WINDOWS FIREWALL WITH ADVANCE SECURITY ON WINDOWS SERVER 2008

I. TỔNG QUÁT

Windows Firewall with Advanced Security trên Windows Server 2008 là một sự kết hợp giữa personal firewall (host firewall) và Ipsec,cho phép bạn cấu hình để lọc các kết nối vào và ra trên hệ thống.

Không giống như những firewall ở các phiên bản Windows trước chỉ sử dụng Windows Firewall trong Control Panel để thực hiện các thao tác cấu hình ở mức độ giới hạn.

Trong Windows Server 2008 bổ sung một thành phần mới có tên gọi là Windows Firewall with Advance Security.

Công cụ này cho phép bạn dễ dàng thực hiện các thao tác cấu hình đa dạng và cao cấp trên firewall,những điểm mới đáng chú ý là :

1. Điều khiển kết nối ra vào trên hệ thống (inbound và outbound)
2. Tích hợp chặt chẽ với Server Manager.Khi bạn sử dụng Server Manager để cài đặt dịch vụ,firewall sẽ được cấu hình một cách tự động để phù hợp với các dịch vụ vừa cài đặt.
3. Những cải tiến trong quản lý và cấu hình các chính sách trên IPsec.Đồng thời ,IPsec cũng được thay bằng một khái niệm mới ,đó là **Connection Security Rules**.
4. Những cải tiến trong hoạt động giám sát các chính sách trên firewall và IPsec (Connection Security Rules)

Windows Firewall with Advance Security sử dụng hai loại rule để cấu hình :

1. **Firewall rules** : dùng để xác định kết nối nào được cho phép hoặc bị cấm
2. **Connection Security rules** : phục vụ cho mục đích bảo mật đường truyền giữa máy tính này với các máy tính khác

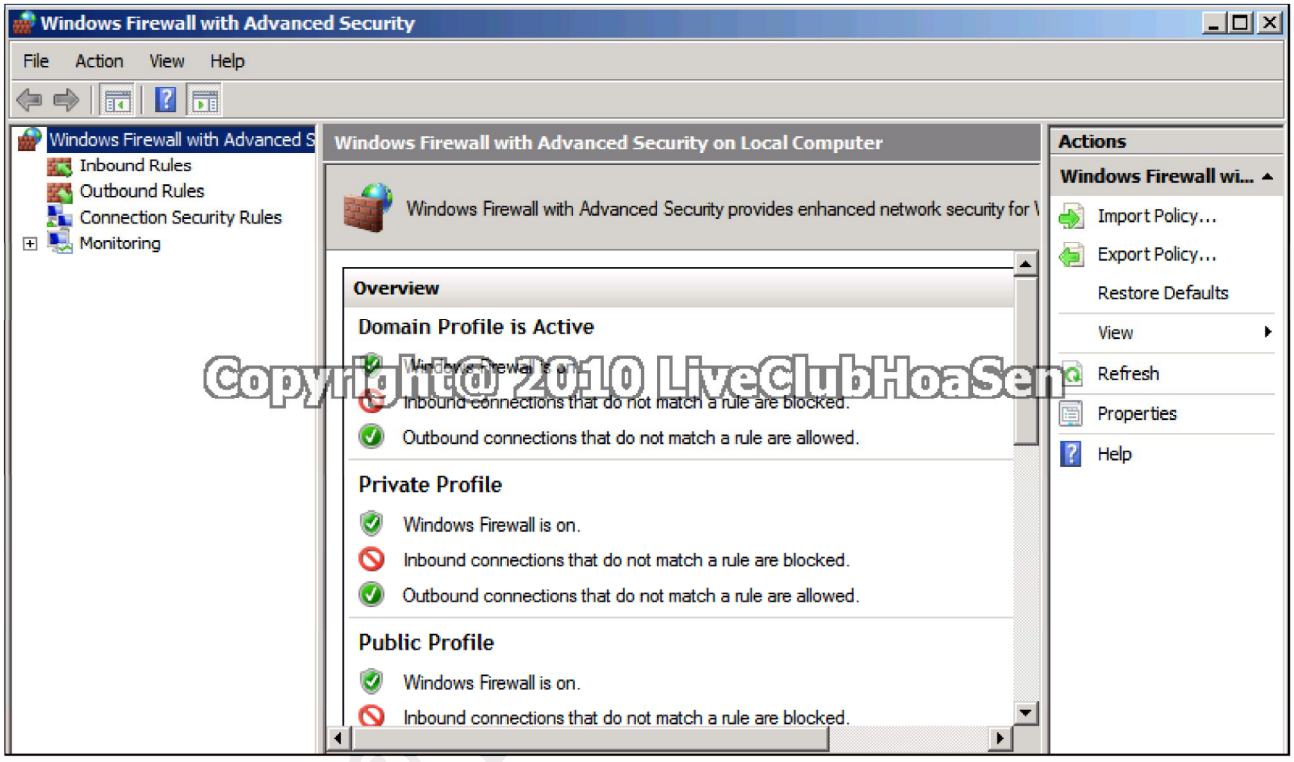
Sau khi hoàn thành việc xây dựng các rule,bạn sẽ dựa vào các firewall profile để áp dụng rule cho máy tính.Firewall profile là khái niệm dùng để chỉ vị trí mà máy tính đã kết nối.Trên Windows Server 2008 có ba loại firewall profile sau:

1. **Domain** : áp dụng khi một máy tính đã được kết nối vào domain
2. **Private** : áp dụng khi một máy tính đã trở thành thành viên của mạng nội bộ nhưng chưa kết nối vào domain.

3. **Public** : áp dụng khi một máy tính đã kết nối vào các hệ thống mạng công cộng,chẳng hạn như Internet.

II. LÀM QUEN GIAO DIỆN

Để mở Windows Firewall with Advance Security vào **Start → Administrative Tools → Windows Firewall with Advance Security**



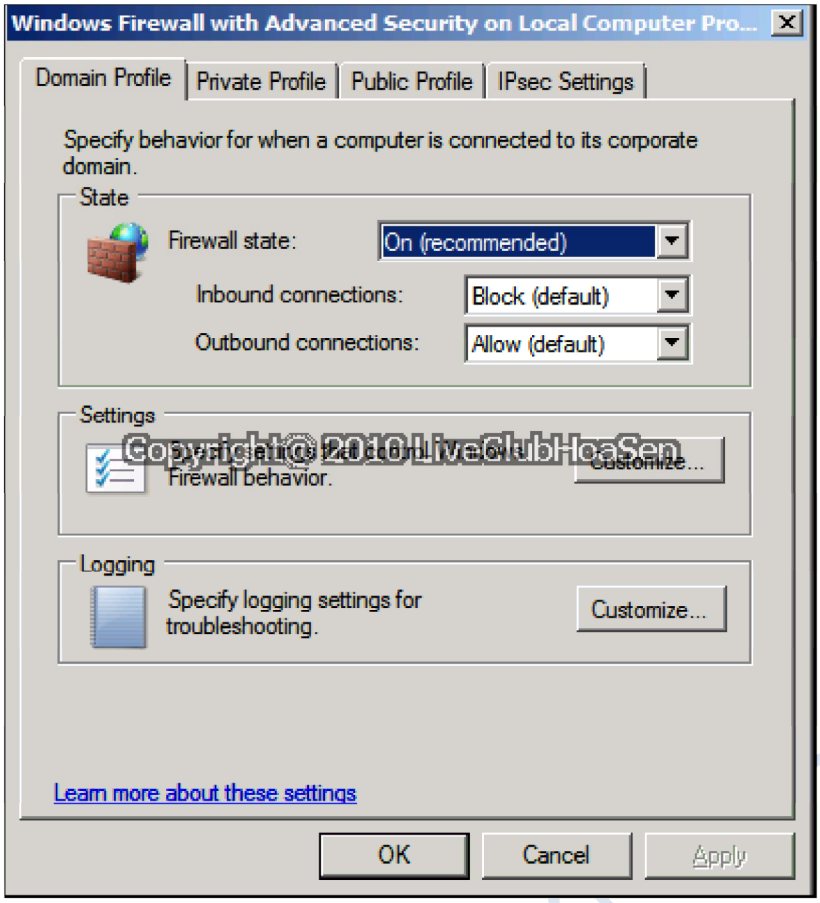
Copyright@ 2010 LiveClubHoaSen

Ở bảng Windows Firewall with Advance Security on Local Computer cung cấp thông tin về các firewall profile như Domain,Private và Public.Đây là những thiết lập mặc định.

Ở khung bên trái có các chức năng chính như **Inbound Rules**,**Outbound Rules**,**Connection Security Rules** và **Monitoring** .

Ở khung Action bên phải là **Import Policy**,**Export Policy** để đưa các chính sách vào và đưa ra.

Chúng ta sẽ khảo sát một số thuộc tính mặc định của Windows Firewall with Advance Security.Ở khung **Actions** bên phải chọn **Properties**

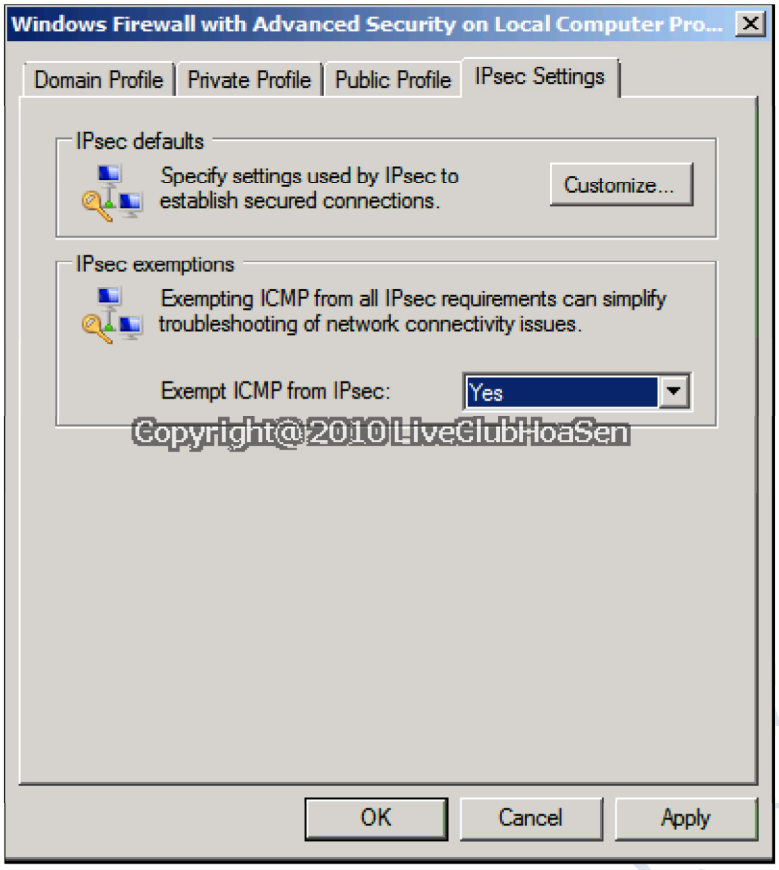


Ở tab **Domain Profile**:

- **Firewall state** : cho phép thay đổi giữa 2 trạng thái của firewall là On hoặc Off.
- **Inbound connections** : điều khiển các kết nối đến máy tính này .Giá trị mặc định là **Block(default)** sẽ khóa tất cả các kết nối không thỏa mãn một trong các rule đã được định nghĩa trên firewall.Ngoài ra còn có 2 tùy chọn khác là Allow và Block all connections.**Allow** là cho phép tất cả các kết nối đến và **Block all connections** chặn các kết nối đến.
- **Outbound connections** : điều khiển các máy tính đi ra từ máy tính này.Giá trị mặc định là Allow(default),cho phép thực hiện các kết nối đến những hệ thống khác.Nếu sử dụng tùy chọn Block,bạn sẽ cấm máy tính này thiết lập các kết nối trong mạng.Do đó,bạn nên giữ nguyên giá trị mặc định để đảm bảo máy tính của mình có thể làm việc tốt.
- **Settings** : chọn **Customize** để thực hiện một số thiết lập bổ sung cho firewall.
- **Logging** : chọn **Customize** để thay đổi các thiết lập mặc định của hệ thống file log

Ở tab **Private Profile** và tab **Public Profile** tương tự như **Domain Profile.**Đây là các thiết lập dành cho những máy tính không thuộc domain.

Ở tab **IPsec Settings :**

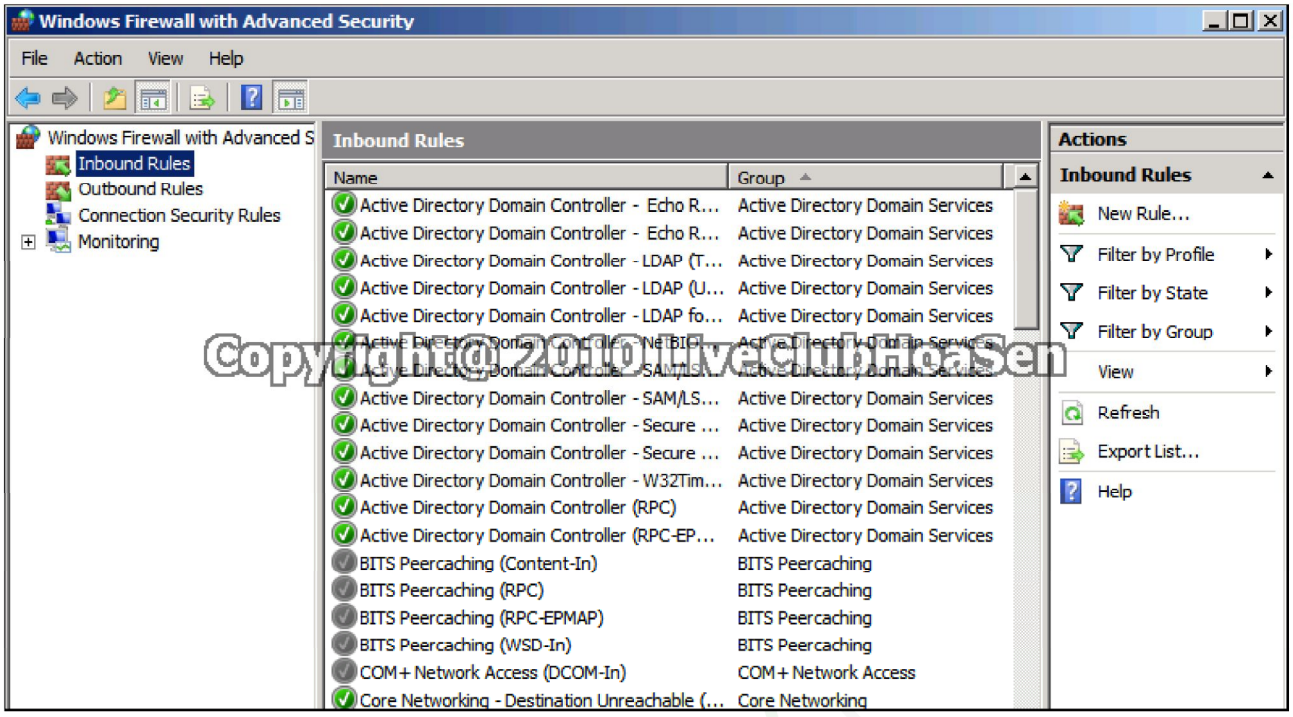


- **IPsec defaults** bao gồm những thiết lập mặc định sẽ được áp dụng khi bạn tạo ra một Connection Security Rule mới.Để thay đổi bạn chọn **Customize.**Lưu ý là bạn có thể hiệu chỉnh các thiết lập này trong quá trình tạo mới một Connection Security Rule.
- **IPsec exemptions** giúp bạn dễ dàng tìm kiếm và khắc phục sự cố trong hệ thống mạng sử dụng IPsec.Nếu thay đổi giá trị mặc định thành **Yes** ,bạn sẽ dễ dàng sử dụng công cụ như **Ping,Tracert**….để dò tìm nguyên nhân và xử lý sự cố.

FIREWALL RULE

Windows Firewall with Advance Security bao gồm 2 loại firewall rule là Inbound Rules và Outbound Rules.Các firewall rule này cho phép bạn tạo ra các rule nhằm điều khiển các kết nối đến và đi từ máy tính chạy hệ điều hành Windows Server 2008

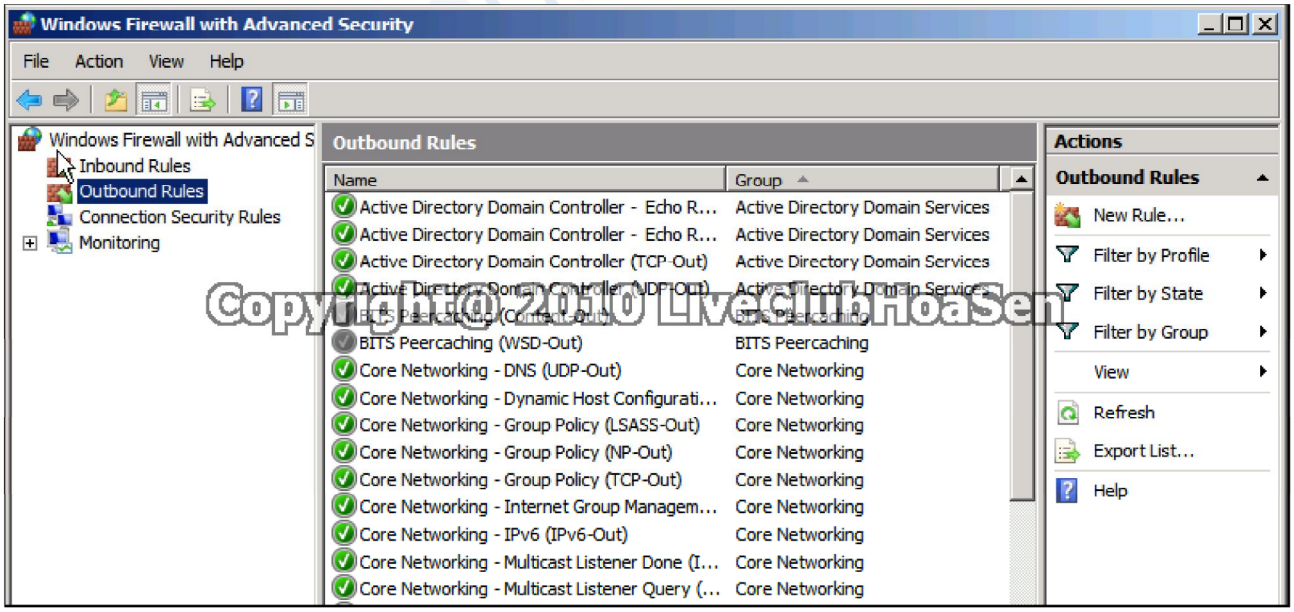
Trong màn hình làm việc của Windows Firewall with Advance Security,click chọn **Inbound Rules**.Bạn sẽ thấy xuất hiện một danh sách firewall rule trên hệ thống,trong khung ở giữa.



Copyright@ 2010 LiveClubHoaSen

Các firewall rule này được tạo ra một cách tự động khi bạn cài đặt các dịch vụ cũng như bổ sung các thành phần vào server.Lưu ý : trong danh sách ở trên chưa có một firewall rule nào có khả năng cho phép các kết nối từ máy tính khác đến máy tính này.

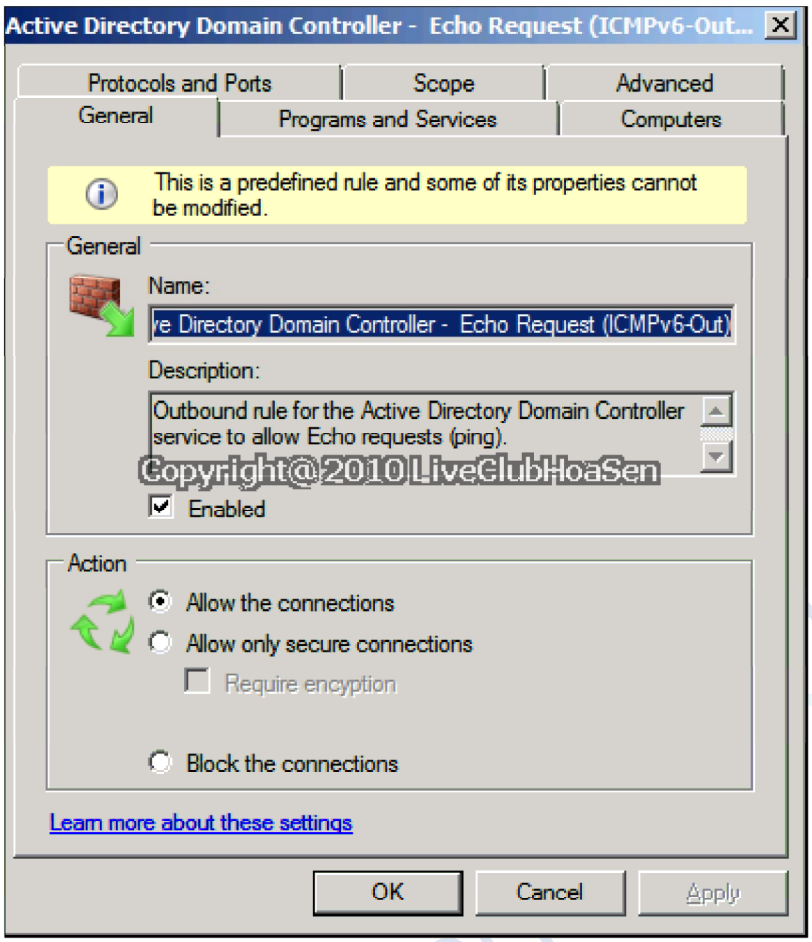
Với **Outbound Rules** cũng tương tự.



Copyright@ 2010 LiveClubHoaSen

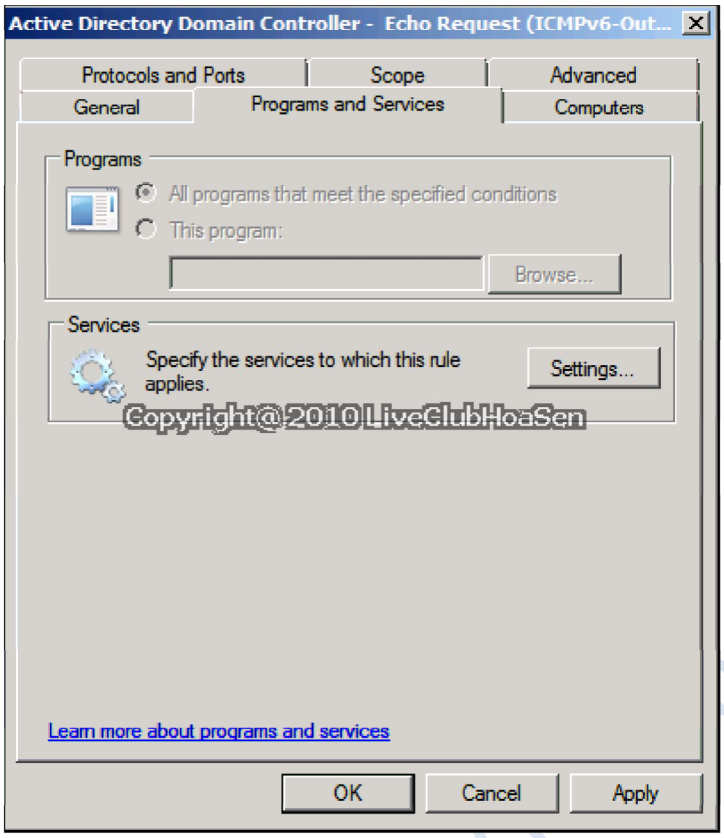
Bạn cũng có thể sắp xếp và xem từng loại firewall rule áp dụng cho firewall profile bằng cách nhấp chuột phải vào Inbound Rules hoặc Outbound Rules và ,lọc theo các điều kiện như Profile ,State,Group .Sau đó chọn Filter by…..

Nếu muốn xem chi tiết của một firewall rule ,click đúp vào rule đó.

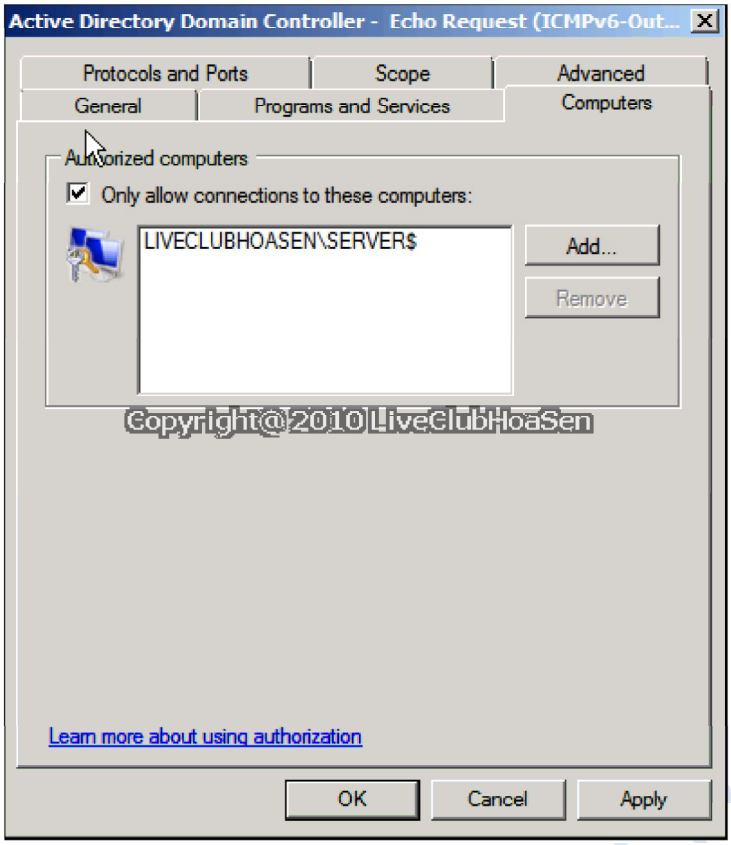


Trên tab **General**,bạn xem và thay đổi trạng thái của firewall rule bằng cách đánh dấu hoặc bỏ chọn mục **Enabled**.Đồng thời ở mục **Action**,chọn một trong 3 chế độ **Allow the connections**,**Allow only secure connections** và **Block the connections** để cho phép hoặc chặn kết nối tương ứng.

Trên tab **Programs and Services**,bạn có thể thực hiện các thao tác nhằm cho phép hoặc cấm truy cập đến các dịch vụ hoặc ứng dụng được cài đặt trên hệ thống.Để thiết lập ứng dụng hoặc dịch vụ cụ thể,sử dụng các chức năng **Browse** hoặc **Settings**.

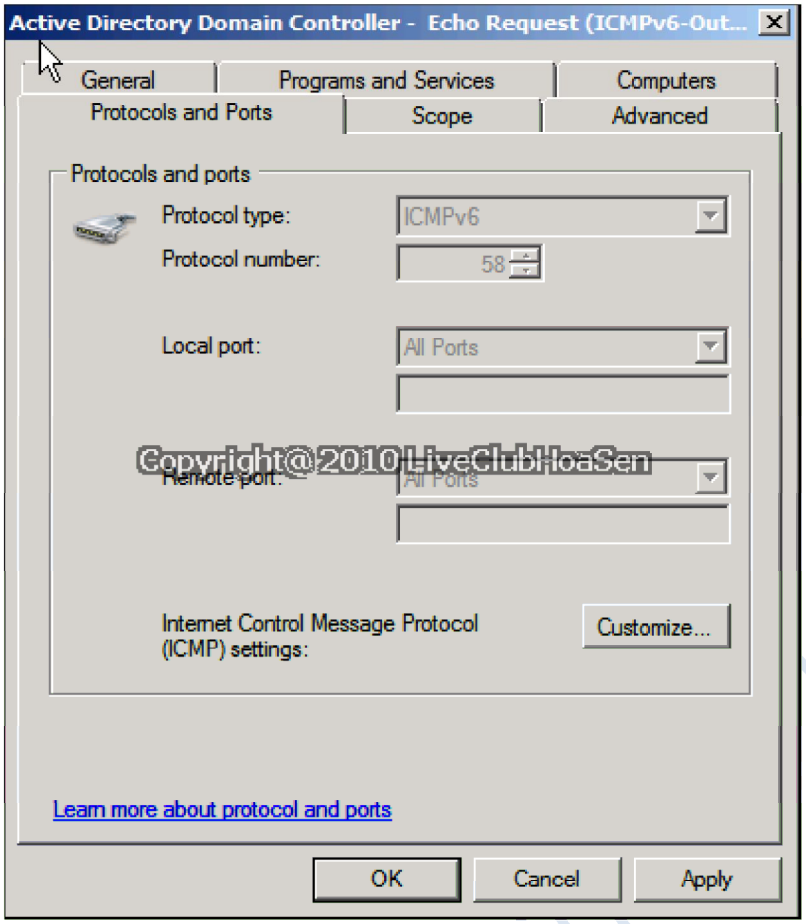


Ở tab **Users and Computers**,bạn có thể thiết lập nhóm user hoặc computer mà firewall rule này sẽ áp dụng.việc này được thực hiện bằng cách đánh dấu chọn vào một trong hai mục **Only allow connection from these computers** và **Only allow connections from these users.**Sau đó sử dụng chức năng **Add** để bổ sung user và compute tương ứng.



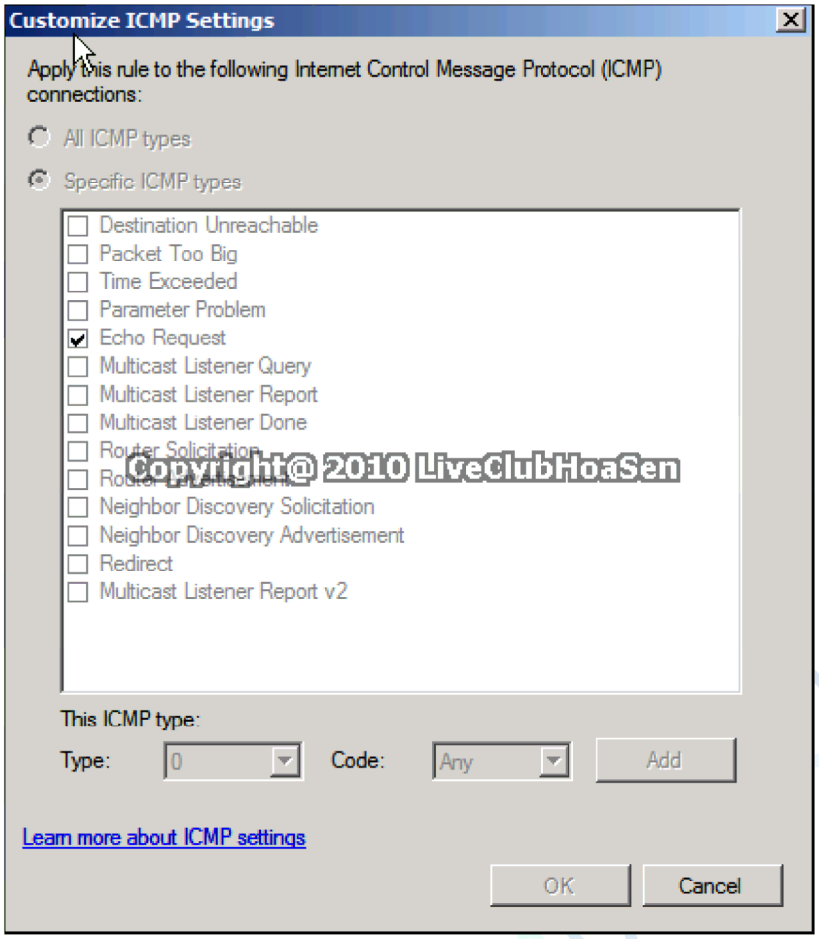
Lưu ý : để xác thực user và computer,bạn cần thiết lập **Allow only secure connections** ở mục **Action** của tab **General.**Đồng thời user và computer đó phải thuộc domain và IPsec phải được cấu hình trên các hệ thống tham gia vào quá trình xác thực.

Trên tab **Protocols and Ports,**thiết lập giao thức và port mà firewall rule sẽ áp dụng.

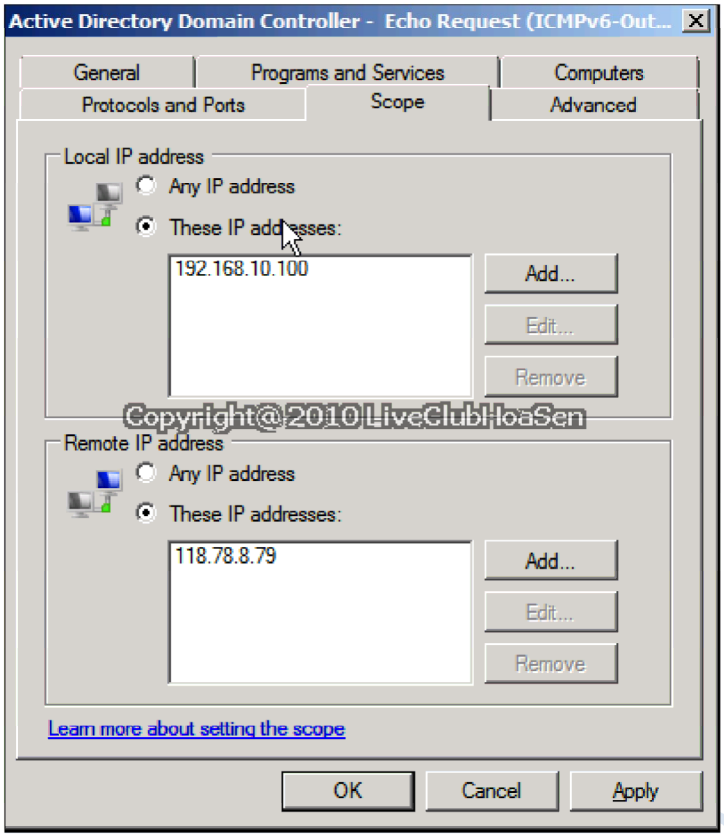


Copyright@2010 LiveClub HoaSen

- **Protocol type** : bạn chọn một giao thức tương ứng trong danh sách như UDP,TCP,ICMP……
- **Protocol number** : bạn nên sử dụng giá trị mặc định của hệ thống .Tất nhiên bạn cũng có thể điền giá trị thích hợp với giao thức của mình
- **Local port** : bạn thiết lập port của server ứng với firewall rule.Nếu tạo một inbound rule,port này sẽ được máy chủ dùng để lắng nghe các yêu cầu truy cập đến.Nếu tạo một outbound rule,port này sẽ được server sử dụng để thiết lập kết nối đến các máy tính khác.
- **Remote port**: bạn thiết lập port của máy tính khác mà firewall rule này sẽ áp dụng (remote machine).Nếu tạo một outbound rule ,đây sẽ là port trên một máy tính ở xa mà server này sẽ kết nối đến (destination port).Nếu tạo một inbound rule,đây chính là port mà máy tính ở xa sử dụng để kết nối đến server này.(source port)
- **Internet Control Message Protocol (ICMP) settings** : nếu bạn muốn thiết lập trên giao thức ICMP ,chọn **Customize** .



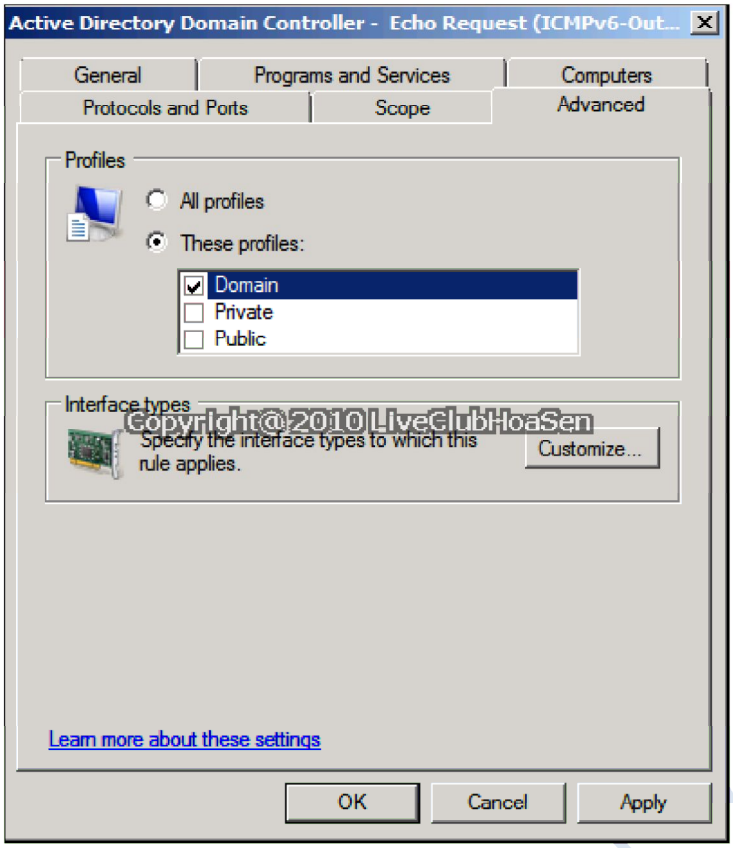
Ở tab **Scope** cho phép bạn thiết lập các giá trị trong mục **Local IP address** và **Remote IP addess** để firewall rule này áp dụng.

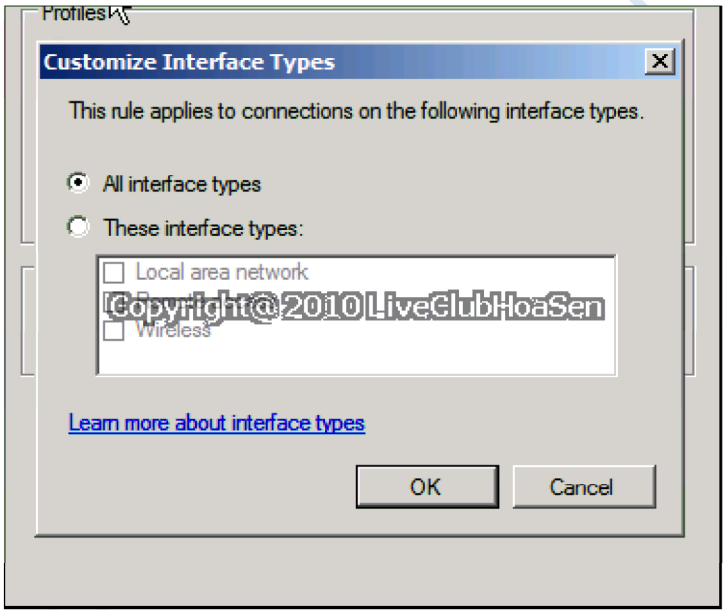


- **Local IP address** là địa chỉ IP mà server này hoặc dùng để lắng nghe kết nối từ máy tính khác đến với inbound rule,hoặc dùng làm địa chỉ IP nguồn cho mình để thiết lập kết nối đến các máy tính khác với outbound rule.
- **Remote IP address** là địa chỉ IP của máy tính ở xa mà server này sẽ kết nối đến với outbound rule,hoặc đây sẽ là địa chi IP nguồn mà máy tính ở xa sẽ sử dụng để kết nối đến server này với inbound rule

Để thêm IP bạn chọn Add và thêm ,có các mục cho bạn tùy chọn.Có thể là dãy IP hoặc chỉ một IP hay subnet.

Ở tab **Advance**,bạn có thể thiết lập các profile và các loại kết nối (interface type) sẽ sử dụng trong firewall rule này.Bạn có thể thiết lập tất cả các profile hoặc một số profile phù hợp.Nếu muốn cấu hình các loại kết nối này chọn **Customize** ở mục **Interface type** và lựa chọn tương ứng.





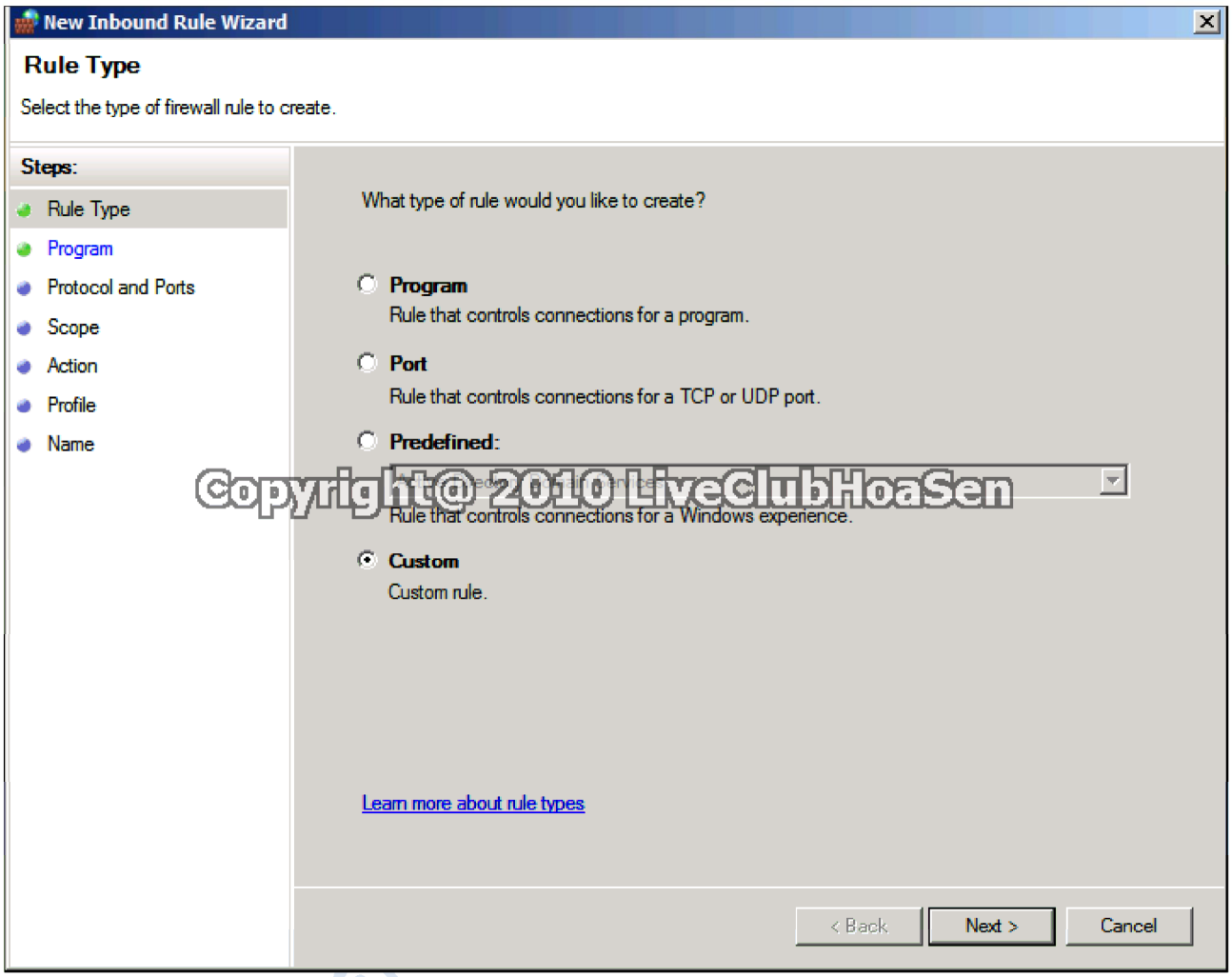
Copyright@2010 LiveClubHoaSen

III. TẠO MỘT FIREWALL RULE

Tạo một firewall rule cho Inbound.(Với outbound bạn làm tương tự)

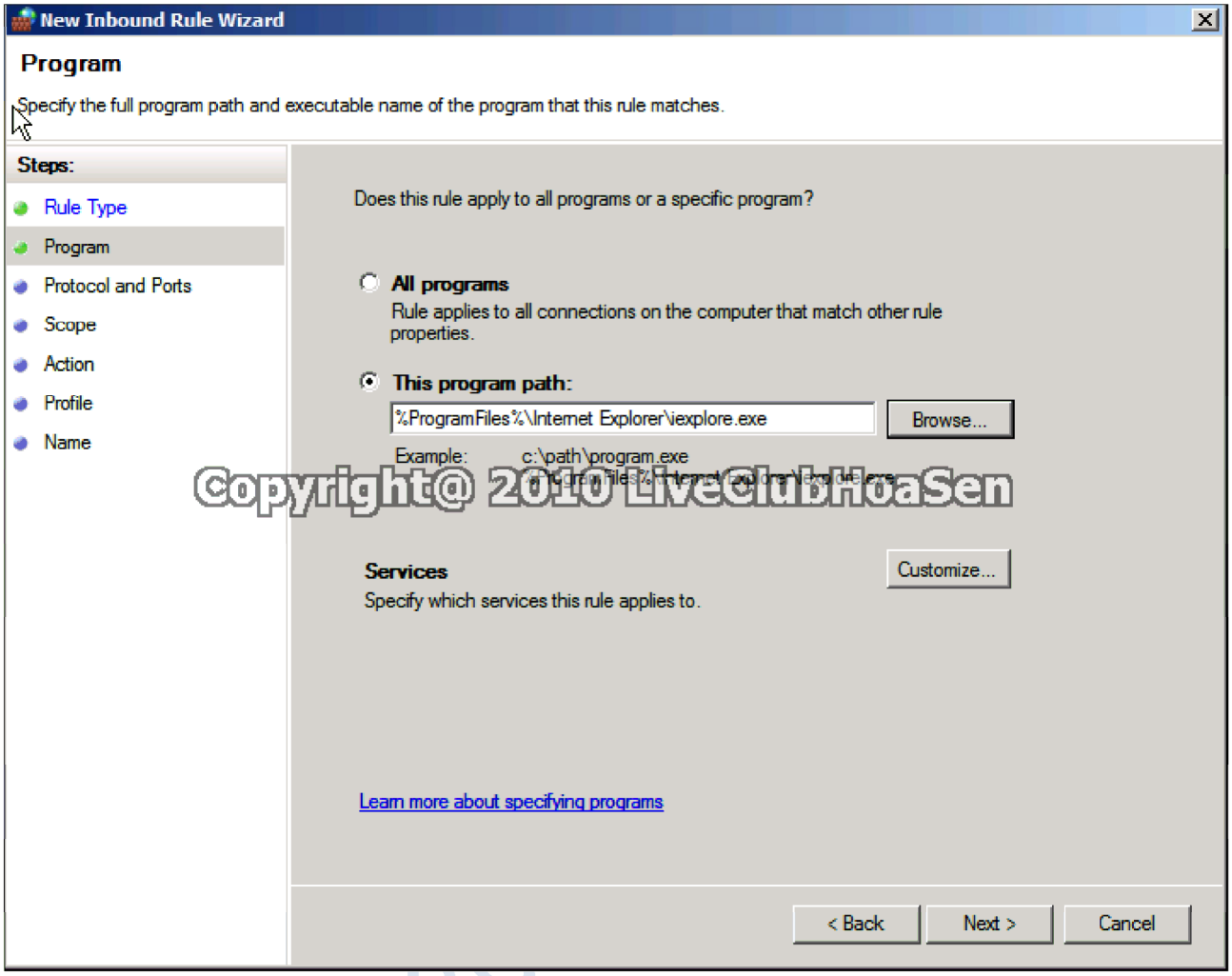
Nhấp chuột phải vào **Inbound Rules** và chọn **New Rule**.

Tại bảng Rule Type chọn Custom để chỉnh được các tùy chọn.



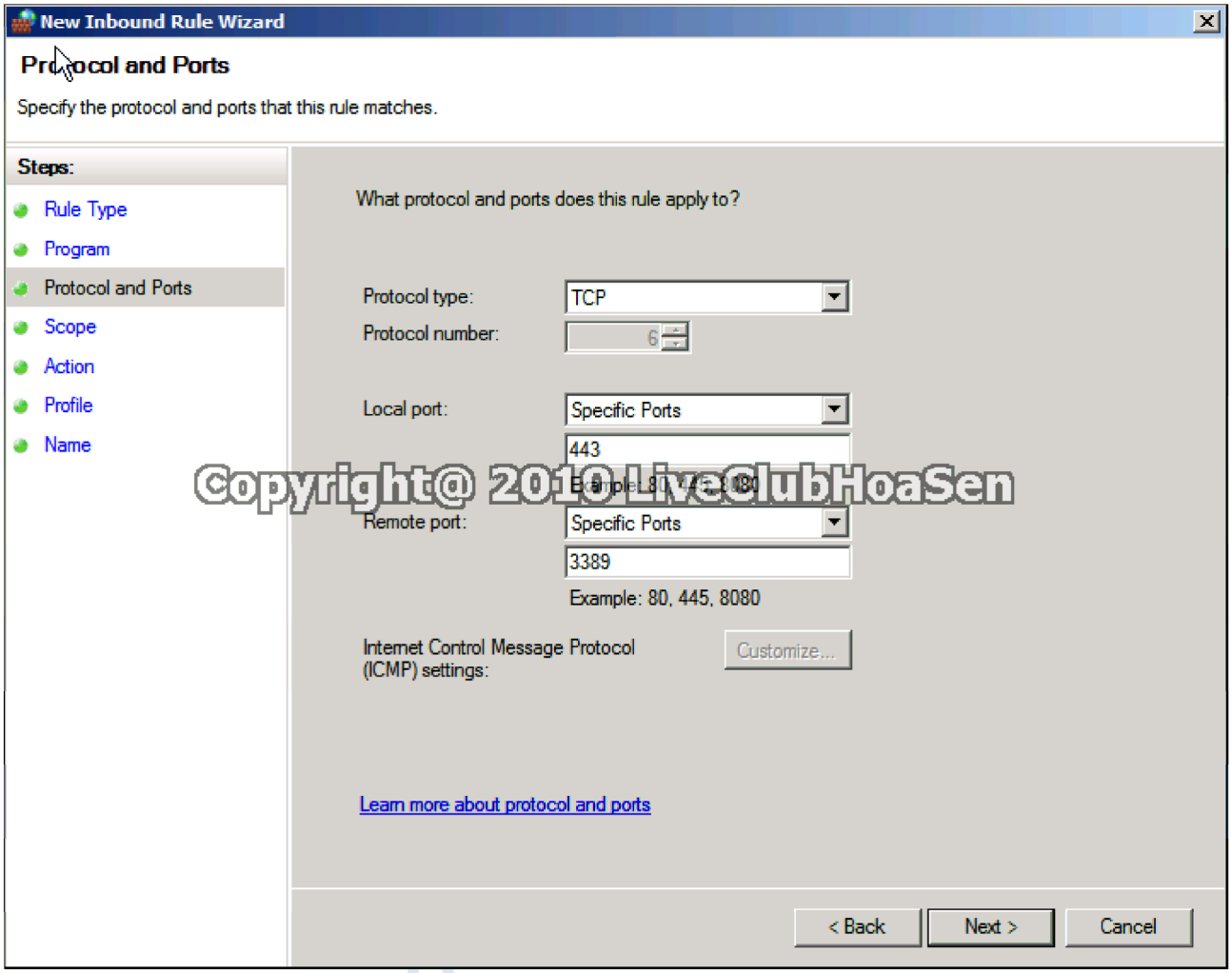
Copyright@ 2010 LiveClubHoaSen

Chọn **Next** để tiếp tục.Tại bảng **Program** bạn có thể chọn **All Program** để áp dụng cho tất cả chương trình hoặc chọn chương trình cụ thể nếu chọn **This program path**.Sau đó chọn **Browse** và tới chương trình đó.



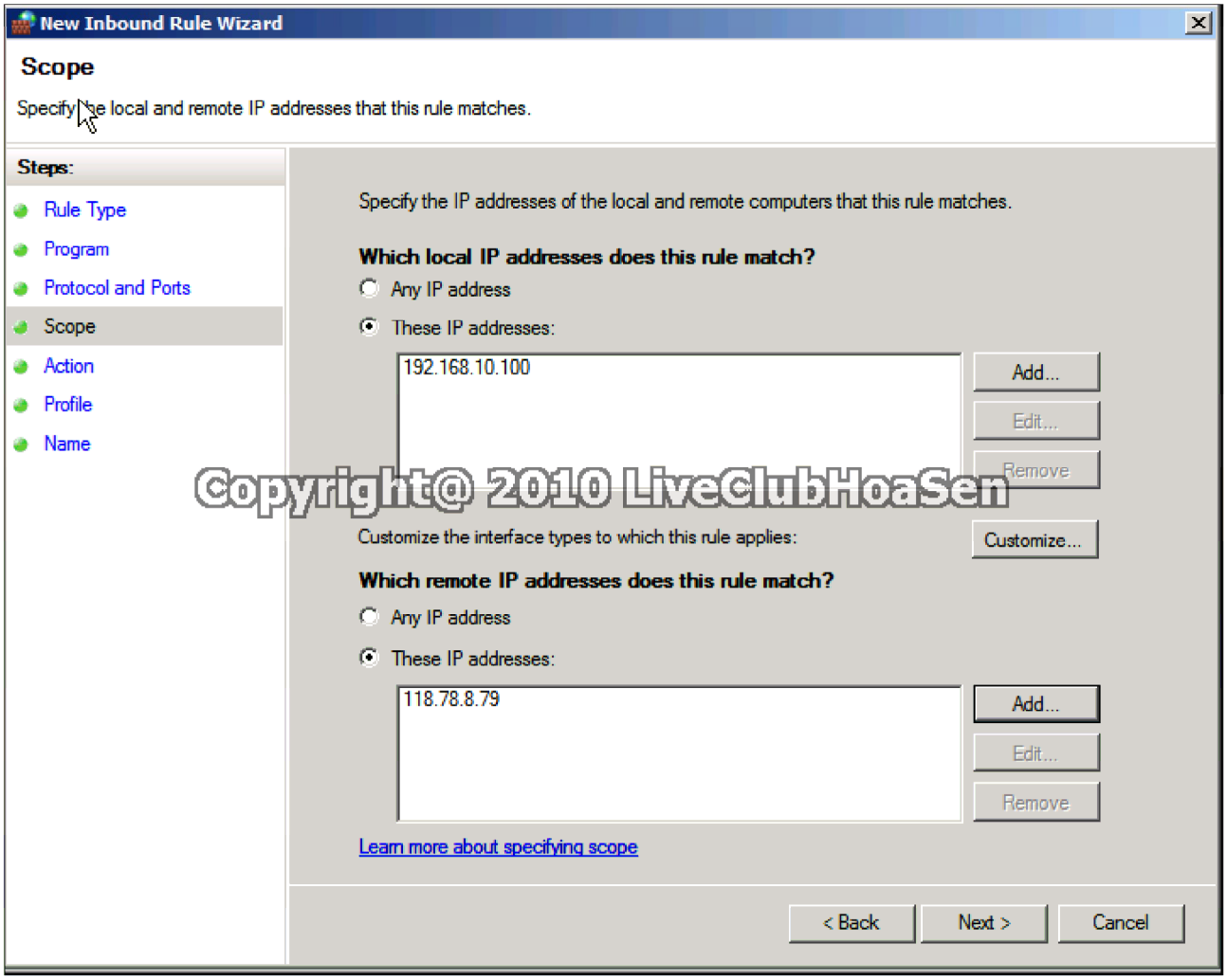
Copyright@ 2010 LiveClubHoaSen

Chọn **Next** để tiếp tục.Tại bảng **Protocol and Ports**,chọn giao thức phù hợp ở mục **Protocol type**.Đồng thời ở 2 mục **Local port** và **Remote port**,chọn các port phù hợp và điền giá trị port tương ứng ngay dưới.



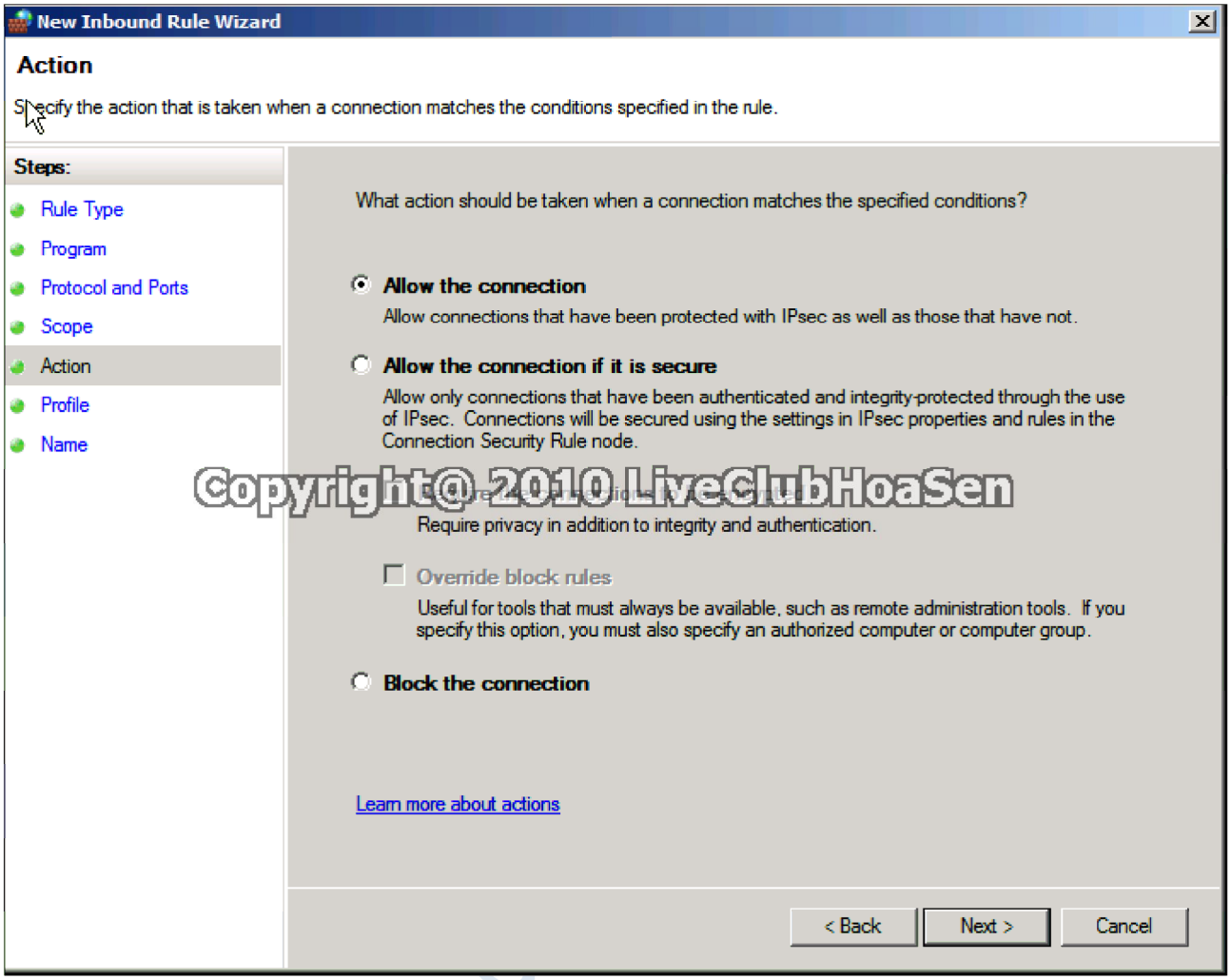
Copyright@ 2010 LiveClubHoaSen

Chọn **Next** để tiếp tục.Tại bảng **Scope** chọn kết nối phụ hợp.(Về định nghĩa Local và Remote đã có đề cập ở phần trên.)



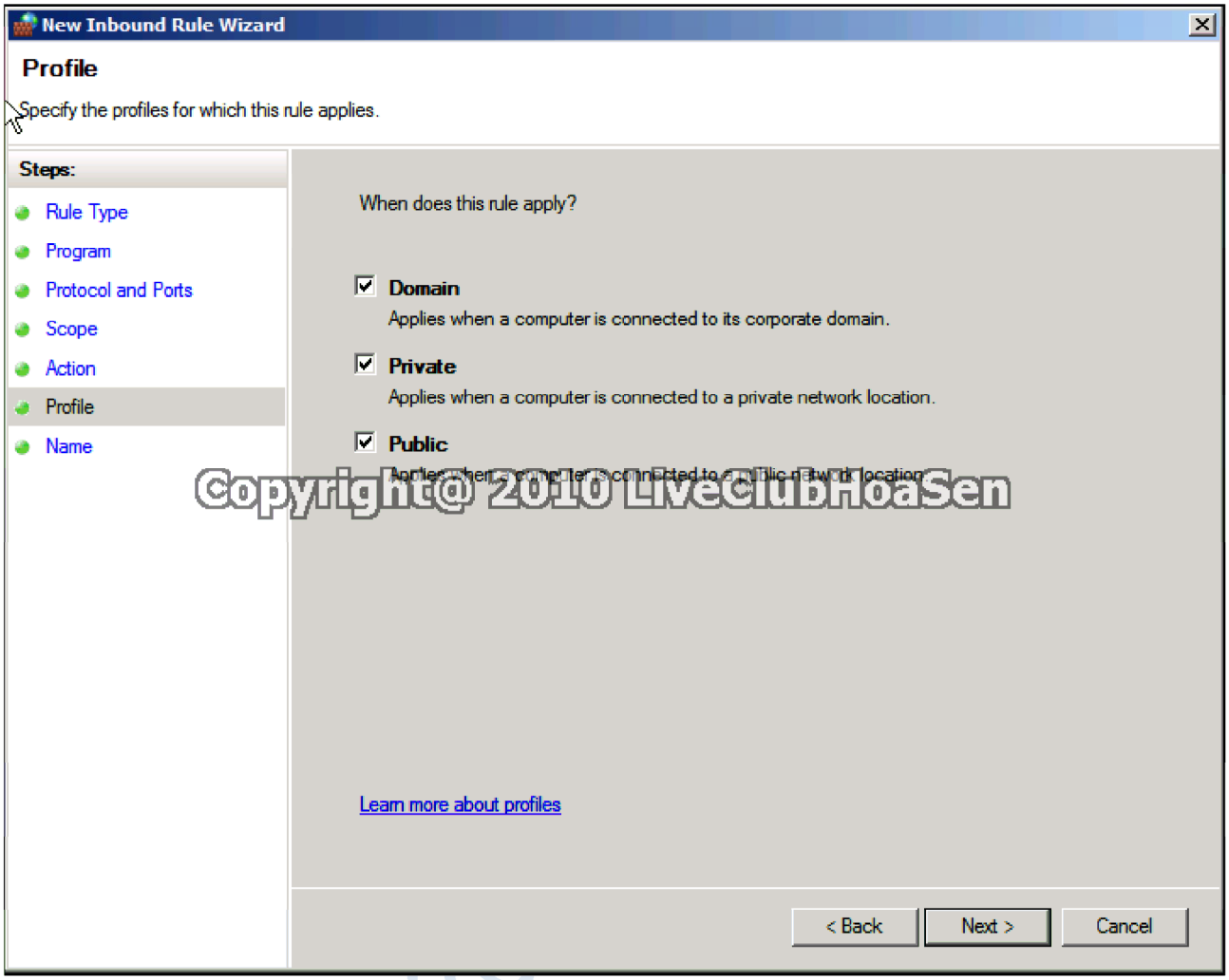
Copyright@ 2010 LiveClubHoaSen

Chọn **Next** để tiếp tục.Tại bảng **Action**,chọn **Allow the Connection** để cho phép kết nối đến. **Allow the connection if it is secure** để cho kết nối đến nhưng đảm bảo điều kiện bảo mật.Chọn **Block the connection** để ngăn chặn kết nối.



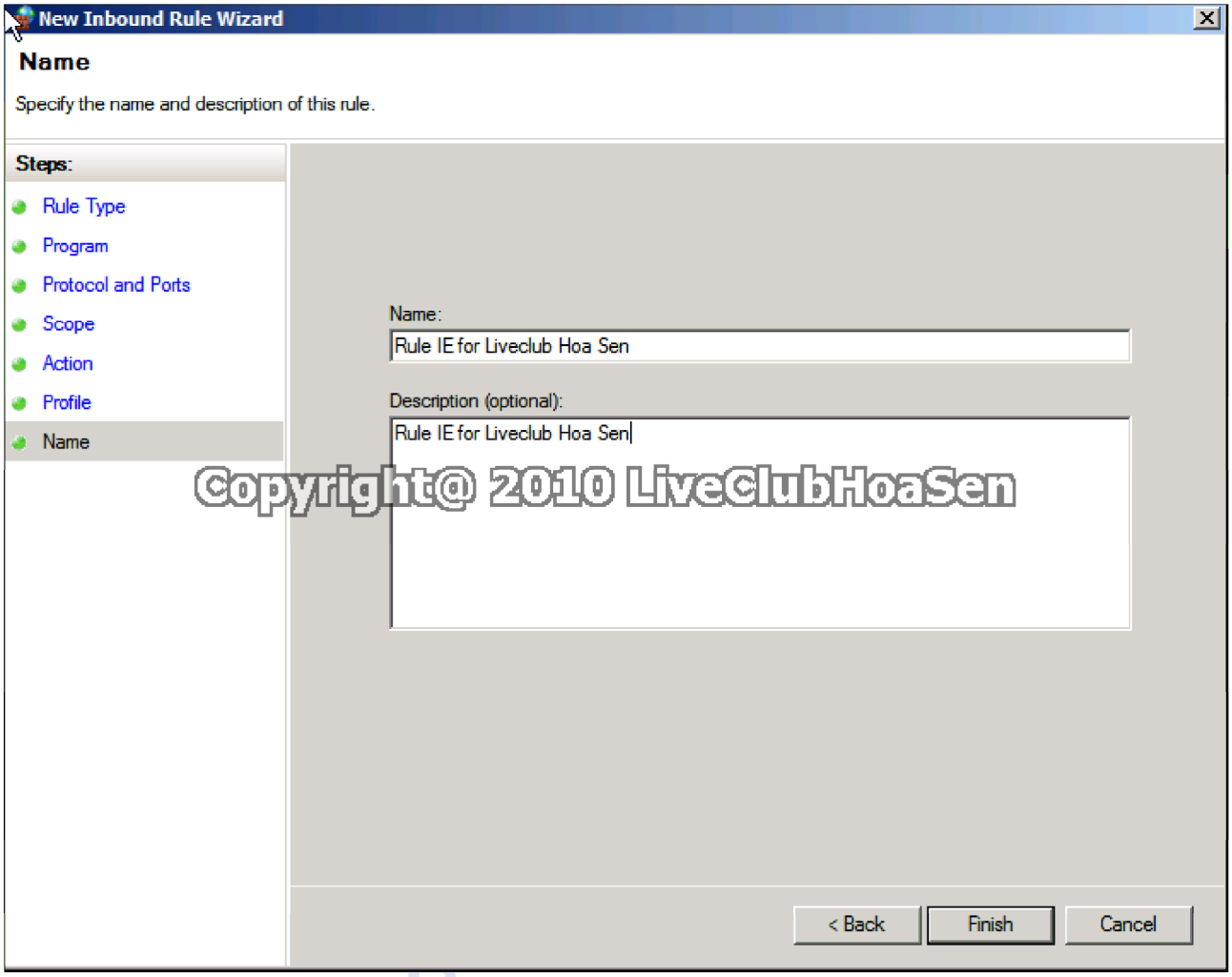
Copyright@ 2010 LiveClubHoaSen

Chọn **Next** để tiếp tục.Tại bảng **Profile** chọn kiểu profile bạn muốn áp dụng rule.



Copyright@ 2010 LiveClubHoaSen

Chọn **Next**.Tại bảng **Name** gõ tên rule và nhập thông tin chú thích về rule ở mục **Descripton**



Chọn **Finish** để kết thúc.

Lúc này đã xuất hiện Inbound rule mới .