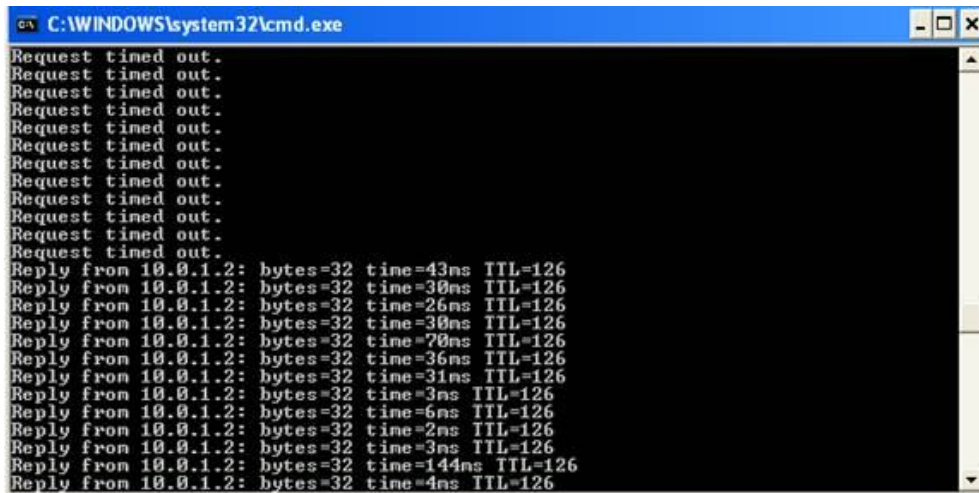
11. Kích **Apply** để lưu các thay đổi và cập nhật chính sách tường lửa. Kích **OK** trong hộp **Apply New Configuration**.

Mặc dù chúng ta đã cấu hình VPN site to site nhưng chưa kích hoạt ISA Firewall văn phòng chính để nó là một máy chủ VPN truy cập xa. Thực hiện các bước dưới đây để kích hoạt máy chủ VPN:

1. Tại máy CSS văn phòng chính, kích nút **Virtual Private Networking (VPN)** trong cây mạng **Main**.

2. Trong nút **Virtual Private Networking (VPN)**, kích vào **Tasks tab** trên Task Pane. Kích liên kết **Enable VPN Client Access**.
3. Kích **OK** trong hộp thoại thông báo cho bạn rằng dịch vụ RRAS có thể khởi động lại.
4. Kích **Apply** để lưu các thay đổi và cập nhật chính sách tường lửa. Kích **OK** trong hộp thoại **Apply New Configuration**.

Giờ đây chúng ta đã kích hoạt kết nối VPN từ máy khách VPN của mình (bằng PPTP, giao thức mặc định được cho phép trong các kết nối VPN sau khi kích hoạt máy chủ VPN trên ISA Firewall). Khi đã kết nối, chúng ta bắt đầu thực hiện một lệnh **ping -t 10.0.1.2**, đó là DC tại văn phòng chi nhánh. Sau một khoảng thời gian thực hiện, bạn sẽ thấy quá trình ping thành công, xem hình bên dưới.



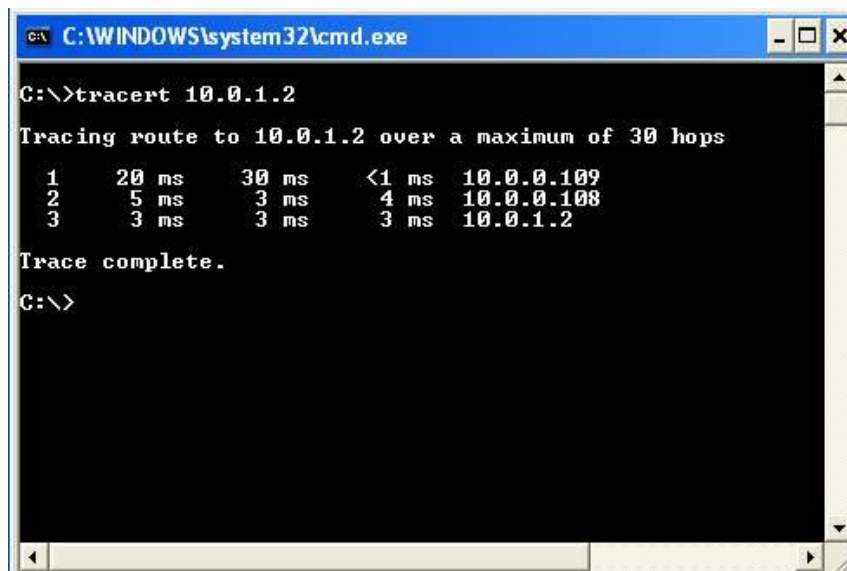
Hình 13

Nếu quan sát việc ghi chép thời gian thực cho mạng văn phòng chi nhánh, chúng ta có thể thấy rule **Ping Main to Branch** đang cho phép kết nối, như thể hiện trong hình bên dưới.

10.0.0.107	10.0.1.2	0	PING	Denied Connection	[Enterprise] Defa... (
10.0.0.107	10.0.1.2	0	PING	Denied Connection	[Enterprise] Defa... (
10.0.0.107	10.0.1.2	0	PING	Initiated Connection	Ping Main to Branch (
10.0.0.108	10.0.0.2	0	PING	Closed Connection	[System] Allow IC... (

Hình 14

Và nếu thực hiện một **tracert** từ máy khách VPN đến DC tại văn phòng chi nhánh, chúng ta sẽ thấy nó sử dụng ISA Firewall văn phòng chi nhánh với tư cách là gateway cho location đó, xem hình bên dưới.



```
C:\WINDOWS\system32\cmd.exe
C:\>tracert 10.0.1.2
Tracing route to 10.0.1.2 over a maximum of 30 hops
  1    20 ms    30 ms    <1 ms   10.0.0.109
  2     5 ms     3 ms     4 ms   10.0.0.108
  3     3 ms     3 ms     3 ms   10.0.1.2
Trace complete.
C:\>
```

Hình 15

## Kết luận

Trong bài này, chúng tôi đã bổ sung thêm cho các bạn một số kiến thức mạng VPN site to site bằng cách giới thiệu cách kích hoạt truy cập máy khách VPN từ xa cho các mạng ở xa được kết nối qua liên kết VPN site to site. Có hai thứ được yêu cầu để thực hiện công việc này: đầu tiên, phải có một rule mạng để kết nối mạng nguồn với mạng đích, thứ hai, phải có các Access Rule thích hợp tại cả ISA Firewall văn phòng chính và chi nhánh để cho phép lưu lượng. Khi đã có các Network Rules và Access Rules thích hợp,

bạn sẽ có sự truyền thông từ các máy khách VPN  
truy cập xa đến các mạng từ xa của mình.