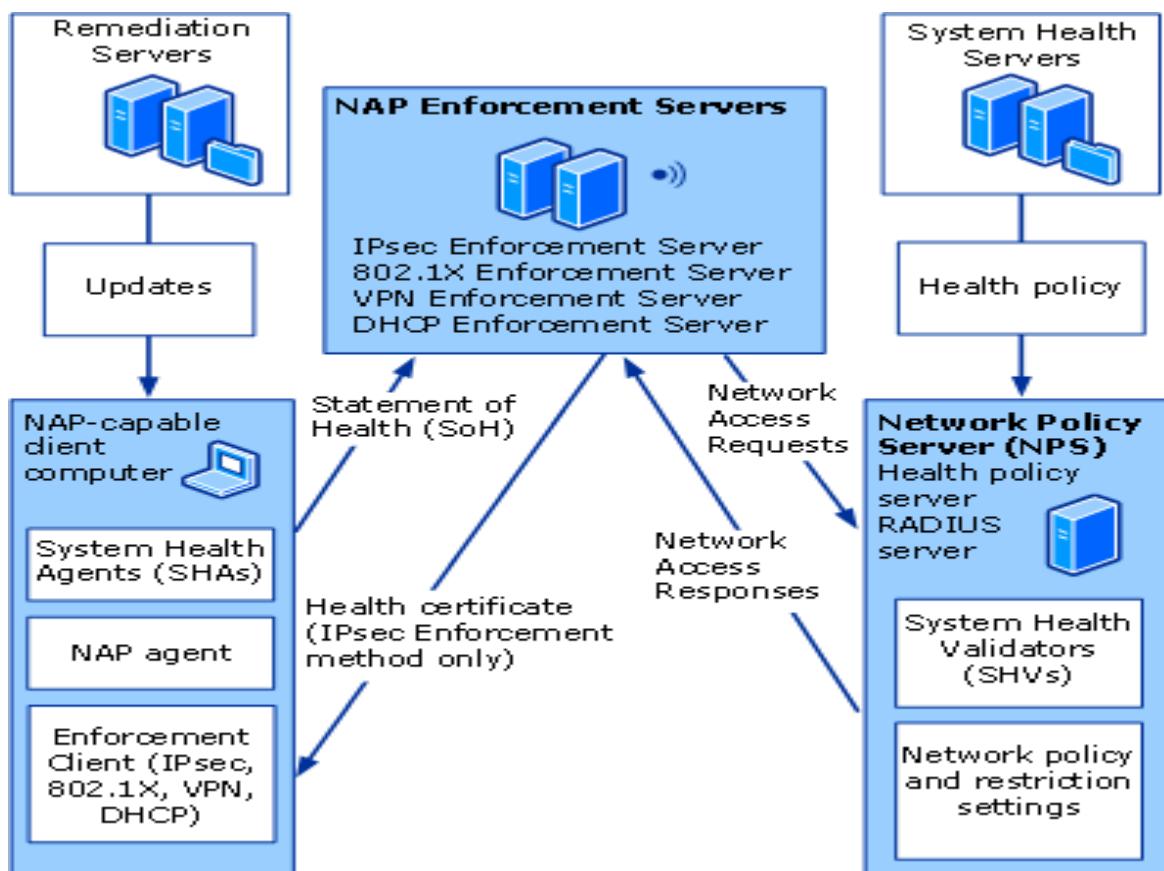


NETWORK ACCESS PROTECTION



I. GIỚI THIỆU NAP

Network Access Protection là một hệ thống chính sách thi hành (Health Policy Enforcement) được xây dựng trong các hệ điều hành Windows Server 2008, Windows Vista và Windows XP Services Park 3 là một giải pháp được thiết kế để khắc phục các vấn đề trên. Mục đích của NAP là bảo đảm các máy tính tuân theo yêu cầu bảo mật trong tổ chức của bạn. Khi một người dùng nào đó kết nối vào mạng, máy tính của người dùng có thể được mang ra so sánh với một chính sách “sức khỏe” mà bạn đã thiết lập. Các nội dung bên trong của chính sách này sẽ khác nhau tùy theo mỗi tổ chức, bạn có thể yêu cầu hệ điều hành của người dùng phải có đầy đủ các bản vá bảo mật mới nhất và máy tính phải đang chạy phần mềm chống virus được cập nhật một cách kịp thời,...và nhiều vấn đề tương tự như vậy. Nếu một máy tính có hội tụ đủ các tiêu chuẩn cần thiết mà bạn đã thiết lập trong chính sách thì máy tính này hoàn toàn có thể kết nối vào mạng theo cách thông thường. Nếu máy tính này không hội tụ đủ các yếu tố cần thiết thì bạn có thể chọn để từ chối sự truy cập mạng cho người dùng, sửa vấn đề lập tức hoặc tiếp tục và cho người dùng sự truy cập nhưng lưu ý về trạng thái của máy tính của người dùng.

Hiện nay NAP hỗ trợ triển khai trên những loại hình sau:

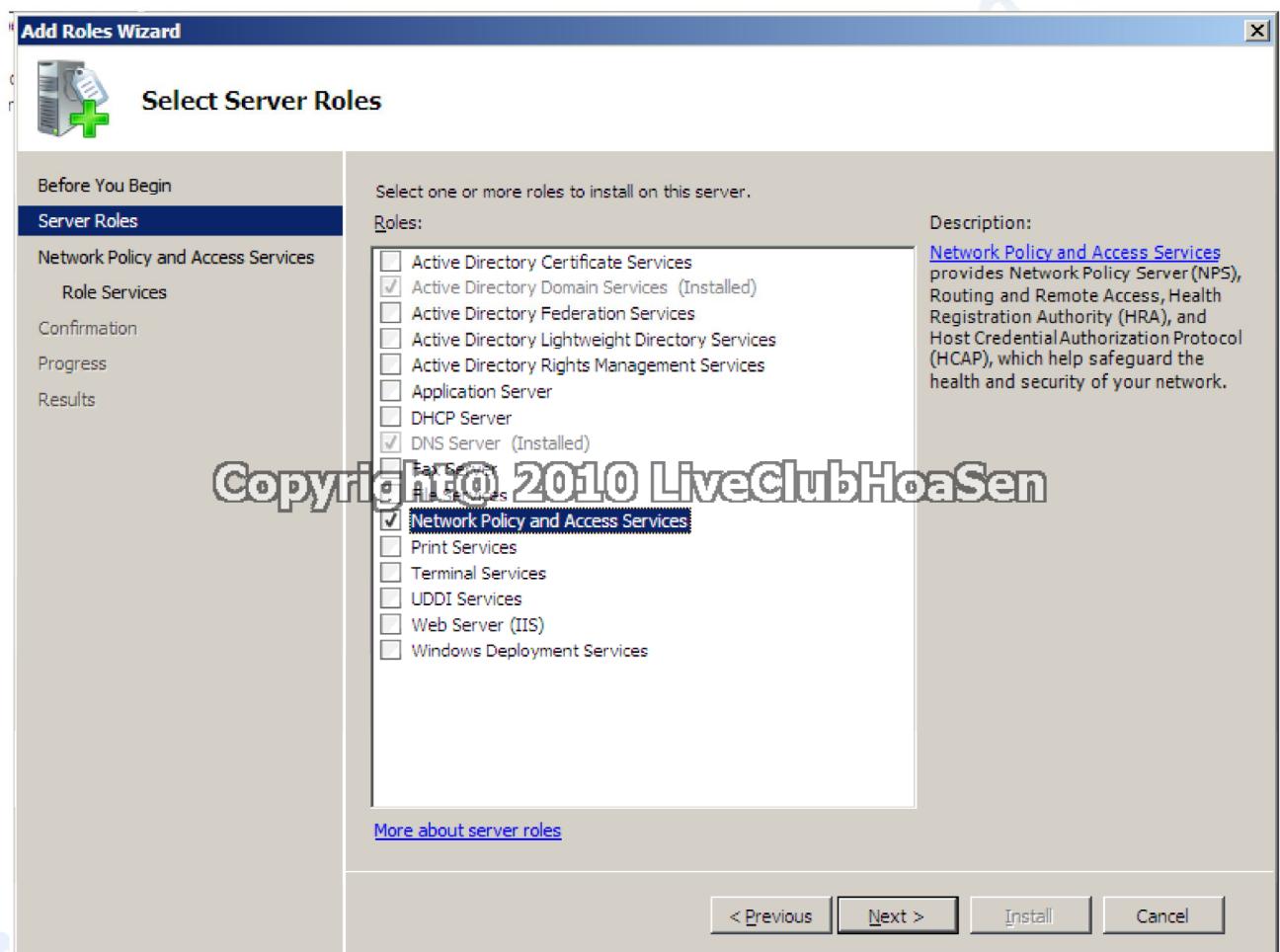
- **Dynamic Host Configuration Protocol (DHCP)**
- **Ipsec with Health Registration Authority (HRA)**
- **IEEE 802.1X (Wired và Wireless)**

- **Virtual Private Network (VPN)**
- **Terminal Services Gateway (TS Gateway)**

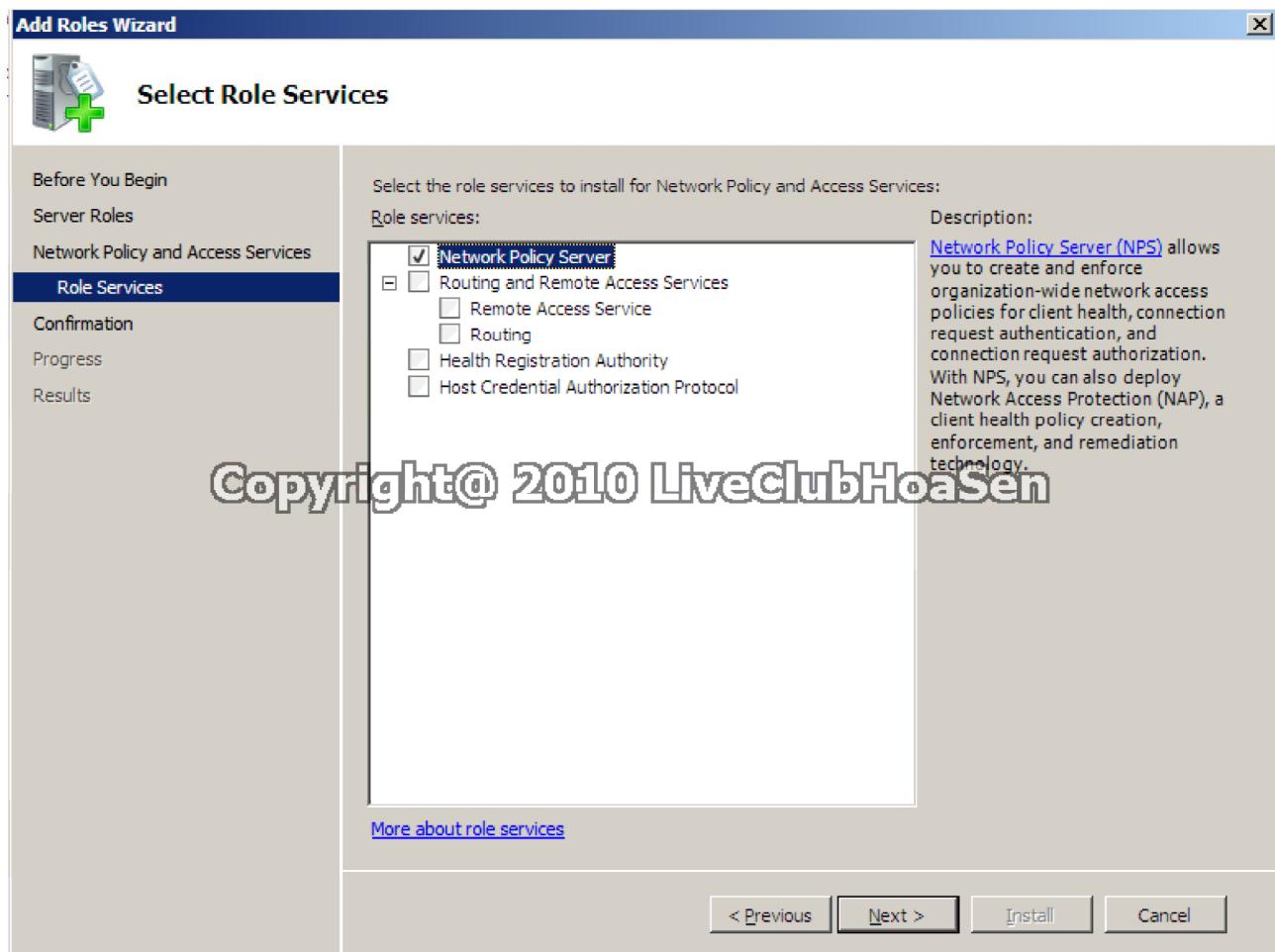
II. CÀI ĐẶT NẠP

Vào Server Manager → Roles → Add Roles.

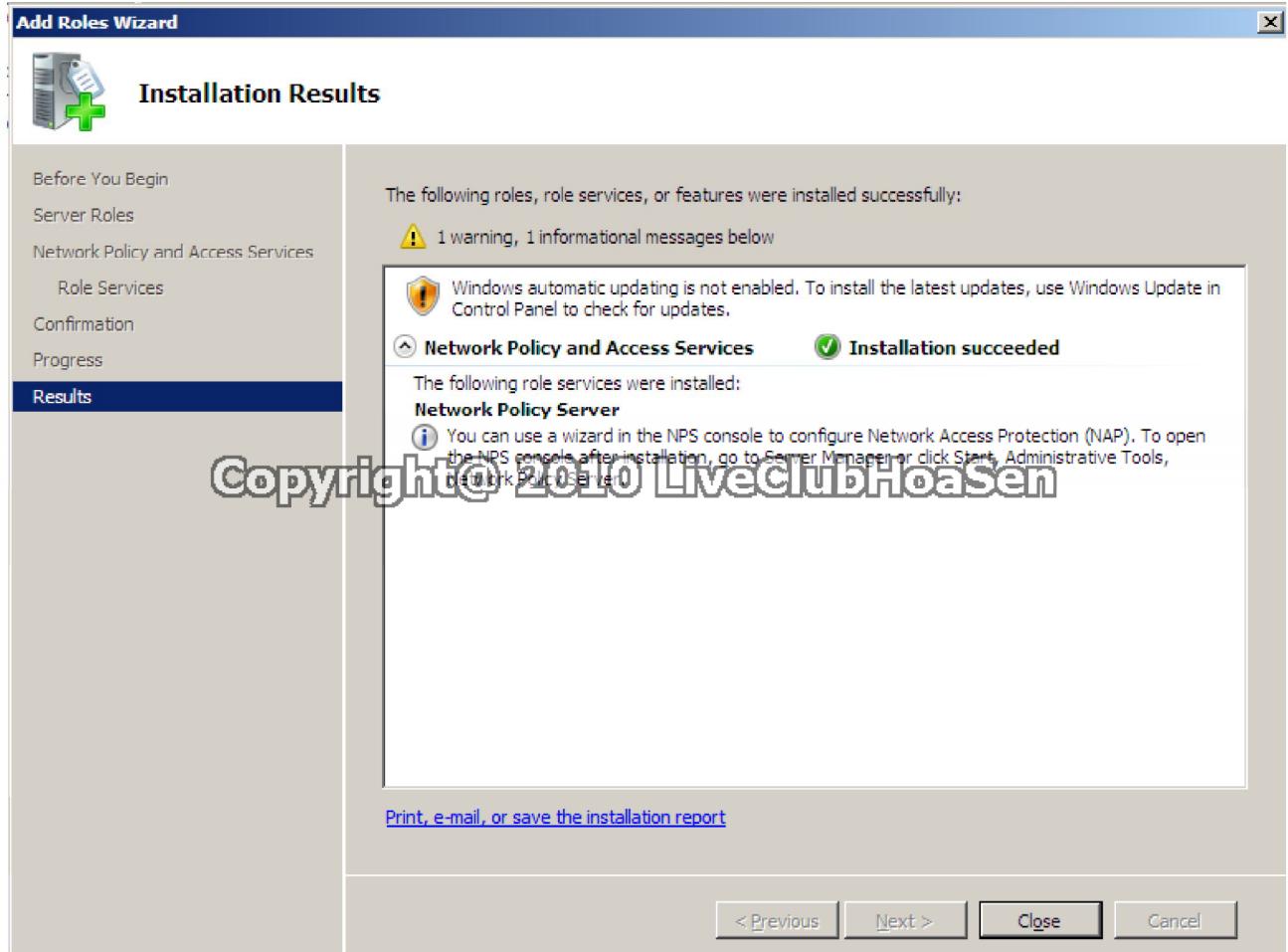
Tại bảng Select Server Roles .Chọn Network Policy and Access Services



Chọn Next. Tại bảng Select Role Services Chọn Network Policy Server



Chọn Next.



Chọn Close để hoàn tất quá trình cài đặt

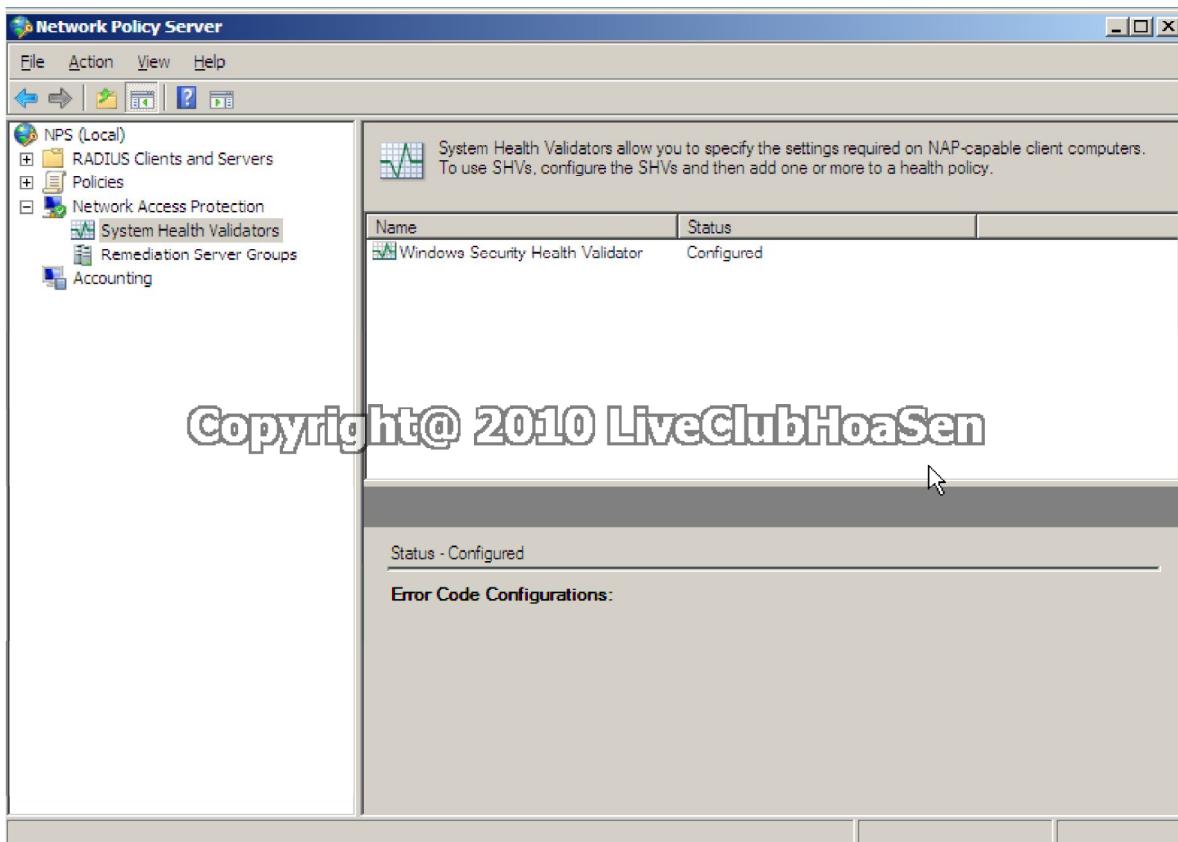
III. CẤU HÌNH NAP

1. Cấu hình Network Policy Server

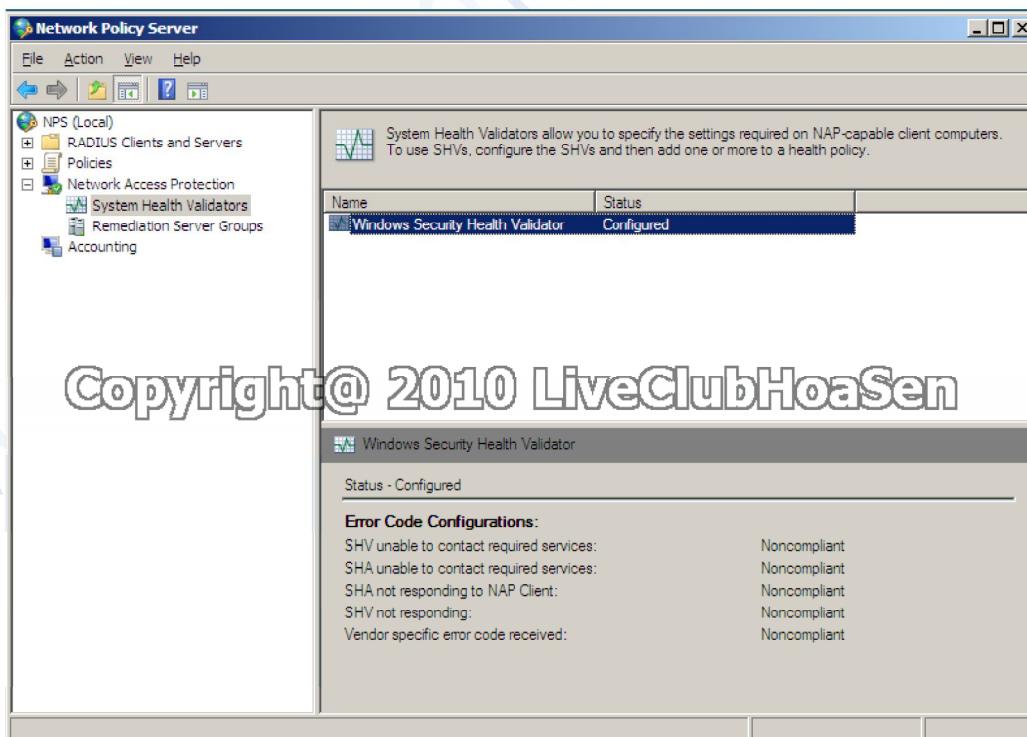
Chọn tùy chọn Network Policy Server từ danh sách Administrative Tools.

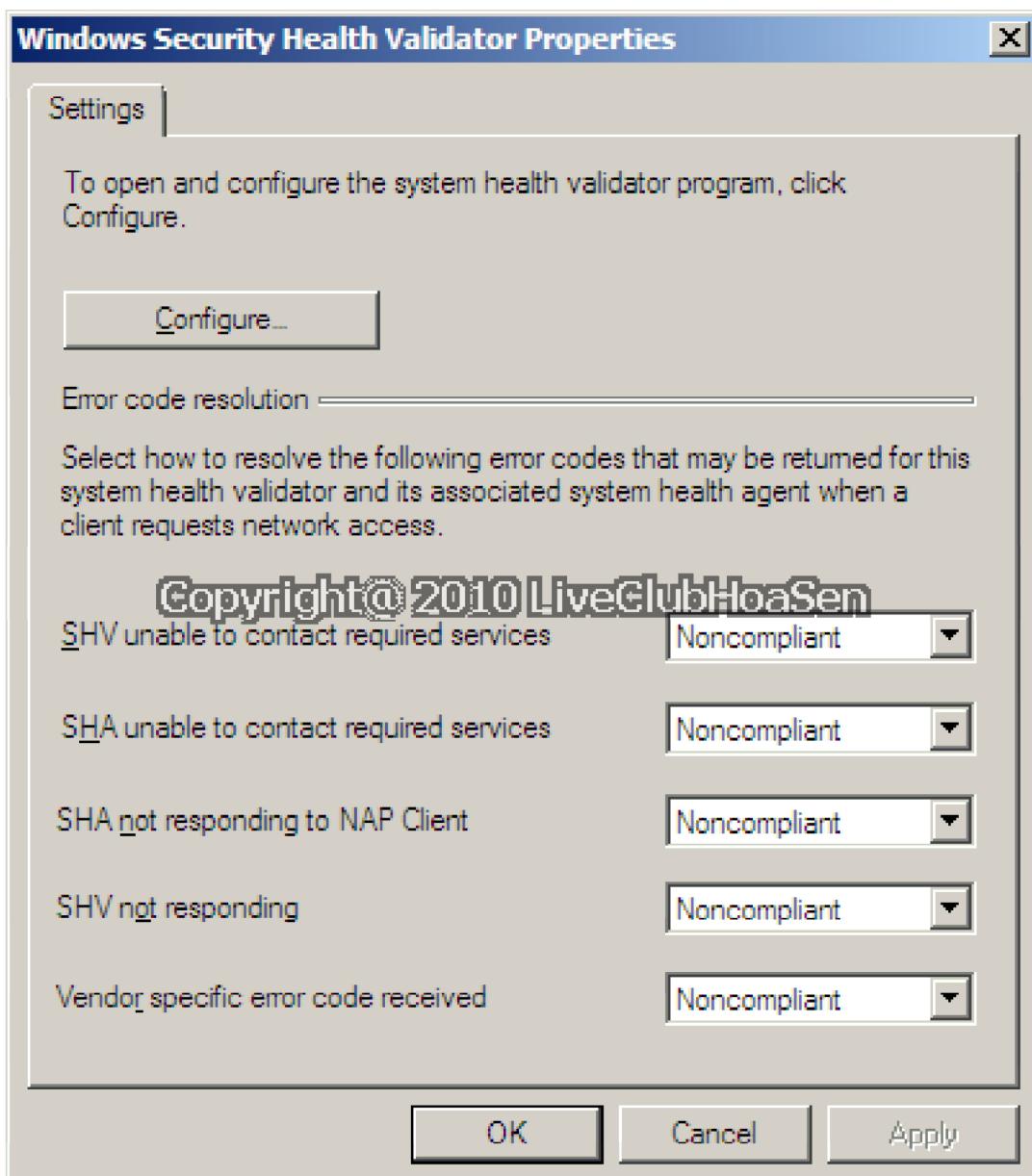
Chọn NPS (Local) -> Network Access Protection -> System Health Validators, là nơi bạn có thể cấu hình các SHV và các nhóm server sửa chữa, vốn là các nhóm cho bạn xác định server sửa chữa sẽ lưu trữ và cung cấp các bạn cập nhật phần mềm cho những client NAP cần chúng.

Kích chuột phải vào đối tượng Windows System Health Validator trong panel trung tâm của giao diện điều khiển và chọn lệnh Properties. Khi đó Windows sẽ hiển thị cho bạn hộp thoại Windows Security Health Validator Properties



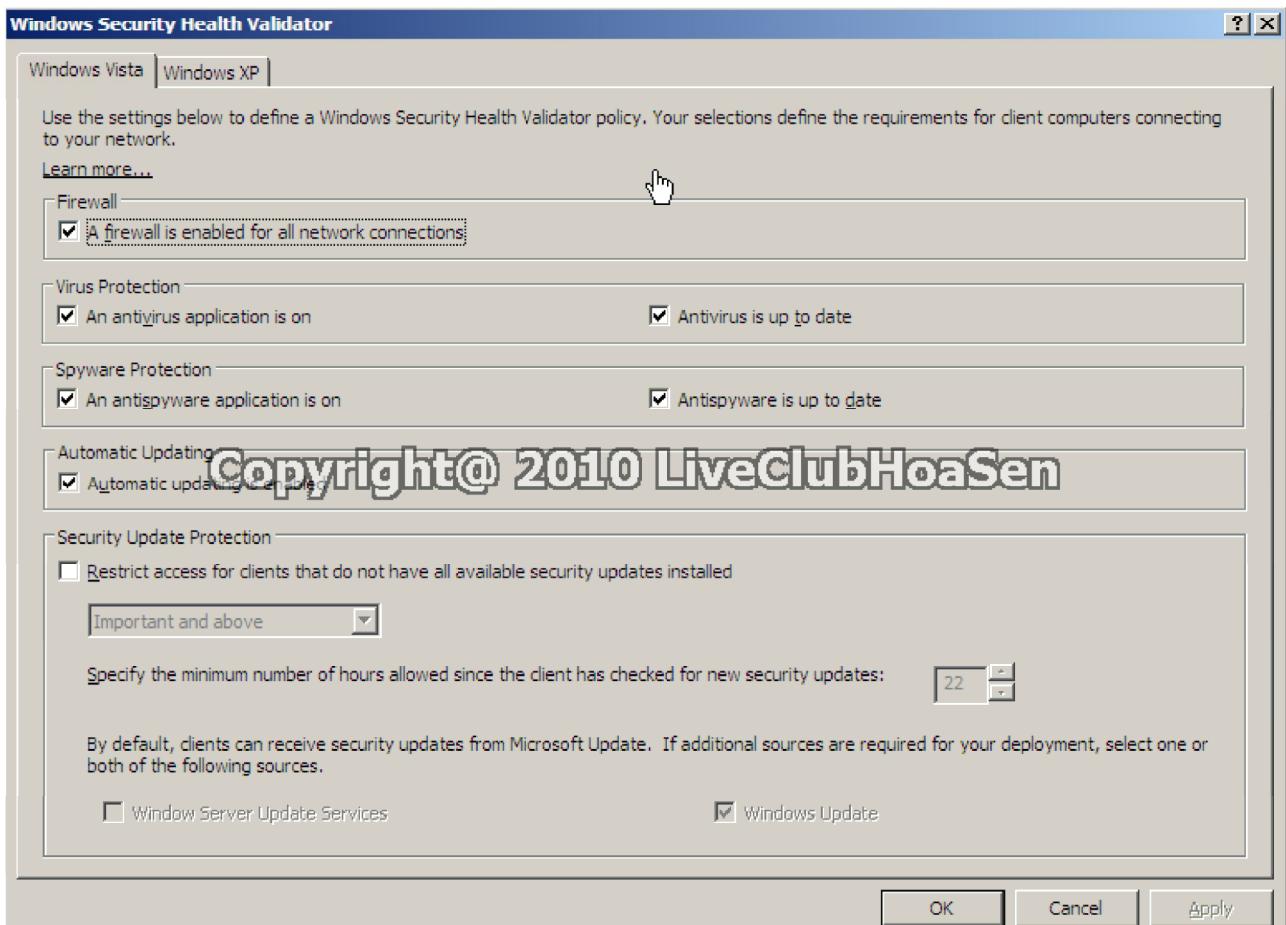
Điều hướng trong cây giao diện đến NPS (Local) | Network Access Protection | System Health Validators





Hộp thoại Windows Security Health Validator Properties được sử dụng để cấu hình bộ chỉ thị tình trạng sức khỏe của hệ thống.

Kích **Configure** của hộp thoại, khi đó Windows sẽ hiển thị hộp thoại Windows Security Health Validator. Như những gì bạn có thể thấy trong hình, hộp thoại này sẽ cho phép bạn định nghĩa chính sách của bộ chỉ thị tình trạng sức khỏe hệ thống. Mặc định hộp thoại này sẽ được cấu hình yêu cầu tường lửa của Windows, Windows update và các bộ bảo vệ chống virus và chống spyware cũng phải được kích hoạt và cập nhật thường xuyên.



Chọn hộp chọn 'A Firewall is Enabled for all Network Connections' và hủy chọn tất cả các hộp chọn còn lại.

Windows SHV thực hiện những loại kiểm tra sức khoẻ sau đây trên các client NAP:

Kiểm tra xem Windows Firewall (hoặc bất kỳ firewall dựa vào host phục vụ NAP khác) có được mở hay không

Kiểm tra xem phần mềm AV có chạy hay không (và file sig của nó có cập nhật hay không)

Kiểm tra xem Windows Defender hoặc một chương trình chống spyware nào đó đang chạy (và cập nhật) hay không

Kiểm tra xem Automatic Updates có được mở trên máy hay không

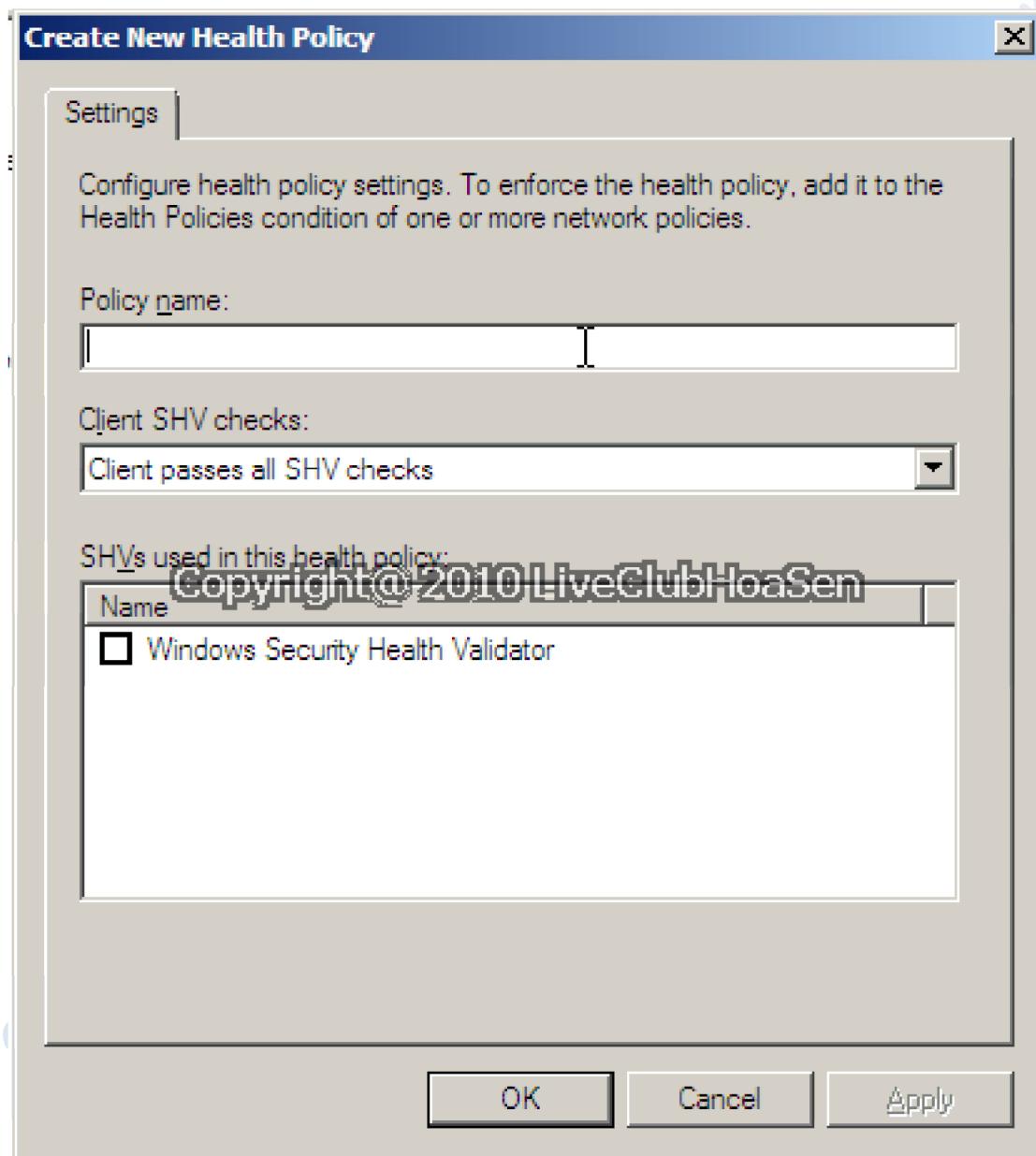
Kiểm tra xem tất cả bản cập nhật an ninh có sẵn trên một cấp độ quan trọng đã xác định có được cài đặt hay không, thời gian tối thiểu kể từ khi client kiểm tra tìm các bản cập nhật an ninh và nơi client có được các bản cập nhật của nó.

a. Tạo một chính sách sức khỏe cho hệ thống

Chúng ta đã cấu hình bộ chỉ thị sức khỏe hệ thống (System Health Validators), lúc này bạn phải cấu hình chính sách sức khỏe cho hệ thống (System Health Policy). Chính sách sức khỏe cho hệ thống sẽ

định nghĩa các kết quả của việc hợp lệ hóa trạng thái sức khỏe hệ thống. Về cơ bản, điều đó có nghĩa là định nghĩa việc cho qua (pass) hay thất bại (fail) khi quá trình hợp lệ hóa trạng thái sức khỏe được thực hiện trên máy khách.

Để cấu hình chính sách sức khỏe của Network Policy Server, chọn đến NPS (Local) -> Policies -> Health Policies. Lúc này, kích chuột phải vào mục Health Policies, chọn lệnh New. Khi đó Windows sẽ hiển thị hộp thoại Create New Health Policy.



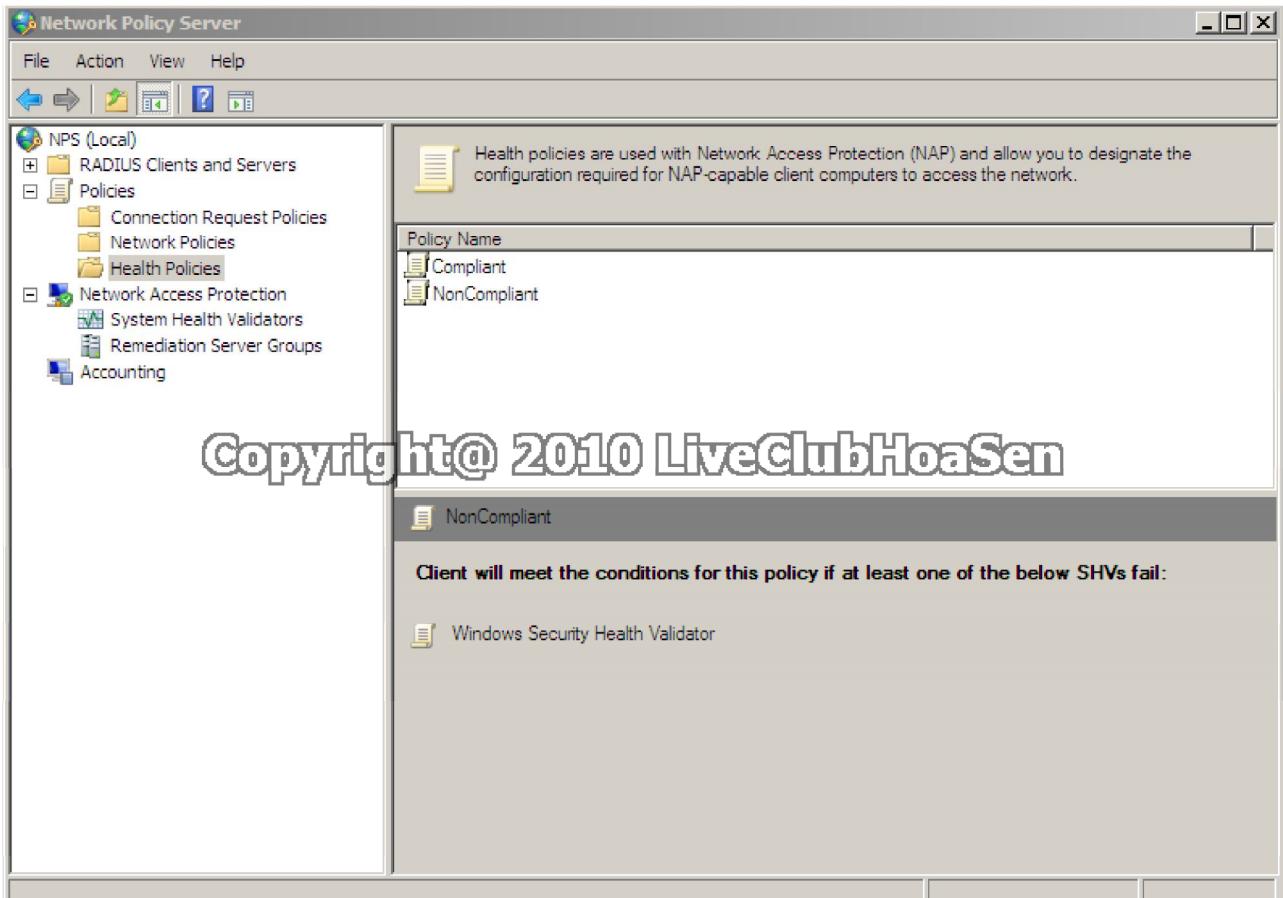
Bạn phải tạo một chính sách sức khỏe mới cho hệ thống.

Nhập từ Compliant vào trường Name. Lúc này, hãy bảo đảm rằng danh sách Client SHV Checks được thiết lập ở Client Passes all SHV Checks. Chọn hộp kiểm Windows System Health Validator và kích OK.

Tiếp đến chúng ta phải tạo một chính sách thứ hai để định nghĩa ý nghĩa của nó cho hệ thống. Chuột phải

vào mục Health Policies -> New.

Đặt tên cho chính sách mới là NonCompliant. Thiết lập danh sách trong hộp chọn Client SHV Checks là Client Fails one hoặc More SHV Checks. Chọn hộp kiểm Windows Security Health Validator -> OK.



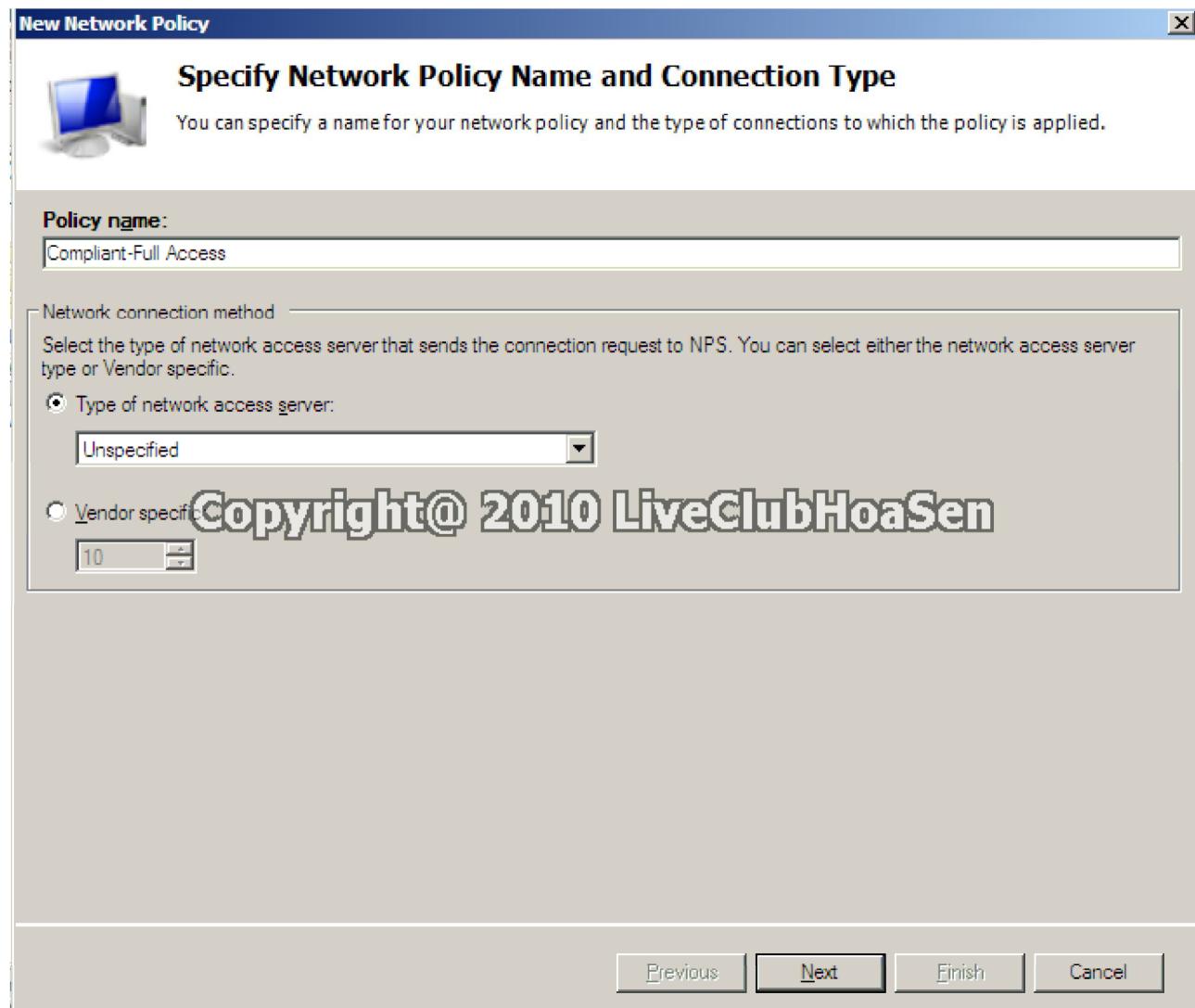
Nếu trở về màn hình chính của giao diện điều khiển Network Policy Server, hãy chọn mục Health Policies, khi đó bạn sẽ thấy cả hai chính sách Compliant và NonCompliant được hiển thị trong panel trung tâm của giao diện điều khiển

b. Tạo các chính sách mạng

Vào Network Policy Server -> Network Policies. **Disable** hai chính sách là *Connections to Microsoft Routing and Remote Access Server policy* và *Connections to Other Access Servers policy..*

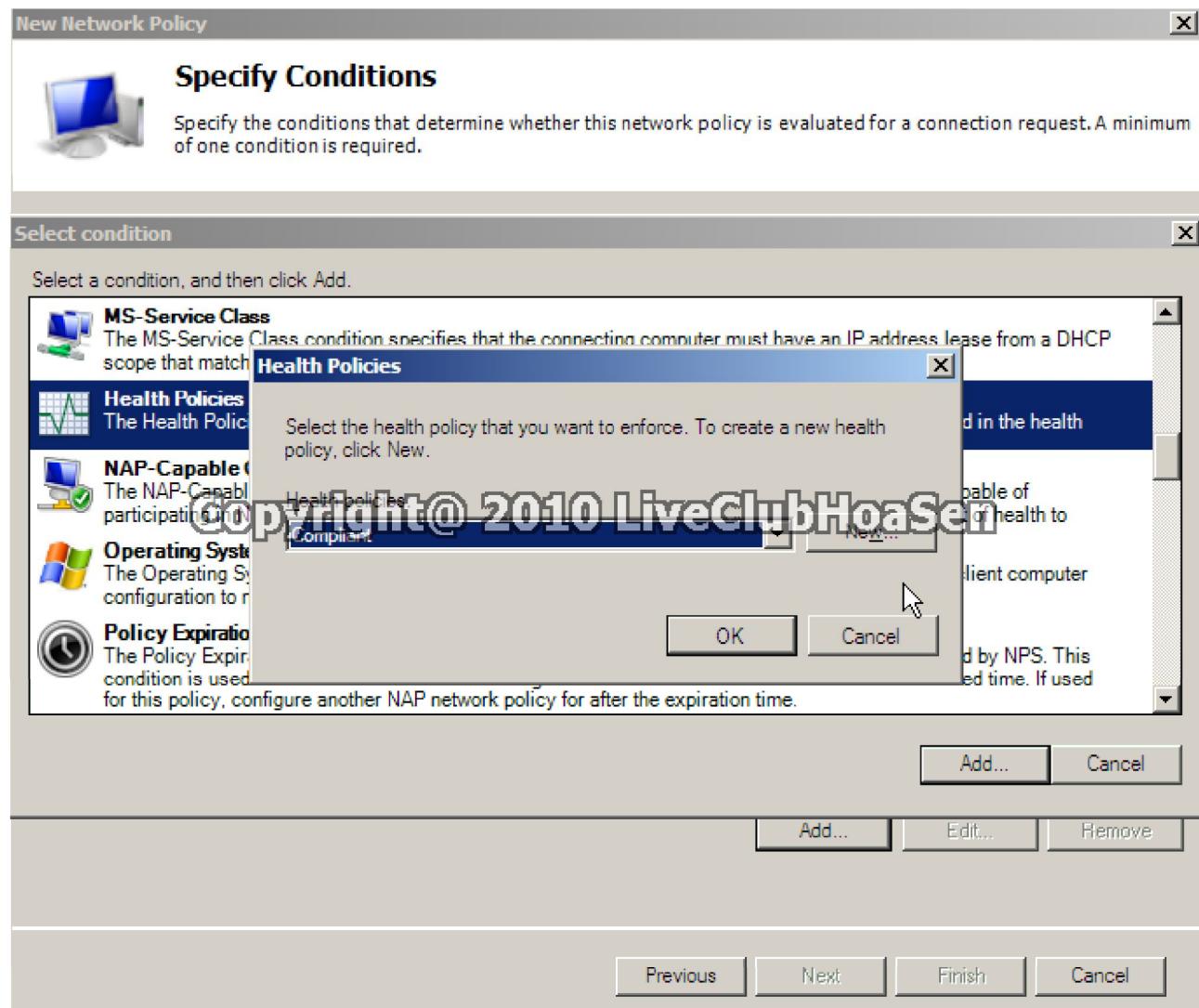
Chuột phải vào mục **Network Policy** ->**New**. Khi đó Windows sẽ khởi chạy *New Network Policy Wizard*.

Trong cửa sổ đầu tiên đặt tên cho chính sách mới là *Compliant-Full-Access..* Chọn **Unspecified** trong hộp chọn *Type of Network Access Server*



Gán tên cho chính sách mới và kích Next

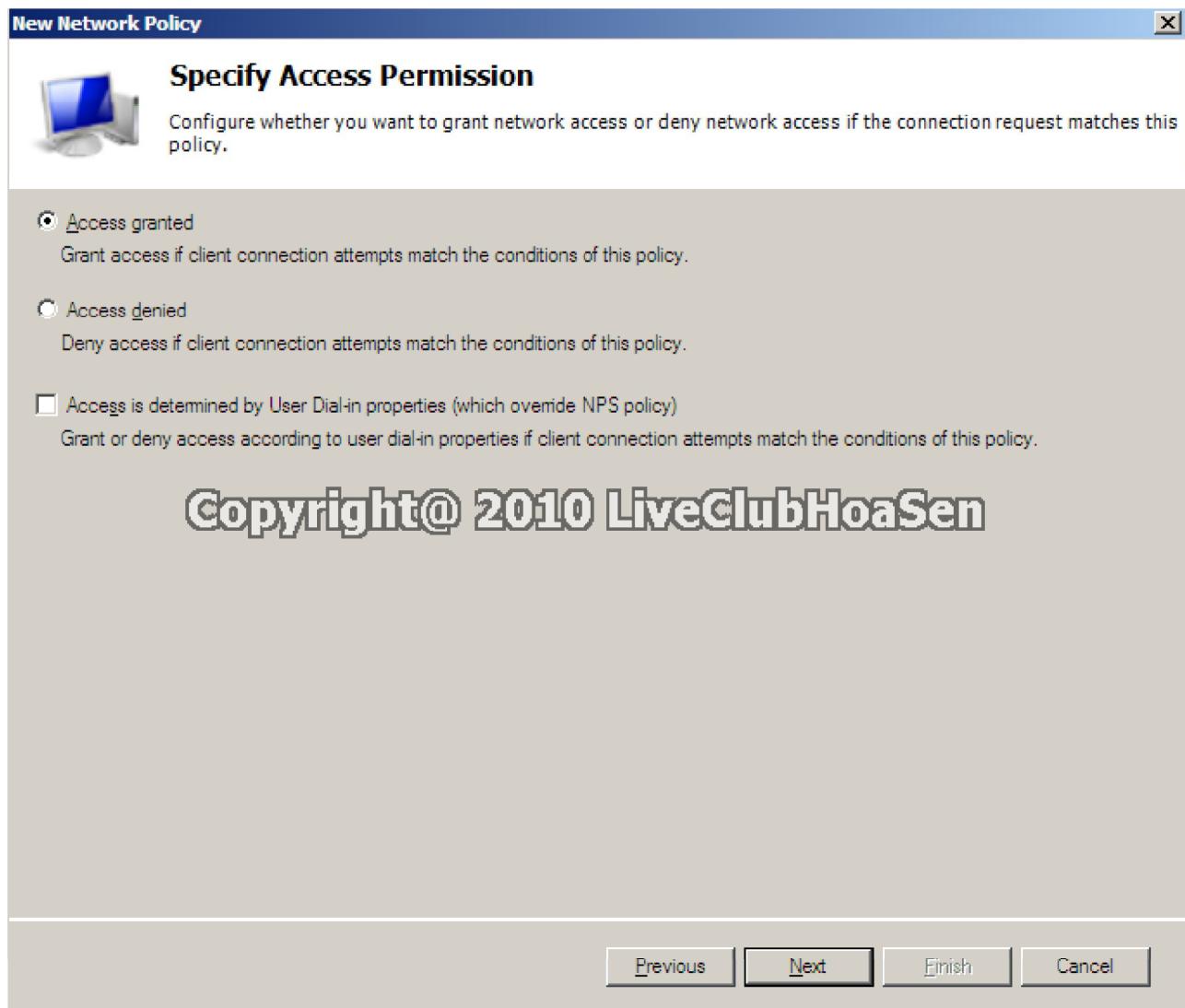
Ké tiếp chọn **Add** để mở hộp thoại *Specify Conditions*. Tìm đến tùy chọn **Health Policies** trong hộp thoại và chọn tùy chọn này, sau đó kích nút **Add**. Chọn tùy chọn **Compliant** từ danh sách .



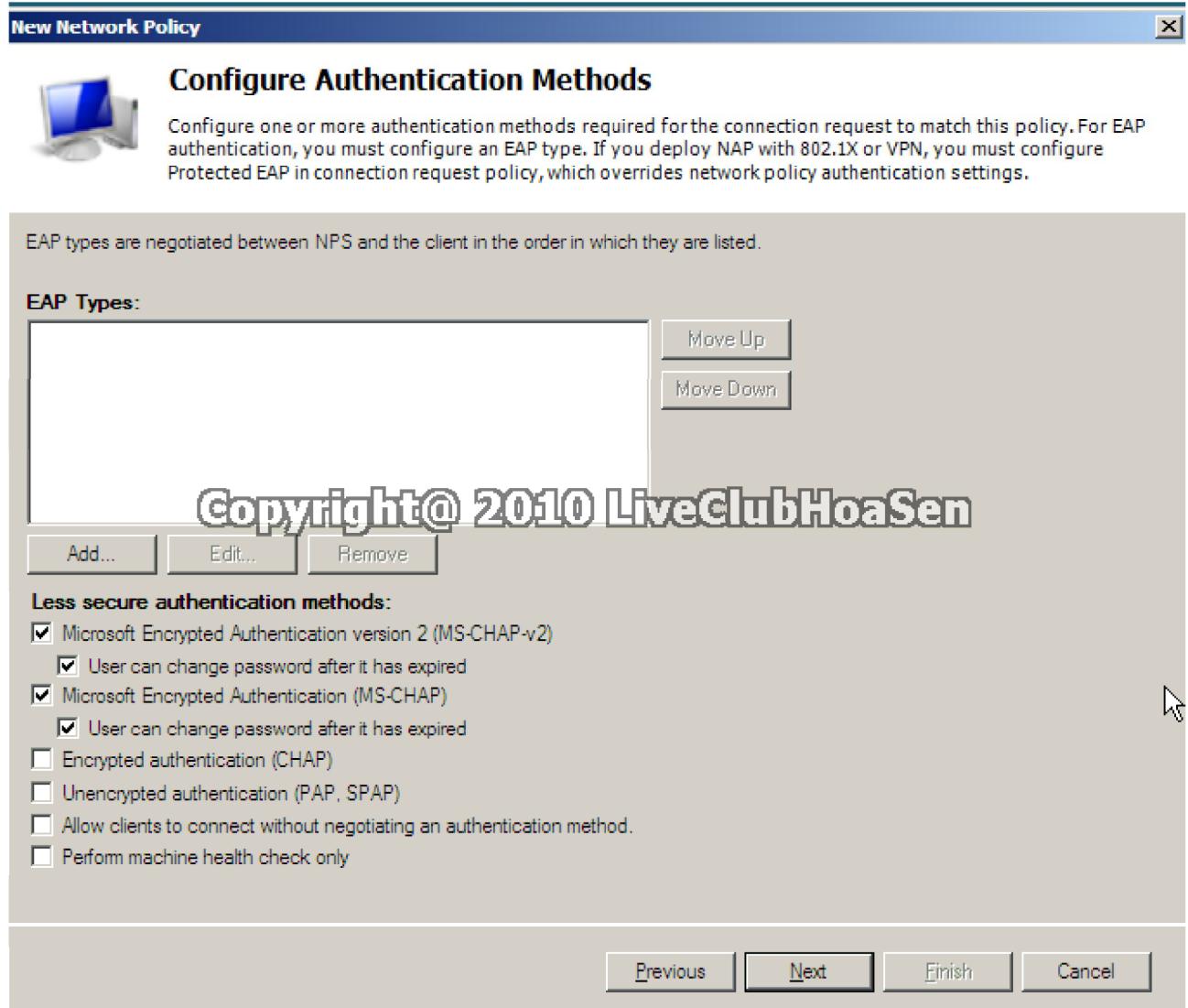
Chọn tùy chọn Compliant từ danh sách các chính sách sức khỏe

Kích OK để đóng hộp thoại Select Conditions ->Next.

Cửa sổ Specify Access Permission. Chọn tùy chọn Grant Access ->Next.



Cửa sổ *Configure Authentication Methods* để mặc định chọn **Next**.



Sử dụng các phương pháp thẩm định mặc định và kích Next.

Cửa sổ *Configure Constraints*. Chọn Next.

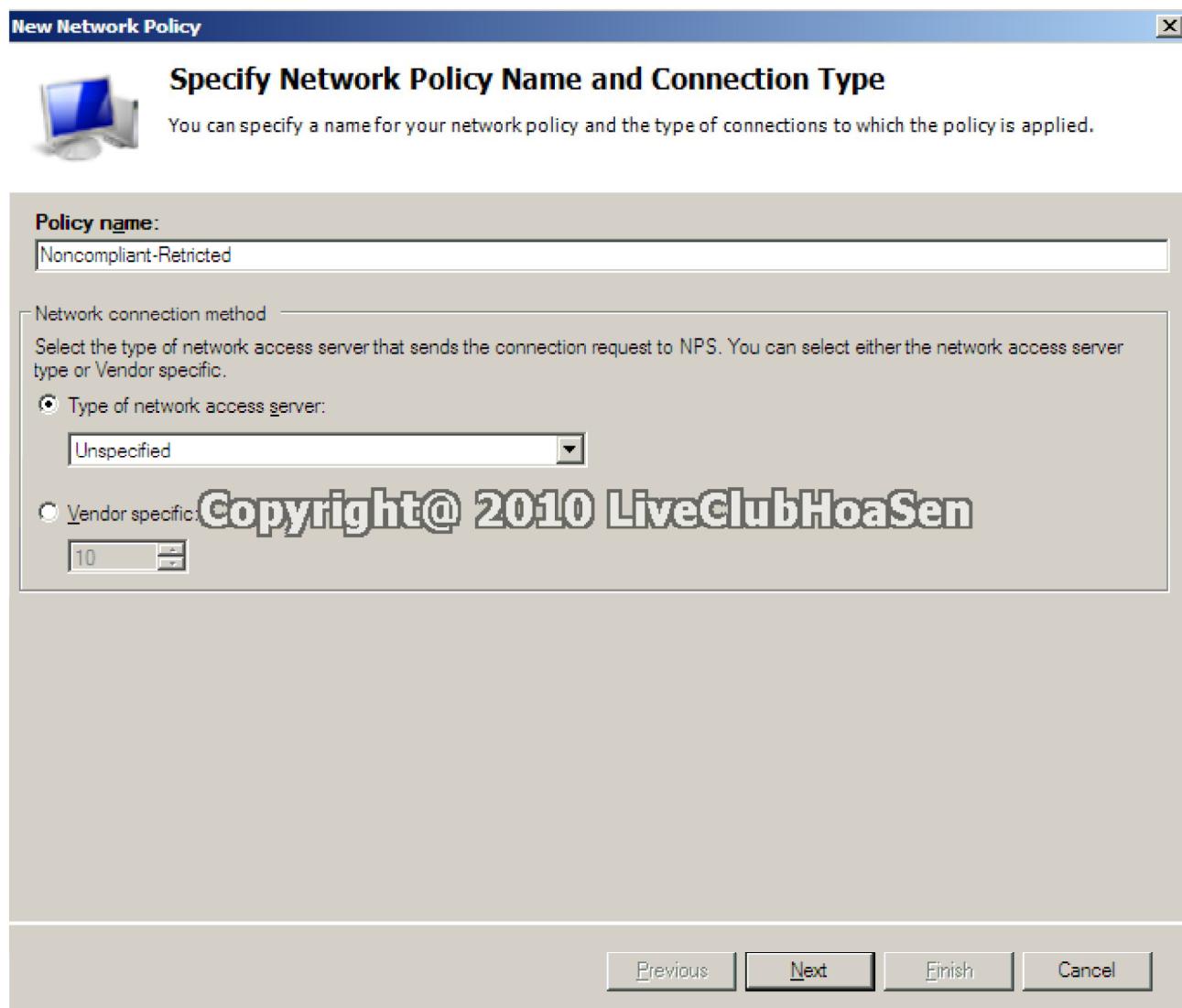
Khi đó bạn sẽ bắt gặp cửa sổ *Configure Settings*. Cửa sổ này cho phép bạn chỉ định các thiết lập cần phải sử dụng nếu máy tính được cho phép truy cập. Chọn Next.

Nhấn Finish để kết thúc quá trình cấu hình.

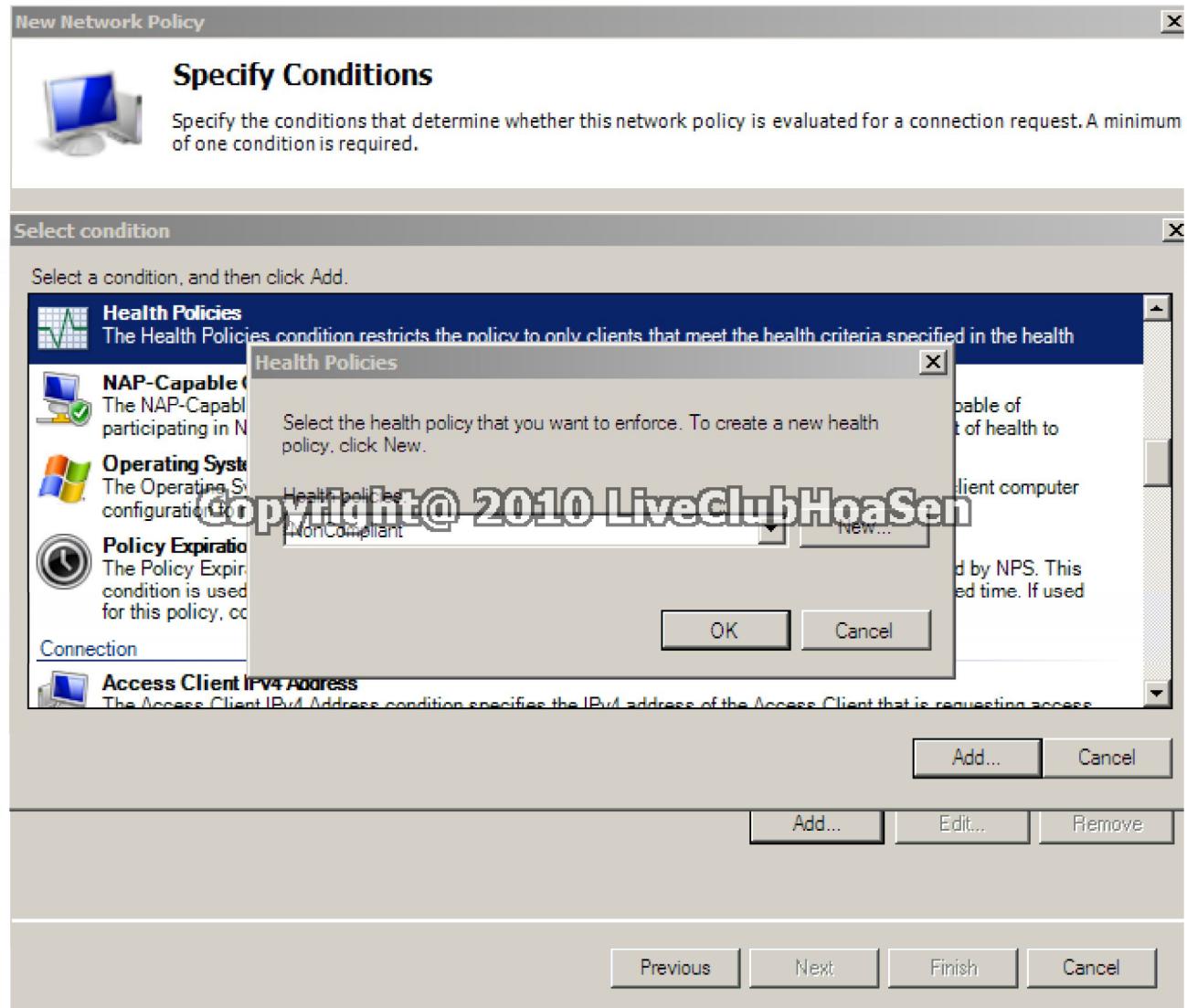
c. Các máy tính không đồng thuận

Cho tới đây chúng ta đã tạo được một chính sách cho các máy tính đồng thuận, lúc này chúng ta phải tạo một chính sách tương tự như vậy cho các máy tính không đồng thuận (tức các máy tính không hội tụ đủ các yếu tố cần thiết với tiêu chuẩn đặt ra).

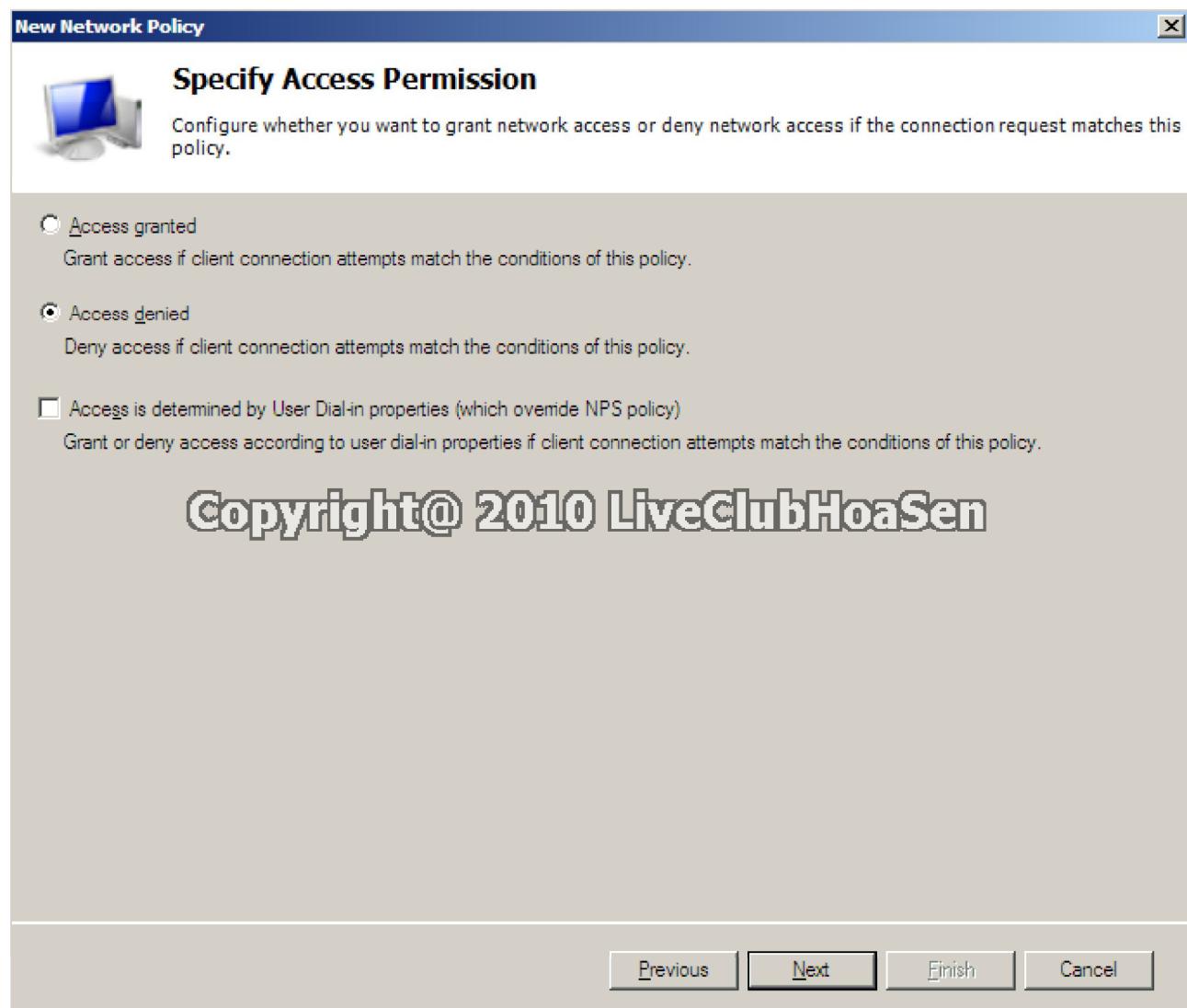
Chuột phải vào mục **Network Policies** -> **New**. Màn hình *New Network Policy wizard* xuất hiện.



Cũng như ở trên, thứ đầu tiên mà bạn phải thực hiện lúc này là nhập vào tên cho chính sách mới định tạo. Đặt tên cho chính sách là *Noncompliant-Restricted*. Thiết lập tùy chọn *Type of Network Access Server* là *Unspecified* -> Next.

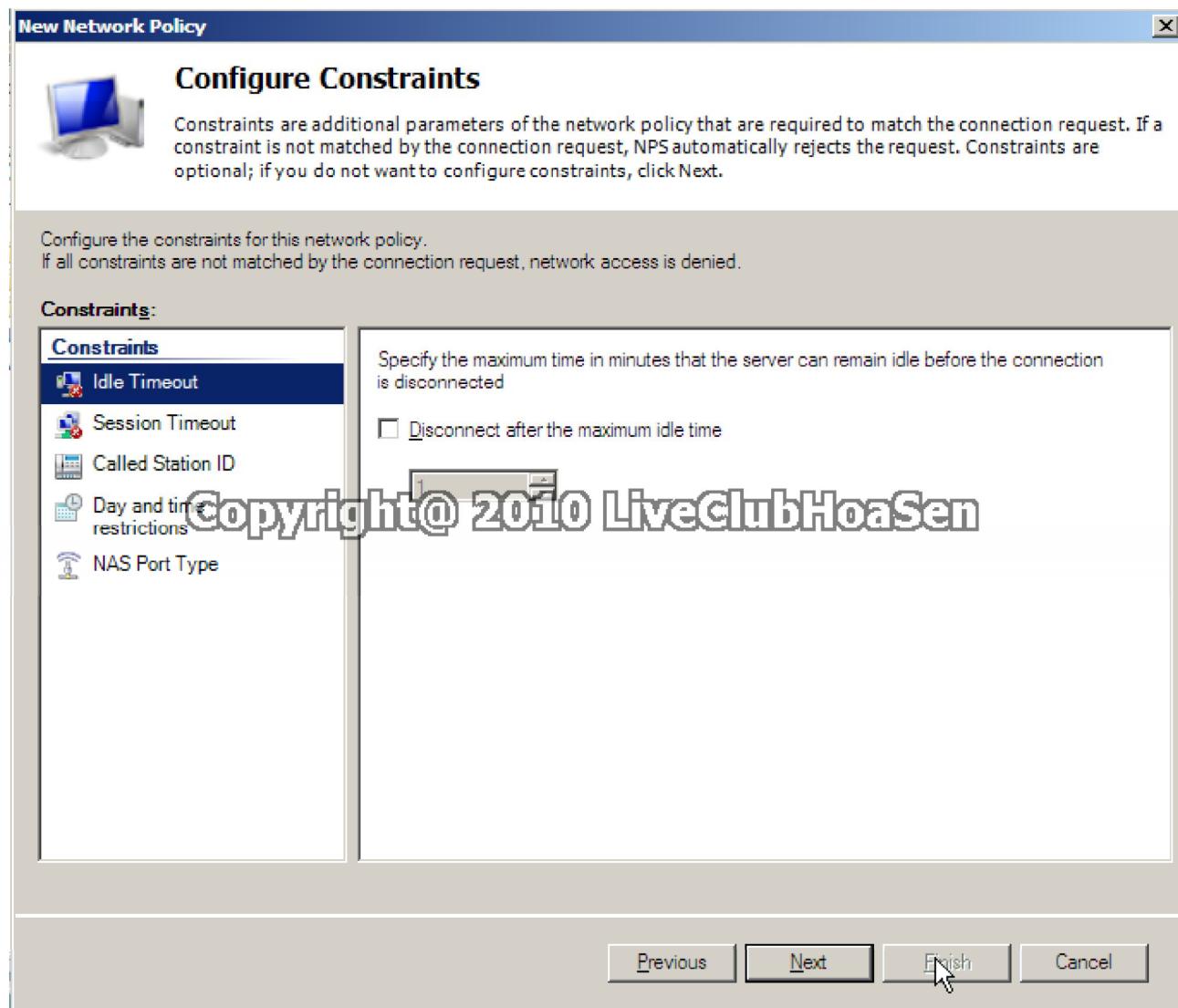


Cửa sổ **Conditions** chọn **Add**, khi đó Windows sẽ hiển thị hộp thoại **Select Conditions**. Chọn tùy chọn **Health Policies** từ danh sách và kích nút **Add**. Lúc này bạn hãy chọn tùy chọn **NonCompliant** từ danh sách các chính sách sức khỏe, kích **OK** tiếp đó là **Next**.

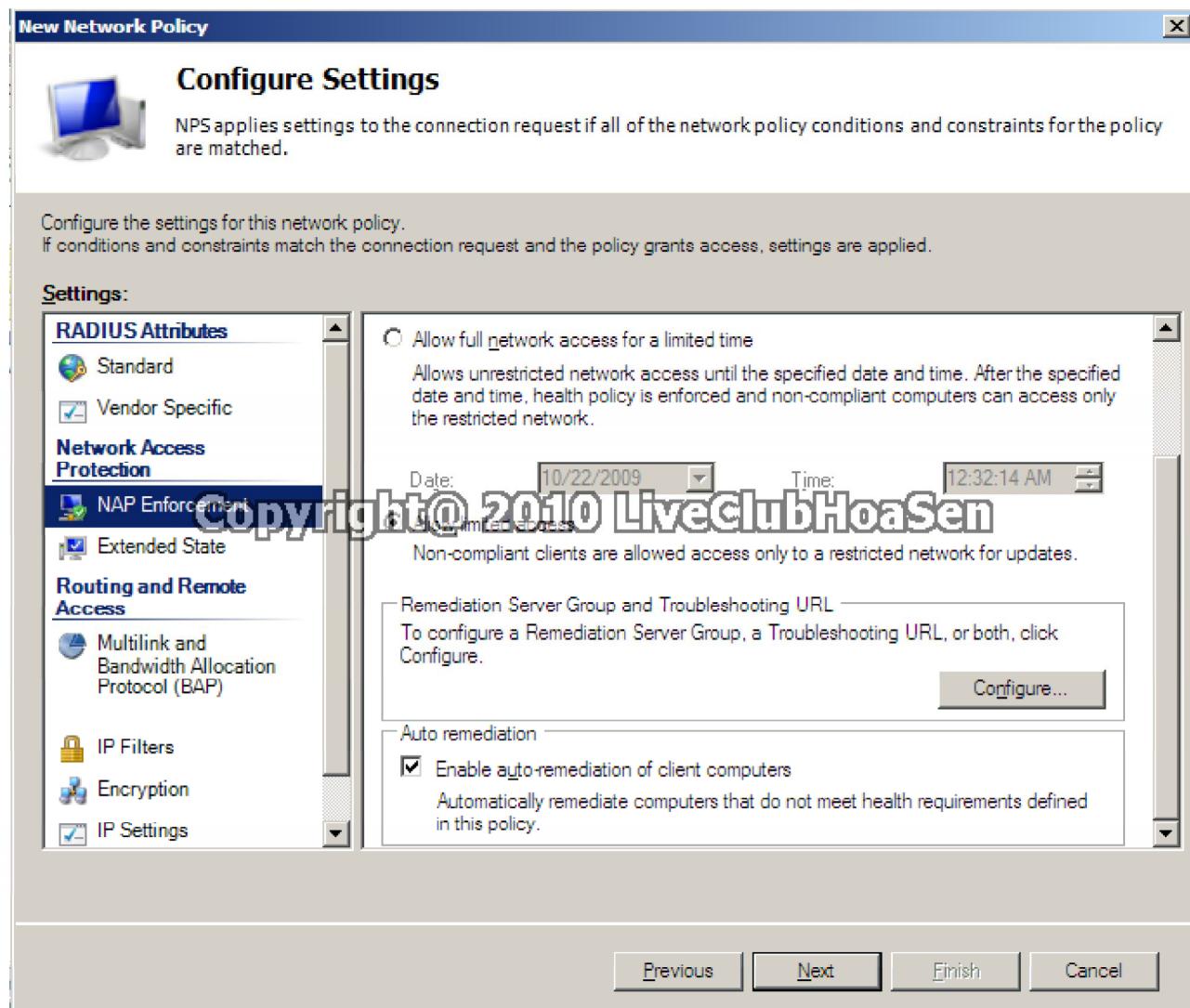


Windows lúc này sẽ hiển thị cửa sổ *Specify Access Permission*. Do chúng ta sẽ tạo một chính sách hạn chế nên bạn phải thiết lập kiểu chính sách cho Grant Access.

Kích **Next**, bạn sẽ được đưa tới cửa sổ *Configure Authentication Methods*. Lúc này chỉ cần chấp nhận các thiết lập mặc định và kích **Next**.

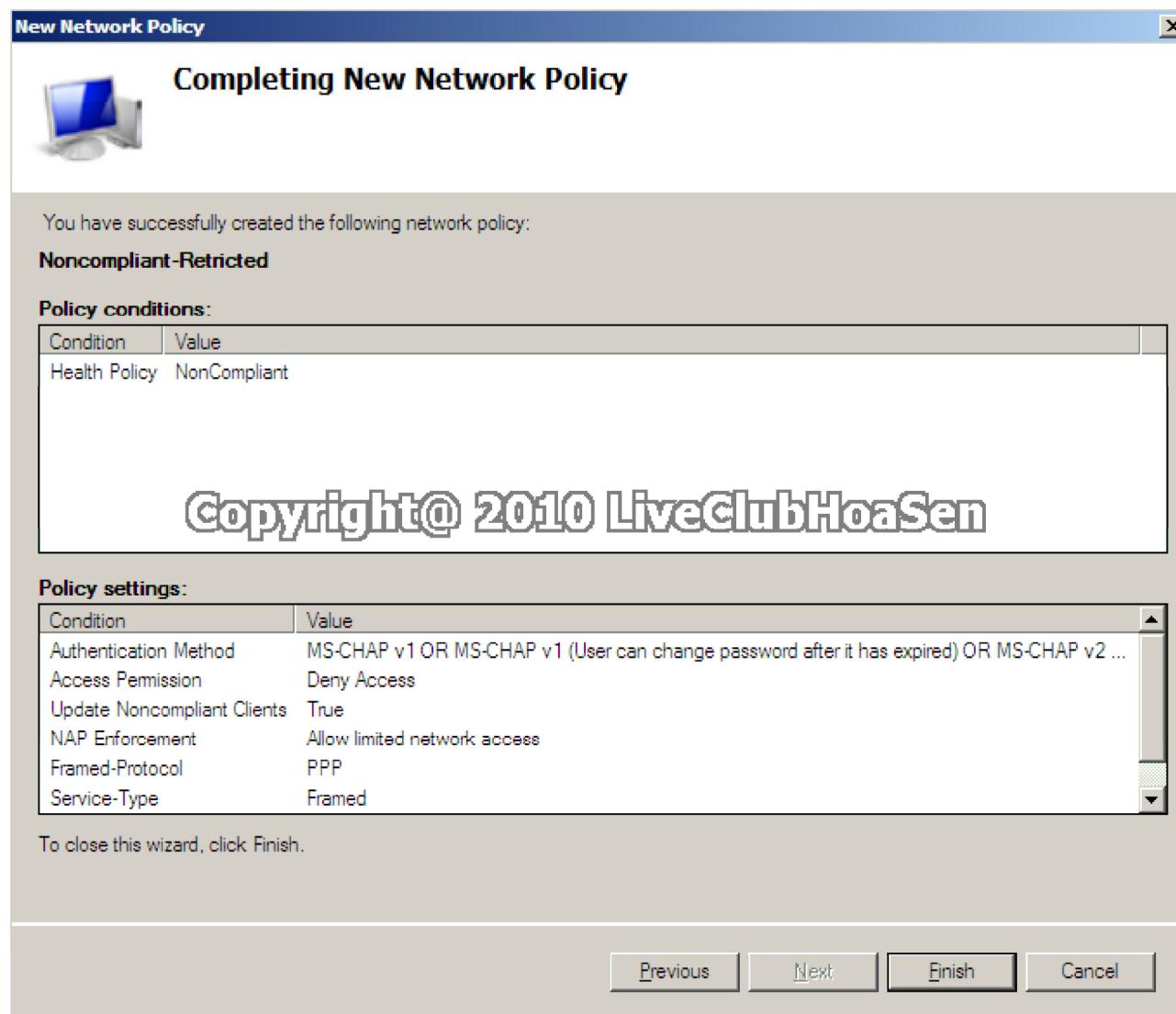


Đến đây, bạn sẽ thấy cửa sổ *Configure Constraints*. Chọn **Next**.



Cửa sổ **Configure Settings**. Cho đến đây, mọi thứ mà bạn đã thực hiện cho các máy tính không đồng thuận hoàn toàn giống hệt với những gì chúng ta đã làm với chính sách cho các máy tính đồng thuận. Nếu chúng ta để chính sách này theo cách mặc định thì các máy tính không đồng thuận sẽ không thể tăng quyền truy cập vào mạng. Nếu không muốn điều đó xảy ra chúng ta cần phải sử dụng NAP enforcement để ngăn chặn việc truy cập mạng.

Để thực hiện điều đó, bạn hãy chọn mục **NAP Enforcement** trong danh sách các thiết lập. Khi đó panel **Details** sẽ hiển thị các tùy chọn thực thi khác nhau. Chọn tùy chọn **Allow Limited Access**, tích vào hộp kiểm **Enable Auto Remediation of Client Computers**. Tùy chọn **Enforce** và sau đó chọn hộp kiểm **Update Non Compliant Computers Automatically**. Kích **Next**.



Sau đó kích **Finish** để tạo chính sách mới.

2. Cấu hình Client NAP

Windows Vista và Windows Server 2008 có một snap-in MMC được gọi là Client Configuration mà bạn có thể sử dụng để cấu hình thủ công các xác lập NAP phía client. Hoặc bạn có thể sử dụng Group Policy để cấu hình các client NAP. Trong Windows Server 2008 và Windows Vista, các xác lập Group Policy cho NAP được tìm thấy bên dưới vị trí policy:

Computer Configuration\Windows Settings\Security Settings\Network Access Protection