

**Trong loạt bài này chúng tôi sẽ giới thiệu cho các bạn về một số vấn đề cơ bản của Access Rules đối với việc quản trị TMG firewall mới.**

Tường lửa ISA đã có lịch sử phát triển khá lâu, các phiên bản dần được nâng cấp lên nên theo thời gian và tiến trình phát triển.

Năm 2010, phiên bản kế tiếp của tường lửa ISA không chỉ có các tính năng và chức năng mới đáng chú ý, nó còn mang một cái tên mới – tên ISA đã được thay bằng TMG - **Threat Management Gateway 2010**. Đây là một thay đổi lớn về mặt quan điểm và là một tín hiệu tốt về tính hiệu quả trong tiến trình phát triển bảo mật của Microsoft, Microsoft đã hoàn toàn thay đổi cách tạo phần mềm và tập trung vào vấn đề bảo mật trong mọi giai đoạn phát triển.

Thách thức đối với các thiết lập tường lửa TMG mới là học những vấn đề cơ bản. Chúng ta đã trải qua hàng thập kỷ làm việc với ISA và hầu hết trong mọi quản trị viên đều hiểu rất sâu về các chi tiết kỹ thuật cũng như các kịch bản triển khai phức tạp của nó. Tuy nhiên có rất nhiều người gặp phải vấn đề khi truy cập cũng như cách làm việc của tường lửa TMG. Rất nhiều quản trị viên TMG mới đã tập trung vào tìm hiểu cách điều khiển truy cập gửi vào (cho ví dụ, để điều khiển sự truy cập đến Exchange và SharePoint). Và lúc này họ muốn biết cách điều khiển truy cập các kết nối gửi ra. Đó là lý do mà chúng tôi giới thiệu cho các bạn bài viết này, bài viết sẽ tập trung vào các những vấn đề cơ bản của Access Rules.

### **Tìm hiểu về Access Rules**

[Key4VIP.info](http://www.Key4VIP.info)

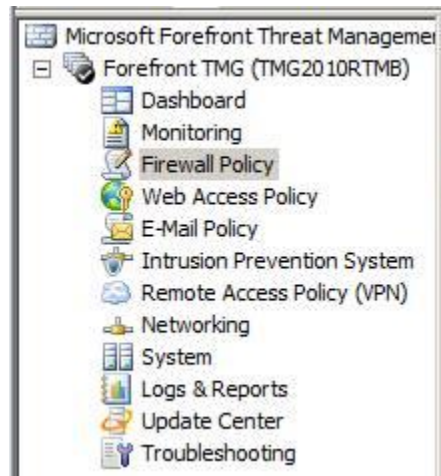
Access Rule được sử dụng để điều khiển truy cập gửi ra từ một mạng được bảo vệ bởi tường lửa TMG. Khi bạn muốn cho phép một máy tính nằm phía sau sự kiểm soát của tường lửa TMG truy cập một mạng khác (gồm có Internet), bạn cần tạo một Access Rule (luật truy cập) để cho phép kết nối đó. Mặc định, không có Access Rule nào cho phép các kết nối qua tường lửa, vì vậy mặc định tường lửa TMG là một bức tường gạch vững chắc bảo vệ cho mạng. Trạng thái đóng cửa mặc định này là một cấu hình an toàn, tuy nhiên nó cũng có nghĩa nếu bạn muốn cho phép lưu lượng qua tường lửa TMG, bạn cần phải hiểu cách Access Rule làm việc và cách tạo chúng như thế nào.

### **Tạo một Access Rule gửi ra**

Để bắt đầu, chúng ta sẽ tạo một Access Rule gửi ra đơn giản cho phép tất cả người dùng có thể truy cập Internet bằng tất cả giao thức. Trong phần tiếp theo của loạt bài này, chúng ta sẽ đi tìm hiểu các vấn đề chi tiết của Access Rules và xem các Access Rules có các vấn đề phụ thuộc gì và cách bạn có thể điều chỉnh các vấn đề phụ thuộc đó.

Chúng ta hãy bắt đầu bằng cách mở giao diện điều khiển tường lửa TMG và kích nút **Firewall Policy** trong phần panel trái của giao diện, như những gì thể hiện trong hình bên dưới.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 1

Sau khi kích nút **Firewall Policy** trong panel trái, chúng ta sẽ kích tab **Tasks** trong panel phải của giao diện. Ở đây bạn sẽ thấy một số tùy chọn, đa số trong chúng có liên quan đến việc tạo các rule tường lửa. Trong ví dụ này, chúng ta sẽ tạo một rule truy cập để cho phép truy cập gửi ra qua tường lửa. Kích liên kết **Create Access Rule** để khởi chạy Access Rule wizard, như hiển thị trong hình bên dưới.



Hình 2

Trong trang **Welcome to the New Access Rule Wizard**, đặt tên trong hộp văn bản **Access Rule name**. Nói chung, bạn nên đặt một tên có ý nghĩa cho Access Rule của mình để có thể quét chính sách tường lửa và biết rule làm gì, đặc biệt là biết mục đích được mục đích của rule. Trong ví dụ này, chúng tôi sẽ đặt tên rule là **All Open 1**. Trong môi trường sản xuất, bạn sẽ không muốn tạo một rule như vậy vì rule này sẽ cho phép tất cả các máy tính có thể truy cập Internet và chắc chắn không phải những gì bạn muốn có trong môi trường sản xuất.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

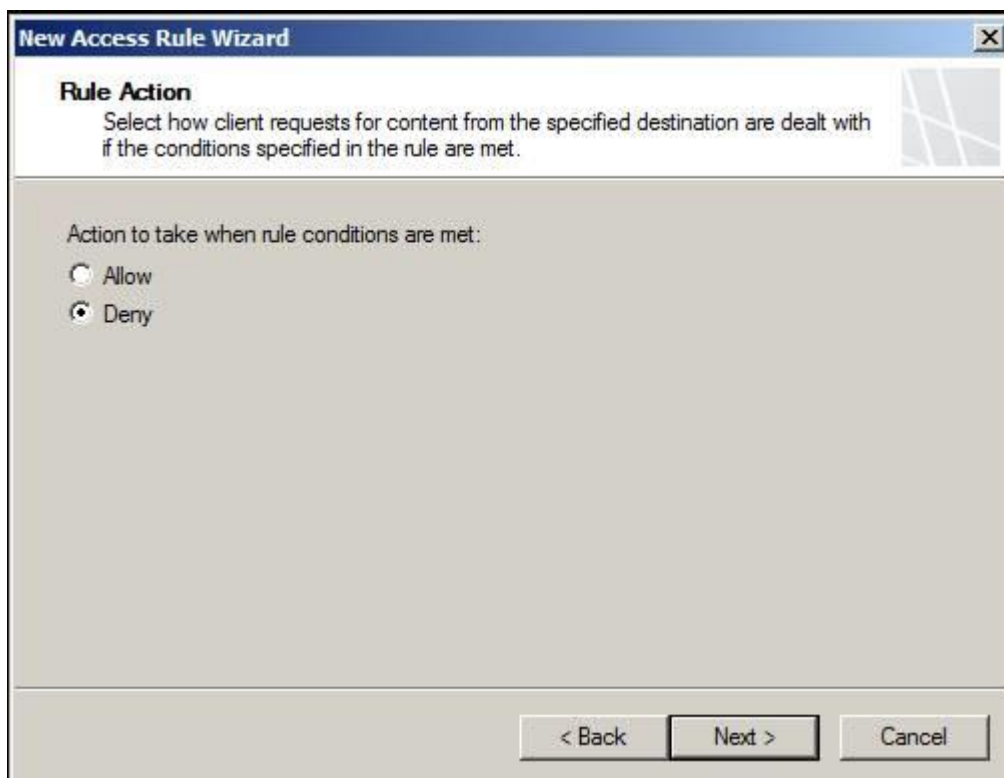


Hình 3

Key4VIP.info

Trong trang **Rule Action**, bạn sẽ có các lựa chọn **Allow** hoặc **Deny** đối với rule. Lưu ý rằng tùy chọn mặc định là Deny, đây là một tùy chọn tốt về góc độ bảo mật. Chúng ta sẽ thay đổi trạng thái **Deny** thành **Allow** trước khi kích **Next** để biến nó trở thành rule Allow.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

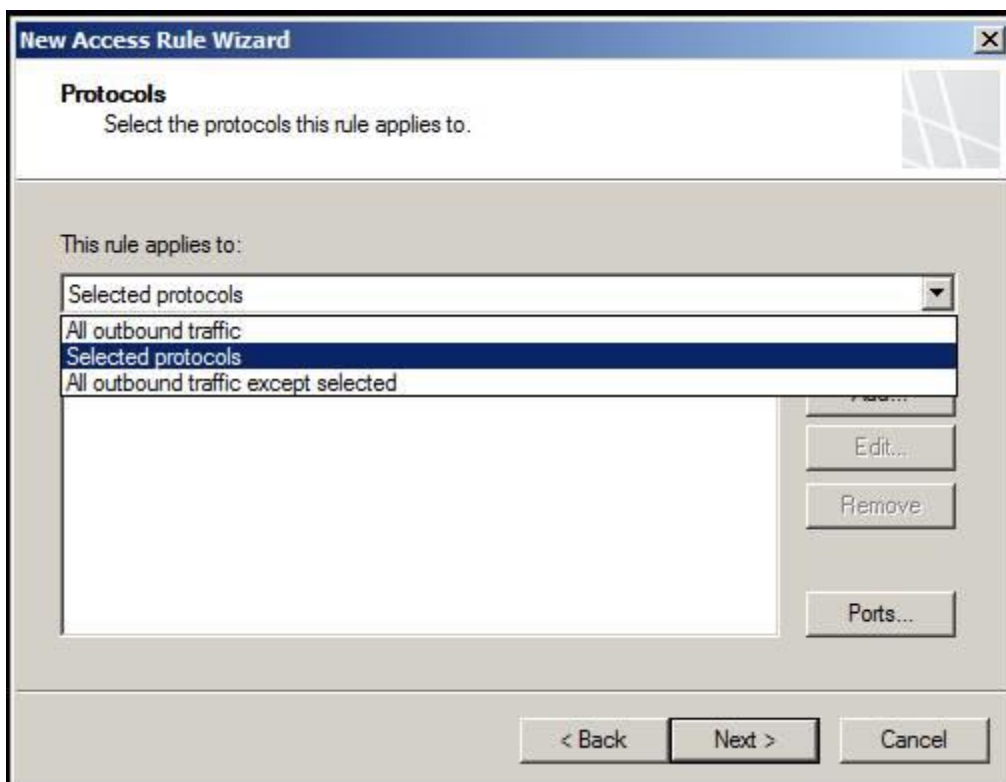


Hình 4

Key4VIP.info

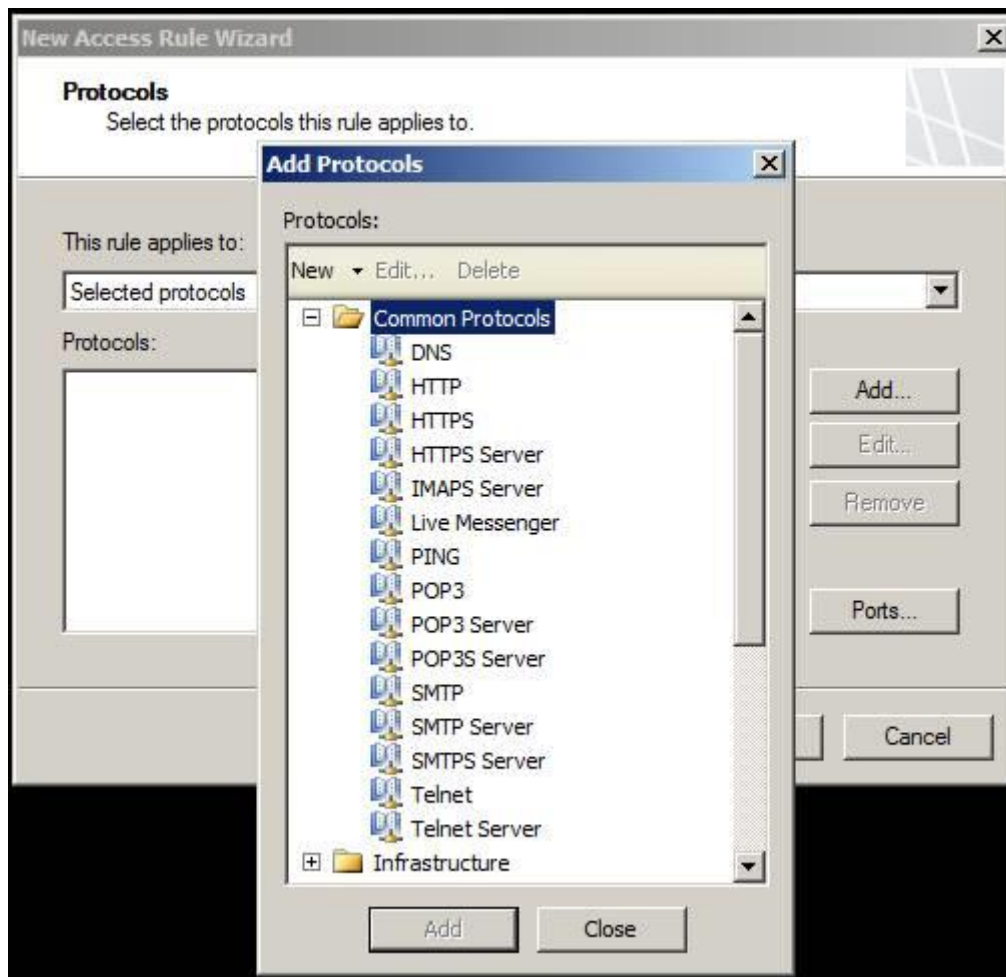
Trong trang **Protocols**, chọn các giao thức mà bạn muốn áp với rule này. Trong hộp sổ xuống **This rule applies to**, bạn có các lựa chọn sau:

- **All outbound traffic** – Sử dụng tùy chọn nếu bạn muốn áp rule này cho tất cả các giao thức.
- **Selected protocols** – Sử dụng tùy chọn này để chọn một số giao thức nào đó mà bạn muốn áp cho rule này. Đây là tùy chọn chắc chắn hầu hết trong số các bạn sẽ cần đến.
- **All outbound traffic except selected** – Tùy chọn này cho phép bạn cho phép hoặc từ chối tất cả các giao thức ngoại trừ một số giao thức nào đó mà bạn chọn ra.



## Key4VIP.info

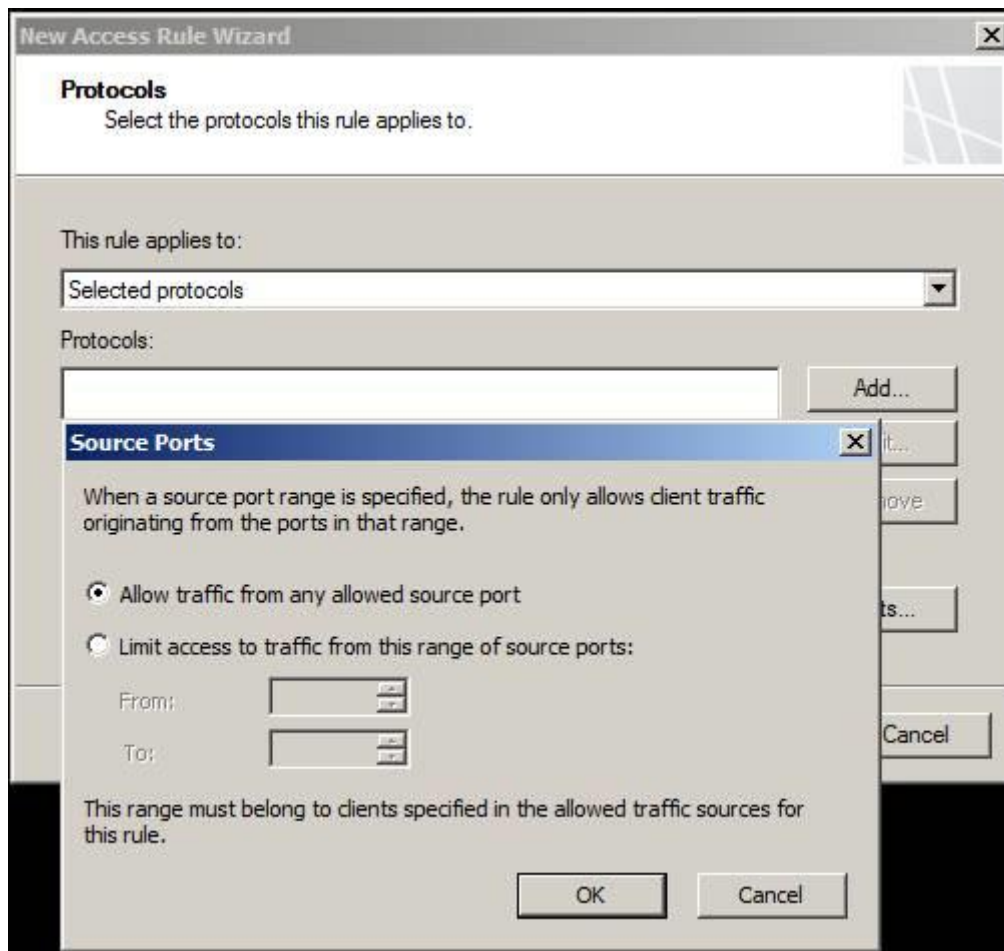
Nếu chọn tùy chọn thứ hai hoặc thứ ba, bạn có thể kích nút **Add** để chọn các giao thức mà bạn muốn áp rule này cho chúng. Sau khi kích nút **Add**, bạn sẽ thấy hộp thoại **Add Protocols** xuất hiện. Khi kích vào một thư mục nào đó nằm trong hộp thoại này, thư mục sẽ được mở và hiển thị cho bạn một danh sách các giao thức. Nhóm phát triển tường lửa TMG đã tạo sự dễ dàng trong sử dụng bằng cách tách biệt các giao thức theo các nhóm để bạn dễ dàng hơn trong việc tìm các giao thức mà mình quan tâm. Kích đúp vào các giao thức mà bạn muốn cho phép, chúng sẽ xuất hiện trên trang **Protocols** trong danh sách **Protocols**.



Hình 6

Một tùy chọn khác bạn có trong trang này sẽ được lộ diện khi bạn kích nút **Source Ports**. Thao tác của bạn sẽ làm xuất hiện hộp thoại **Source Ports**. Ở đây bạn có thể điều khiển các cổng nguồn được phép cho các kết nối tương xứng với rule này. Mặc định **Allow traffic from any allowed source port** được chọn, tuy nhiên nếu bạn muốn khóa các cổng nguồn, bạn có thể chọn **Limit access to traffic from this range of source ports** và sau đó nhập các giá trị vào trong các trường **From** và **To** để chỉ rõ các cổng nguồn này.

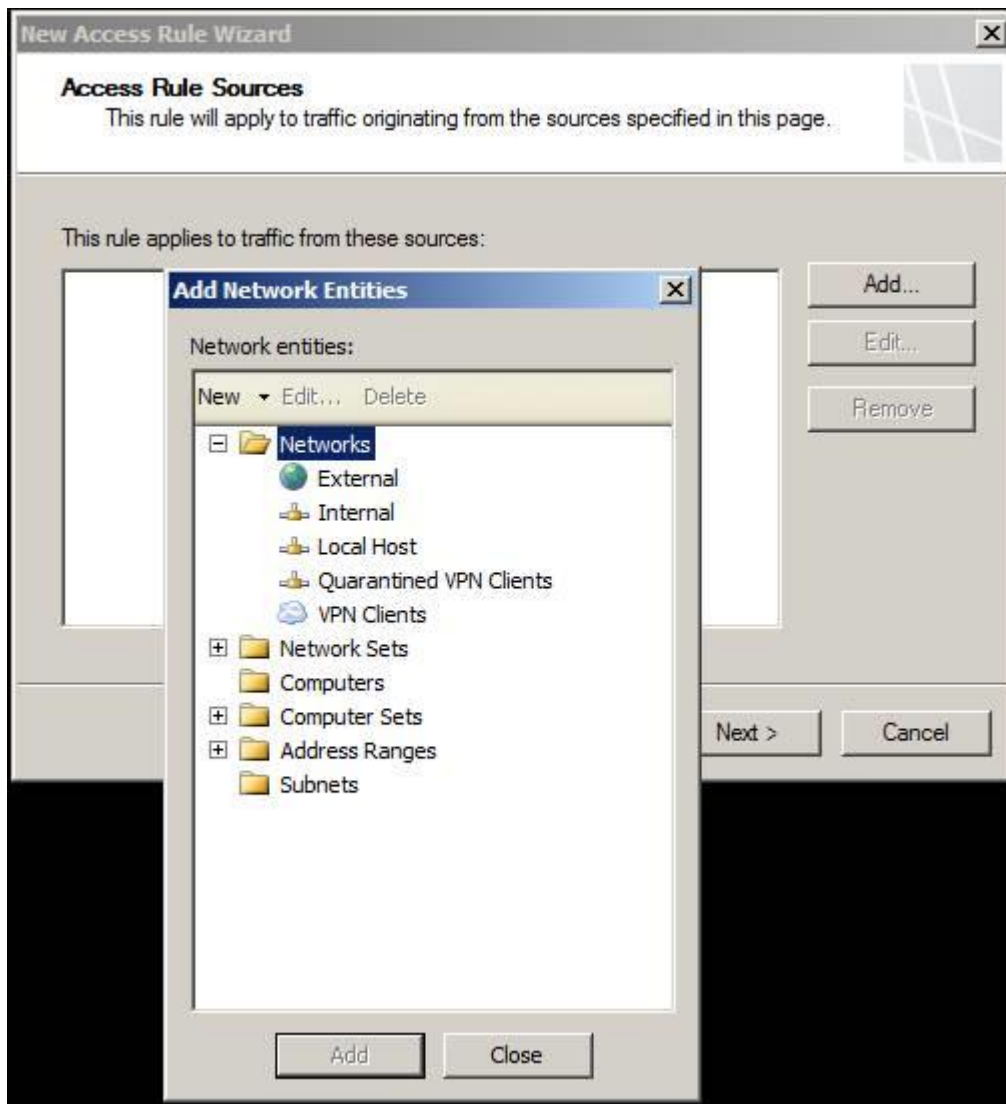




Hình 7

Chúng ta sẽ không chọn bất cứ cổng nguồn nào lúc này mà sẽ chọn tùy chọn **All outbound traffic** và sau đó kích **Next**.

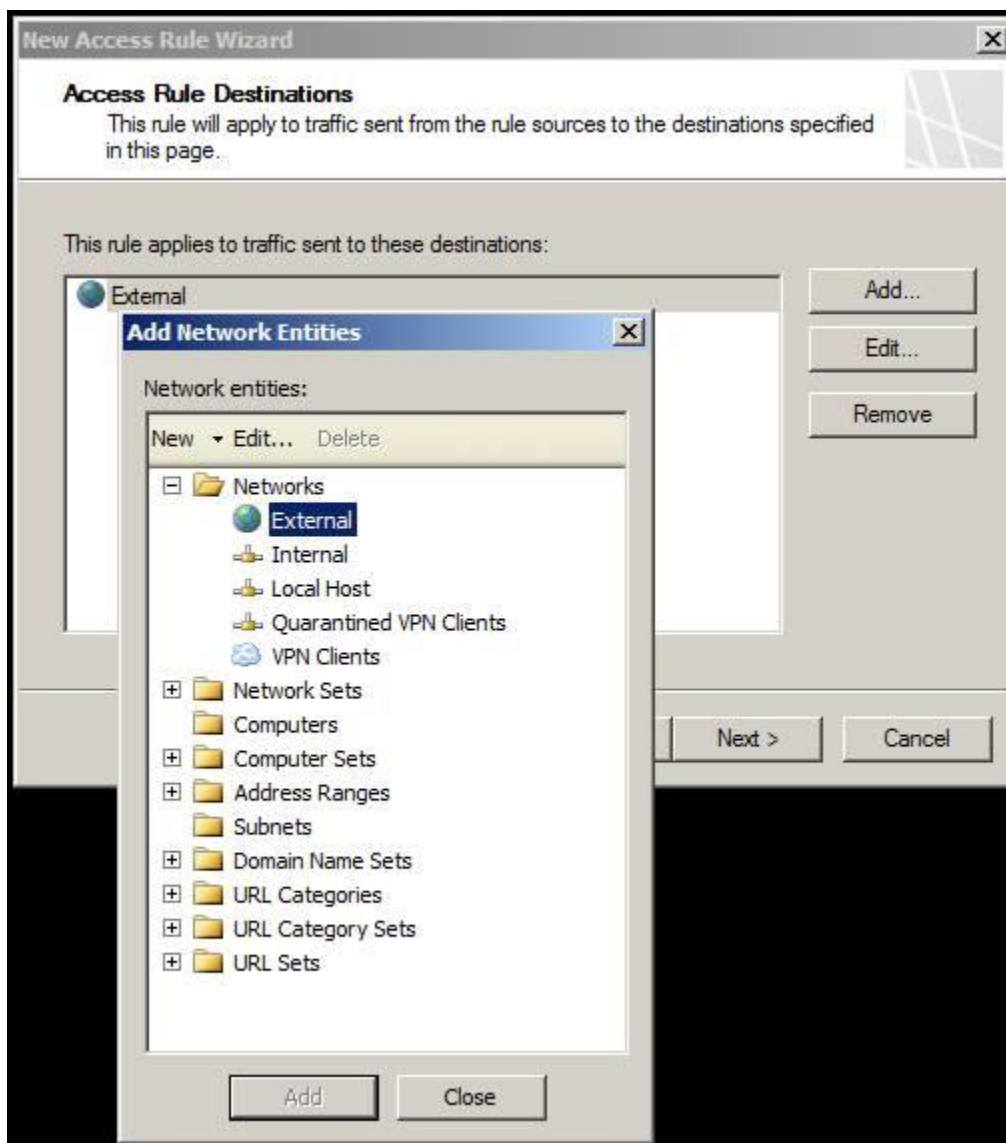
Trang tiếp theo là **Access Rule Sources**. Ở đây bạn sẽ chọn vị trí của các máy tính nằm phía sau tường lửa TMG mà bạn muốn áp với rule này. Kích nút **Add** khi đó bạn sẽ thấy hộp thoại **Add Network Entities**. Kích thư mục có chứa thành phần mạng hiện diện vị trí nguồn của các máy tính mà bạn muốn áp với rule này. Trong ví dụ này, chúng ta sẽ cấu hình rule này áp với tất cả các máy tính nằm trên mạng bên trong mặc định bằng cách kích thư mục **Networks** và sau đó kích đúp vào mạng **Internal**.



Hình 8

Sau khi chọn Network nguồn là Internal Network và kích **Next**, bạn sẽ thấy trang kế tiếp, đây là trang **Access Rule Destinations**. Ở đây bạn thiết lập các đích đến mà bạn muốn các máy tính từ nguồn đã chọn trước có thể truy cập qua rule này. Trang **Access Rule Destinations** làm việc giống như trang trước, nơi bạn kích nút **Add** và sau đó trong hộp thoại **Add Network Entities**, kích thư mục, tiếp nữa là kích đúp vào thành phần mạng muốn cho phép truy cập bằng rule này. Trong ví dụ này, chúng ta sẽ chọn mạng **External** mặc định.

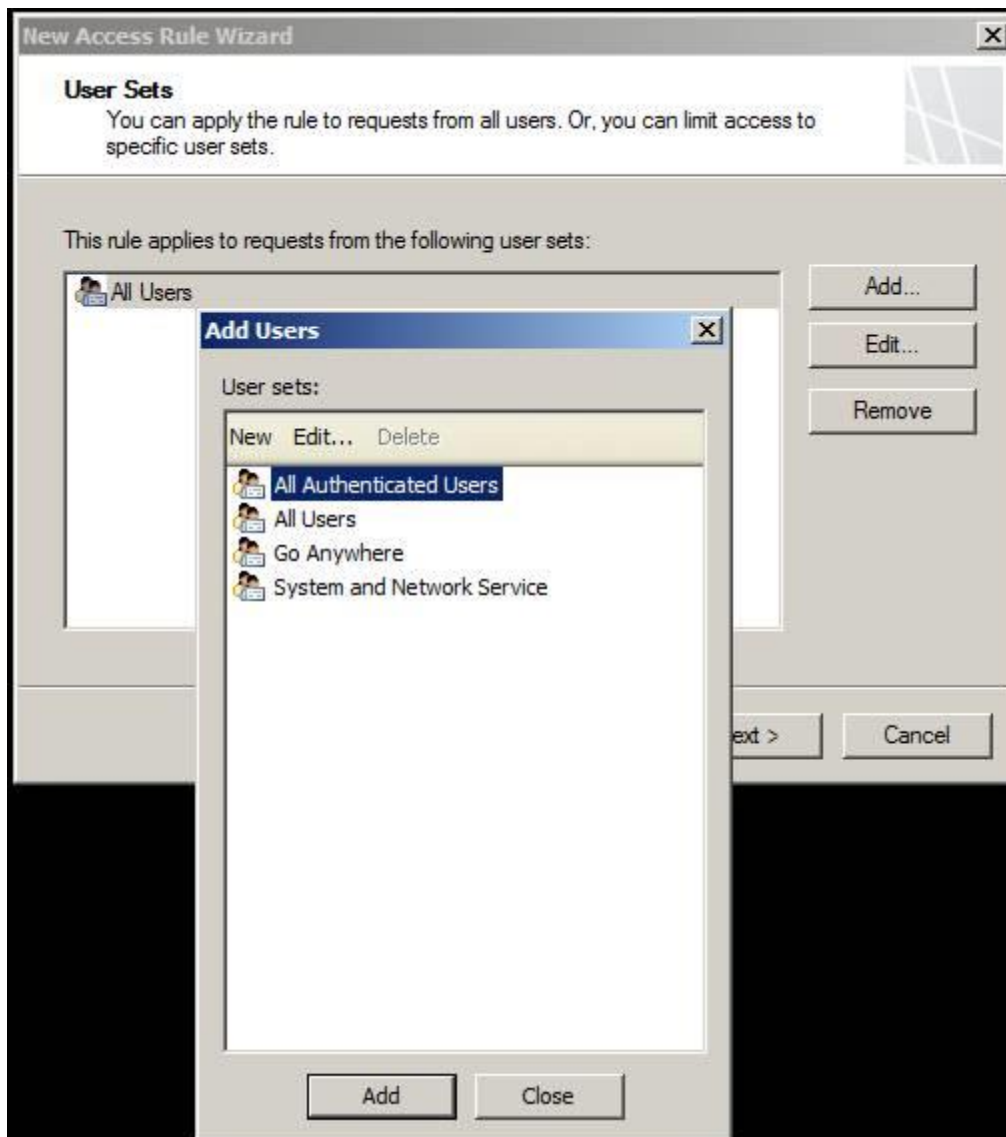




Hình 9

Trang tiếp theo của wizard là **User Sets**. Trong trang này, bạn chỉ định người dùng mà mình muốn áp với rule này. Mặc định, Access Rules được áp cho tất cả người dùng. Còn lúc này, định nghĩa “all users” của bạn có thể không giống như định nghĩa “all users” của tường lửa TMG. “All users” không có nghĩa rule của bạn sẽ áp với tất cả các tài khoản trong tổ chức của bạn mà “All users” từ phối cảnh của tường lửa TMG có nghĩa tất cả người dùng nặc danh – các kết nối không được nhận thực. Nếu kích nút **Add**, bạn có thể chọn người dùng khác, chẳng hạn như **All Authenticated Users** hoặc **System and Network Service**. Cũng có thể tạo các tập người dùng tùy biến dựa trên Active Directory và các tài khoản RADIUS. Tuy nhiên chúng ta sẽ đề cập thêm về các tùy chọn này trong phần tiếp theo. Trong ví dụ này, chúng ta sẽ chọn tùy chọn **All Users** và kích **Next** để chuyển sang trang khác.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 10

Trang cuối cùng của wizard là **Completing the New Access Rule Wizard**. Đây là trang cho phép bạn xem lại các thiết lập của mình và sau đó kích **Finish**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 11  
[Key4VIP.info](http://www.Key4VIP.info)

Sau khi rule đã được tạo, nó sẽ vẫn chưa có hiệu lực cho tới khi bạn kích nút **Apply** ở phía trên của panel ở giữa trong TMG firewall console. Chúng ta sẽ kích nút **Apply** này ngay bây giờ.



Hình 12

### Các tùy chọn khác

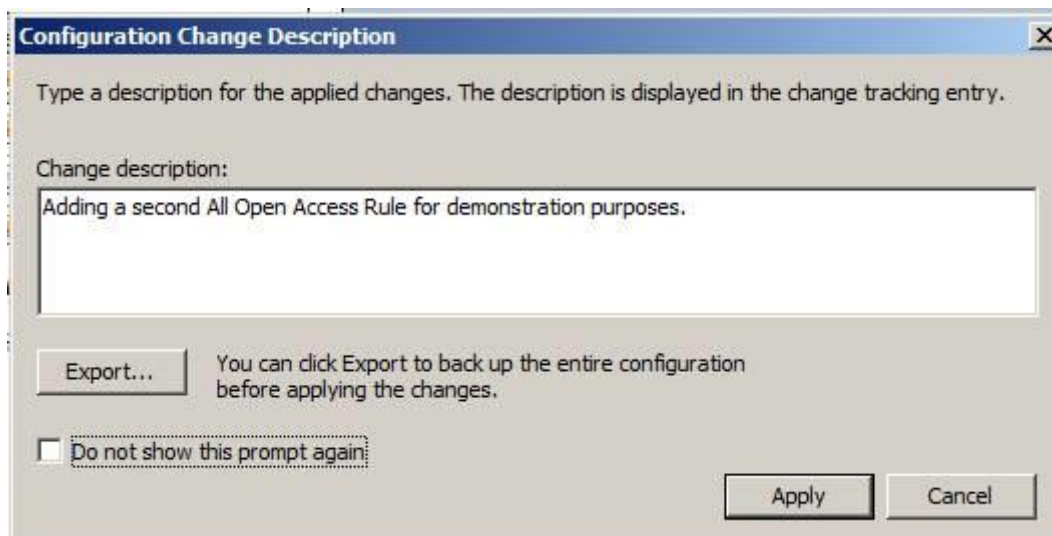
Sau khi kích nút **Apply**, hộp thoại **Configuration Change Description** sẽ xuất hiện. Ở đây bạn có thể thêm vào phần mô tả cho những thay đổi mà bạn đã thực hiện đối với chính sách tường lửa và phần mô tả này sẽ xuất hiện trong bản ghi về sự thay đổi. Bản ghi về sự thay đổi rất hữu dụng khi bạn cần kiểm tra lại và tìm ra những gì bạn hoặc ai đó đã thực hiện đối với chính sách tường lửa trong trường hợp gặp vấn đề gì đó không như mong đợi.

Lưu ý rằng bạn có một tùy chọn để backup chính sách tường lửa bằng cách kích **Export**. Thao tác này cho phép bạn backup cấu hình để có thể khôi phục trở về thời điểm trước khi thực hiện thay đổi. Bạn

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

cũng có tùy chọn không hiển thị nhắc nhở này trong tương lai, tuy nhiên chúng tôi không khuyến khích bạn chọn tùy chọn này vì đây là hộp thoại rất hữu dụng cho bạn trong tương lai. Lúc này chúng ta hãy kích **Apply**.

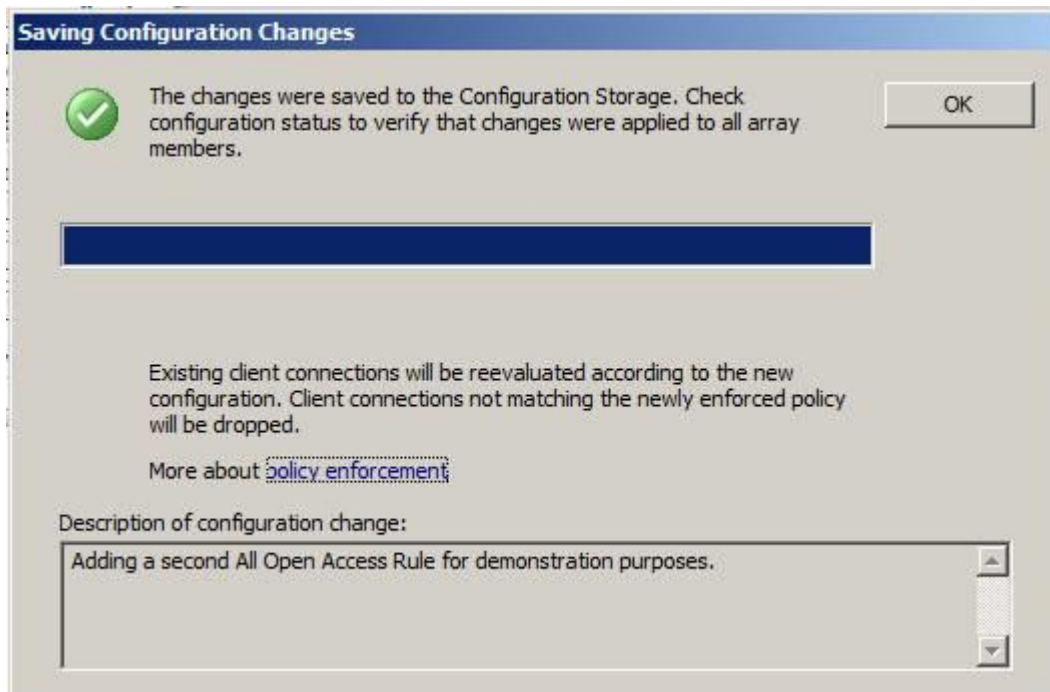


Hình 13

Hộp thoại **Saving Configuration Changes** xuất hiện và cho bạn biết rằng các thiết lập chính sách tường lửa đã được lưu vào kho lưu trữ cấu hình. Lưu ý dòng chữ **“Existing client connections will be reevaluated according to the new configuration. Client connections not matching the newly enforced policy will be dropped”** có nghĩa “Các kết nối máy khách đang tồn tại sẽ bị định giá lại theo cấu hình mới. Các kết nối máy khách không tương ứng với chính sách mới sẽ bị chặn”. Đây là một tính năng mới trong tường lửa TMG. Với tường lửa ISA, chính sách tường lửa mới chỉ được áp dụng cho các kết nối mới, không áp dụng cho các kết nối đang tồn tại. Đây là một cải thiện tuyệt vời và là một trong những lý do bạn nên nâng cấp lên phiên bản mới nhất của tường lửa ISA – mang tên TMG.

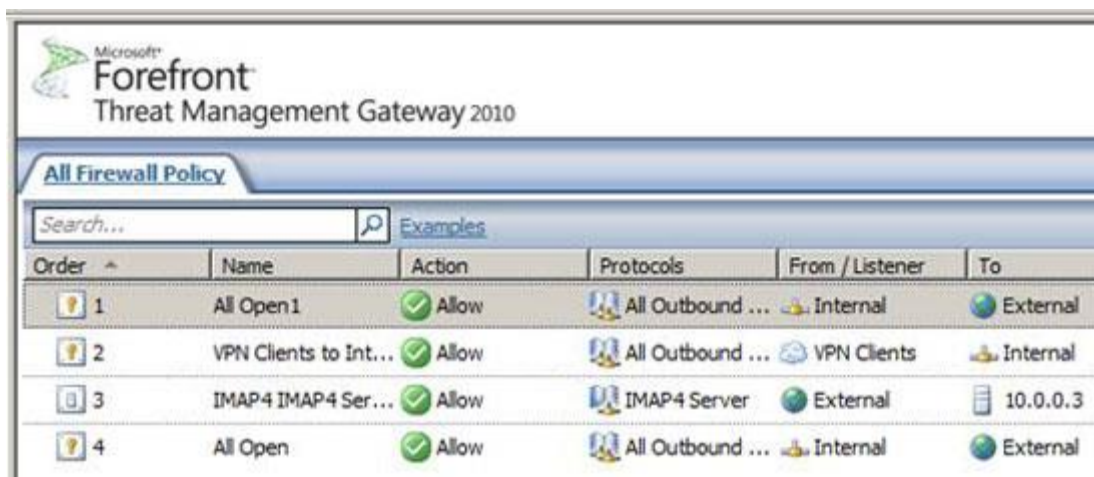
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 14

Rule mới này xuất hiện trong danh sách chính sách của tường lửa, như những gì bạn có thể thấy trong hình bên dưới. Vị trí trên danh sách phụ thuộc vào nơi bạn đã kích khi bắt đầu wizard. Mặc dù vậy, như những gì chúng tôi sẽ giới thiệu cho các bạn trong phần tiếp theo, bạn có thể đẩy rule này lên trên hoặc xuống dưới trong danh sách.



Hình 15

## Kết luận

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Trong bài này, chúng tôi đã giới thiệu cho các bạn một số vấn đề cơ bản về Access Rules của tường lửa TMG. Như những gì các bạn thấy, Access Rules được sử dụng để điều khiển lưu lượng gửi ra từ mạng được bảo vệ TMG đến các mạng khác. Mặc định, không có Access Rules và không có lưu lượng nào có thể qua tường lửa TMG. Một Access Rule cần phải được thiết lập để cho phép lưu lượng gửi ra. Access Rules cho phép bạn có thể điều khiển lưu lượng, dựa trên một số các hệ số, chẳng hạn như vị trí nguồn, vị trí đích, người dùng, các giao thức sẽ được sử dụng. Ngoài ra còn có nhiều tùy chọn khác chưa được lộ diện trong Access Rule wizard, và chúng tôi sẽ giới thiệu cho các bạn các tùy chọn này trong phần tiếp theo.

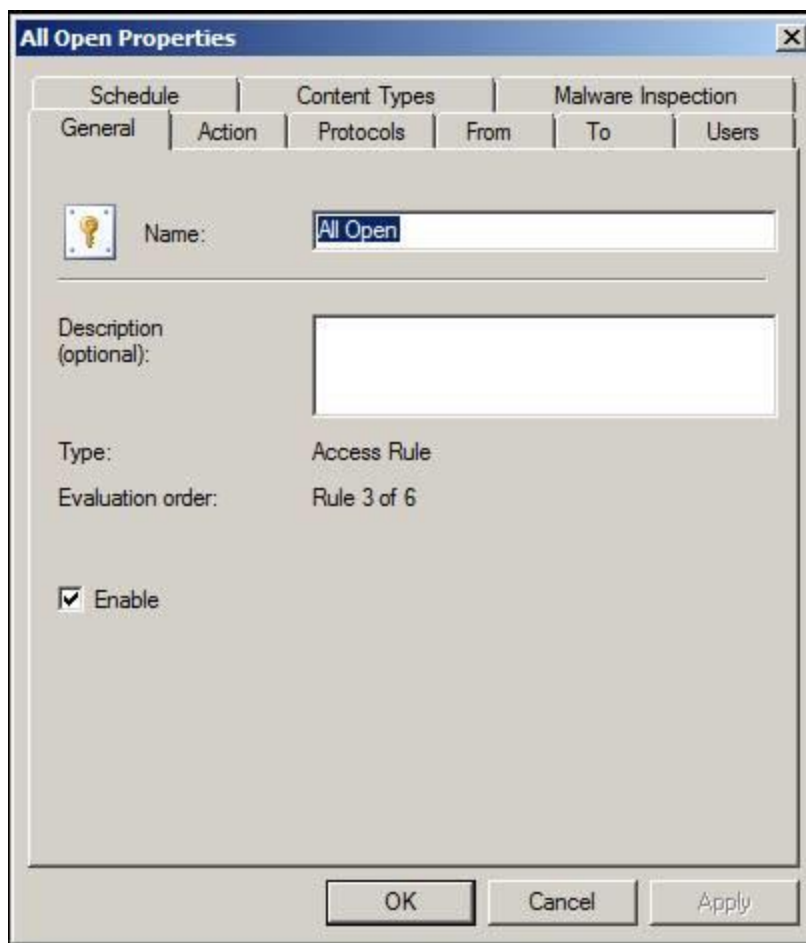
**Trong phần hai của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn chi tiết về Access Rules sau khi đã cùng nhau đi tạo xong một rule bằng wizard trong phần 1.**

Trong phần 1 của loạt bài gồm có hai phần về Access Rules này, chúng tôi đã giới thiệu cho các bạn về mục đích và quá trình tạo Access Rule cũng như cách sử dụng Access Rule wizard cho việc tạo một rule nào đó. Trong phần này, chúng tôi sẽ giới thiệu cho các bạn chi tiết về Access Rules sau khi đã cùng nhau đi tạo bằng wizard trong phần 1. Chúng tôi muốn thực hiện điều này là vì có một số thiết lập không lộ diện trong Access Rule wizard.

Nếu kích đúp vào một rule truy cập nào đó sau khi tạo nó, bạn sẽ thấy hộp thoại **Properties** cho rule xuất hiện. Tab đầu tiên mà bạn sẽ thấy là tab **General**. Ở đây bạn có thể đặt lại tên của rule và cung cấp phần mô tả cho nó. Chúng tôi thấy phần mô tả là rất hữu dụng, vì bạn có thể minh chứng bằng tài liệu mục đích của rule, ai đã tạo rule, rule được tạo khi nào và lý do nó được tạo, chẳng hạn như ai đó đã yêu cầu tạo rule hoặc vấn đề doanh nghiệp nào đó mà nó cần giải quyết.

Lưu ý rằng thứ tự đánh giá **Evaluation order** nằm trong tab này. Mặc dù vậy, bạn cần biết đây là thứ tự đánh giá cho danh sách các rule tường lửa nằm bên ngoài các rule System Policy. Các rule System Policy luôn được đánh giá trước các rule chính sách. Bạn cũng có thể kích hoạt hoặc vô hiệu hóa rule bằng cách sử dụng hộp kiểm **Enable**.





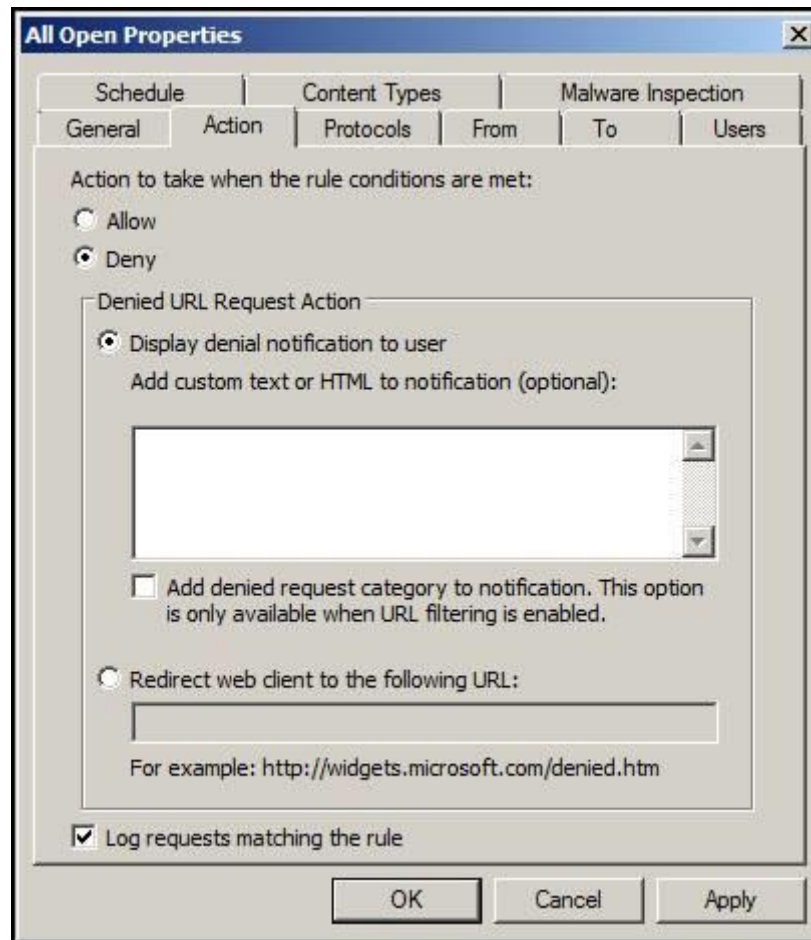
Hình 1

Trên tab **Action**, bạn có một số tùy chọn:

- **Allow** – Khi chọn tùy chọn này, rule sẽ trở thành rule cho phép và khi cố gắng kết nối khớp với các thiết lập trong rule này, kết nối sẽ được cho phép.
- **Deny** – Khi chọn tùy chọn này, rule trở thành rule từ chối và cố gắng kết nối khớp với các thiết lập trong rule này, kết nối sẽ bị từ chối.
- **Display denial notification to user** – Nếu rule là HTTP rule và chọn tùy chọn này thì bạn có thể nhập vào một đoạn văn bản, đoạn văn bản này sẽ được trả về với người dùng khi kết nối bị từ chối. Thông tin này sẽ được hiển thị trong cửa sổ của trình duyệt. Bằng cách sử dụng tùy chọn này, bạn có thể cho phép người dùng biết tại sao kết nối bị từ chối.
- **Add denied request category to notification** – Tùy chọn này chỉ có sẵn khi URL filtering được kích hoạt nếu kích hoạt URL filtering trên tường lửa TMG của mình, bạn sẽ có tùy chọn để cho phép người dùng biết, khi yêu cầu bị từ chối, site mà người dùng cố gắng truy cập nằm trong hạng mục nào. Nói chung, người dùng không thực sự quan tâm đến các thông tin này, tuy nhiên nếu bạn có các rule áp cho các quản trị viên và một số người dùng đặc biệt, rất có thể họ sẽ quan tâm đến các thông tin này để tạo các yêu cầu nhằm phân loại lại các site.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

- **Redirect web client to the following URL** – Nếu không muốn cung cấp cho người dùng một trang hiển thị tại sao kết nối bị từ chối, bạn có tùy chọn để chuyển hướng (redirect) người dùng đến một website nào đó. Đây có thể là website gồm có các hạng mục thỏa thuận dịch vụ mà bạn đặt ra với người dùng hoặc một site giáo dục cung cấp cho họ các thông tin về việc sử dụng thích hợp kết nối Internet công ty.
- **Log requests matching this rule** – Tùy chọn này được kích hoạt mặc định và cho phép các kết nối khớp với rule này sẽ được ghi vào trong bản ghi của tường lửa TMG. Mặc dù vậy, sẽ có lần bạn không muốn ghi các thông tin – chẳng hạn như lưu lượng không thích hợp. Điều này sẽ làm giảm được kích thước tổng thể của file bản ghi và tạo cho các bản ghi của bạn trong sáng hơn, dễ dàng đọc và phân tích cú pháp hơn.



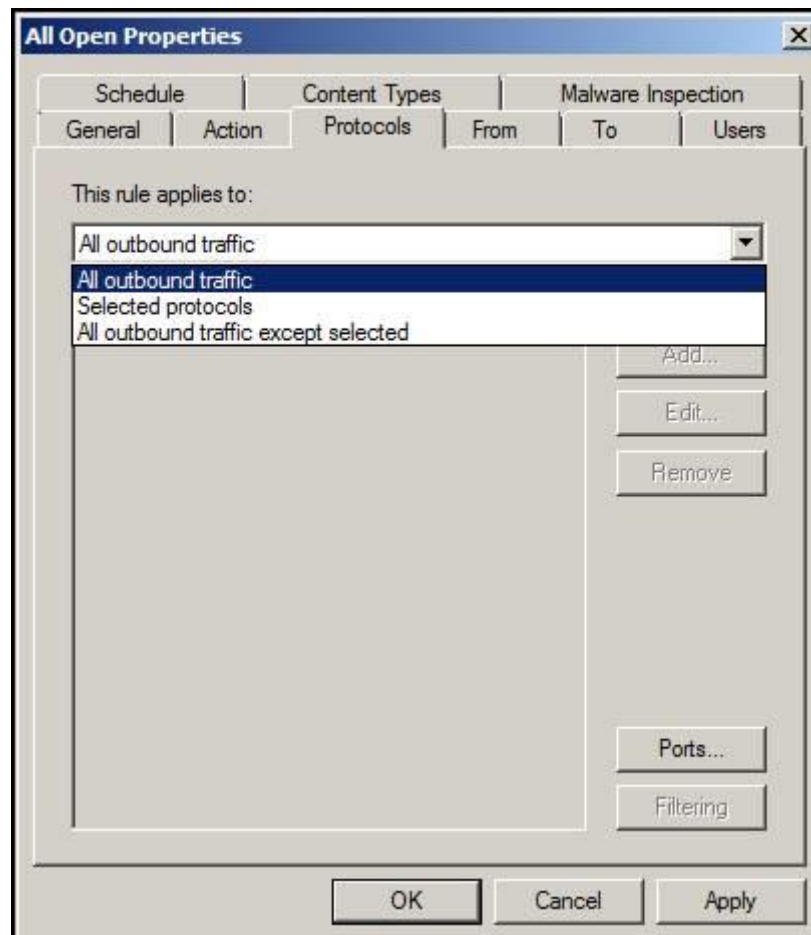
Hình 2

Trong trang **Protocols**, bạn có một số tùy chọn tương tự như các tùy chọn có trong Access Rule wizard. Hộp chọn **This rule applies to** cũng cung cấp các tùy chọn tương tự và bạn có thể sử dụng các nút **Add**, **Edit** và **Remove** để chỉnh sửa, thêm, bớt các giao thức sẽ áp với rule này. Bạn cũng có tùy chọn **Ports** đã có sẵn. Nút **Filtering**, khi được kích hoạt, sẽ cho phép bạn cấu hình **HTTP Policy** cho rule (nếu nó là một HTTP rule). Tính năng này được nhóm vào các phiên bản trước của tường lửa ISA, được biết đến nhiều hơn với các tên **HTTP Security Filter**. Cũng có thể có các bộ lọc khác – phụ

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

thuộc vào giao thức bạn sử dụng – nếu bộ lọc có thể áp với các giao thức gửi ra. Hầu hết các bộ lọc giao thức mà chúng ta có với TMG đều được thiết kế để bảo vệ kết nối gửi vào, tuy nhiên có một số áp cho các giao thức gửi ra.

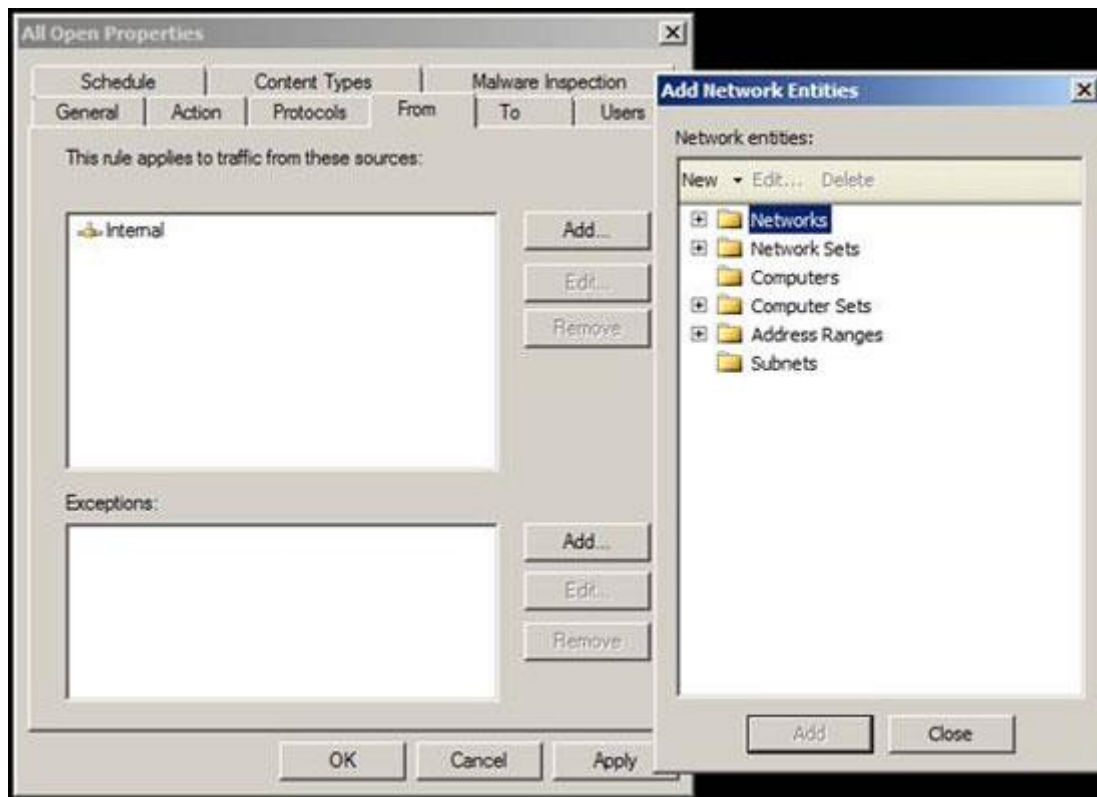


Hình 3

Trong tab **From**, bạn có thể định nghĩa các nguồn mà rule sẽ áp cho chúng. Có nhiều máy khách nằm trên mạng bảo vệ TMG. Tùy chọn này tương tự như những gì bạn thấy trong Access Rule wizard. Khi kích **Add**, bạn sẽ thấy xuất hiện hộp thoại **Add Network Entities** và có thể chọn từ một số entry mạng hoặc tạo các entry mới. Một tùy chọn có sẵn trong tab này nhưng không lộ diện trong Access Rule wizard là phần **Exceptions**. Ở đây bạn có thể thiết lập các nguồn mà mình muốn rule áp với nó, tuy nhiên lại có một tập con bên trong nhóm đó là ngoại lệ, bạn có thể đặt các trường hợp ngoại lệ đó vào phần **Exceptions**. Đây là một tùy chọn hết sức mạnh và đôi khi cần phải lưu ý trong thiết kế Access Rules của bạn.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

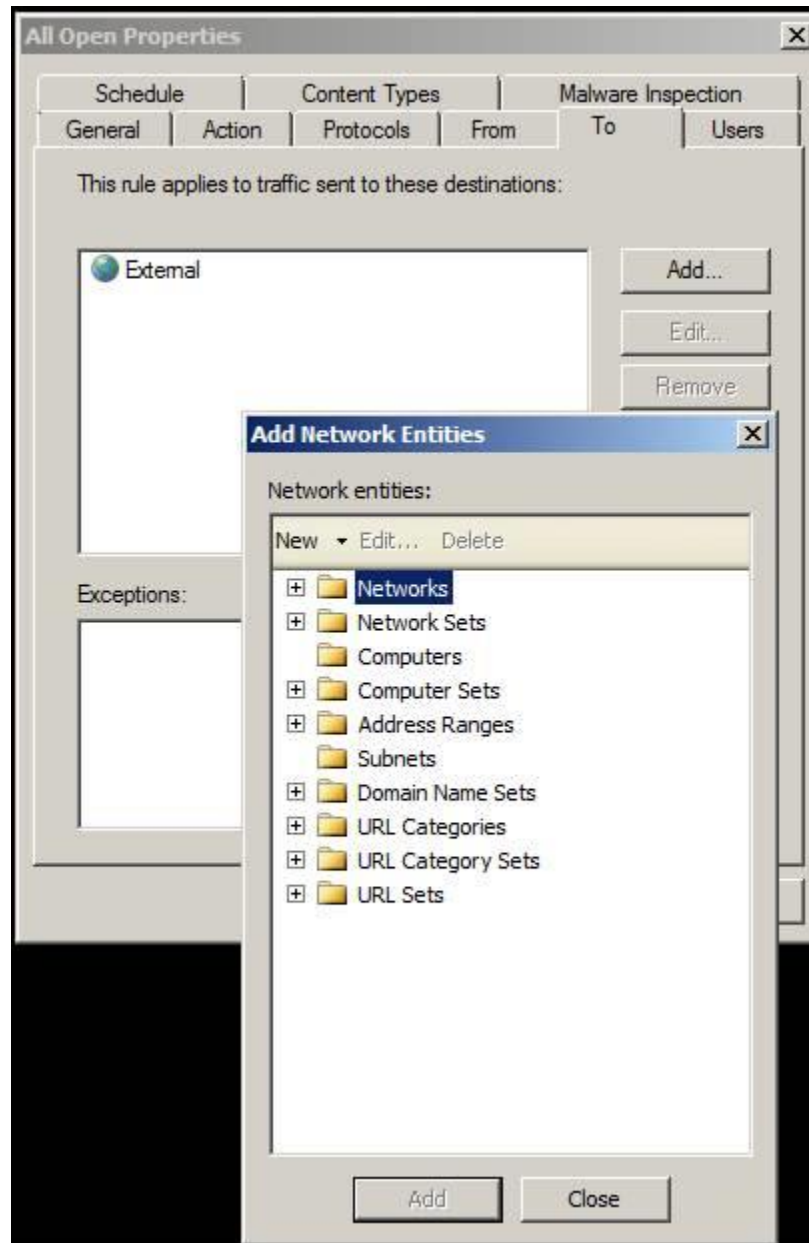


Key4VIP.info

Tab **To** cũng tương tự với tab **From**, nơi bạn định nghĩa đích mà mình muốn rule khớp với. Khi kích **Add**, bạn sẽ thấy hộp thoại **Add Network Entities**, có thể chọn đích từ danh sách hoặc có thể tạo một đích mới. Như bên trong tab **From**, bạn cũng có tùy chọn cho việc tạo các ngoại lệ **Exceptions**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 5

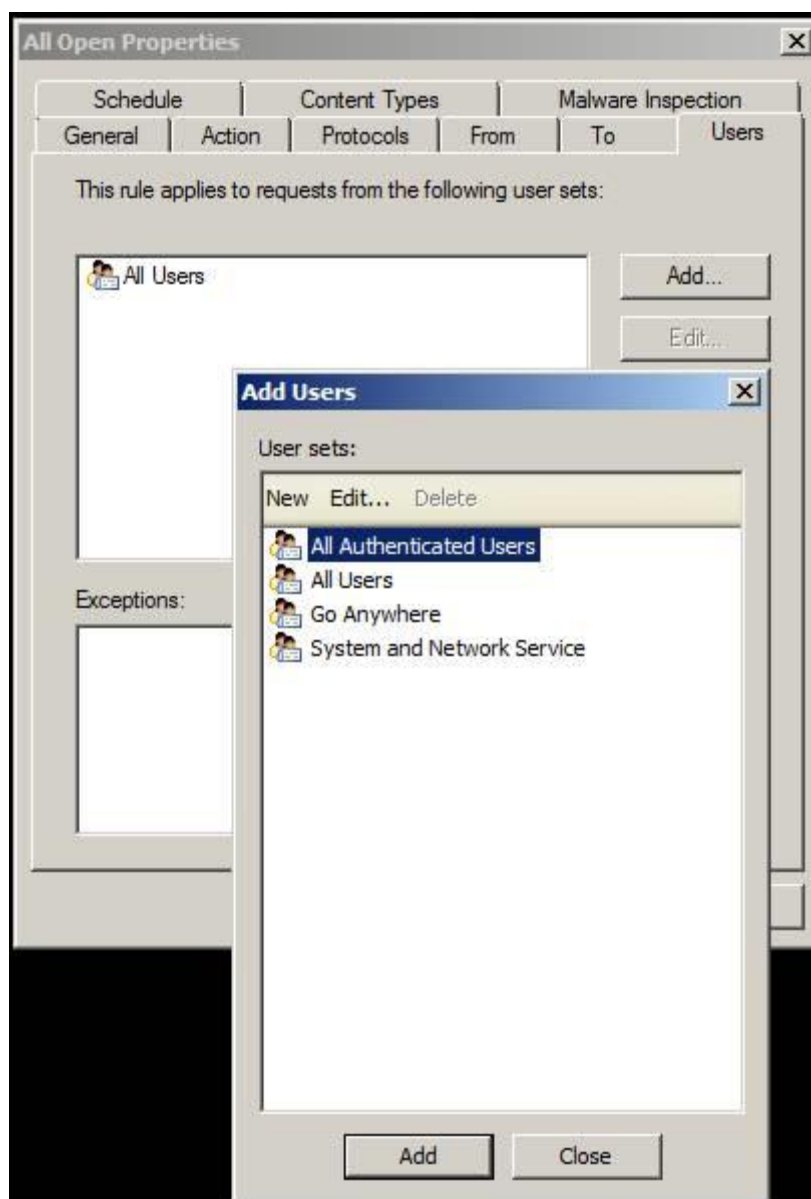
Trong tab **Users**, bạn có thể định nghĩa rule sẽ áp cho người dùng nào. Mặc định, **All Users** là tập người dùng được sử dụng cho Access Rules. Cần lưu ý **All Users** ở đây không thực sự có nghĩa là tất cả người dùng mà chỉ là các kết nối nặc danh và các kết nối được nhận thực – vì vậy nó có nghĩa “phạm vi người dùng không được xem xét”. Nếu bạn muốn bắt người dùng phải nhận thực, bạn cần phải sử dụng một tập người dùng khác và remove tập người dùng **All Users**.

Nếu kích **Add**, bạn có thể chọn **All Authenticated Users** và chỉ có người dùng có thể nhận thực với tường lửa TMG mới được phép truy cập qua rule này. Sự nhận thực có thể được thực hiện qua cấu hình

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

web proxy máy khách hoặc cấu hình Firewall máy khách (TMG máy khách). Nếu muốn tạo một tập người dùng của riêng mình, bạn hãy kích nút **New**.



Hình 6

Khi kích **New**, chương trình sẽ khởi chạy **Welcome to the New User Set** wizard. Trên trang đầu tiên của wizard, nhập vào tên cho tập người dùng. Trong ví dụ này, chúng ta sẽ tạo một tập người dùng gồm có nhóm Domain Admins Active Directory, vì vậy hãy đặt tên cho rule này là **Administrators** và kích **Next**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..





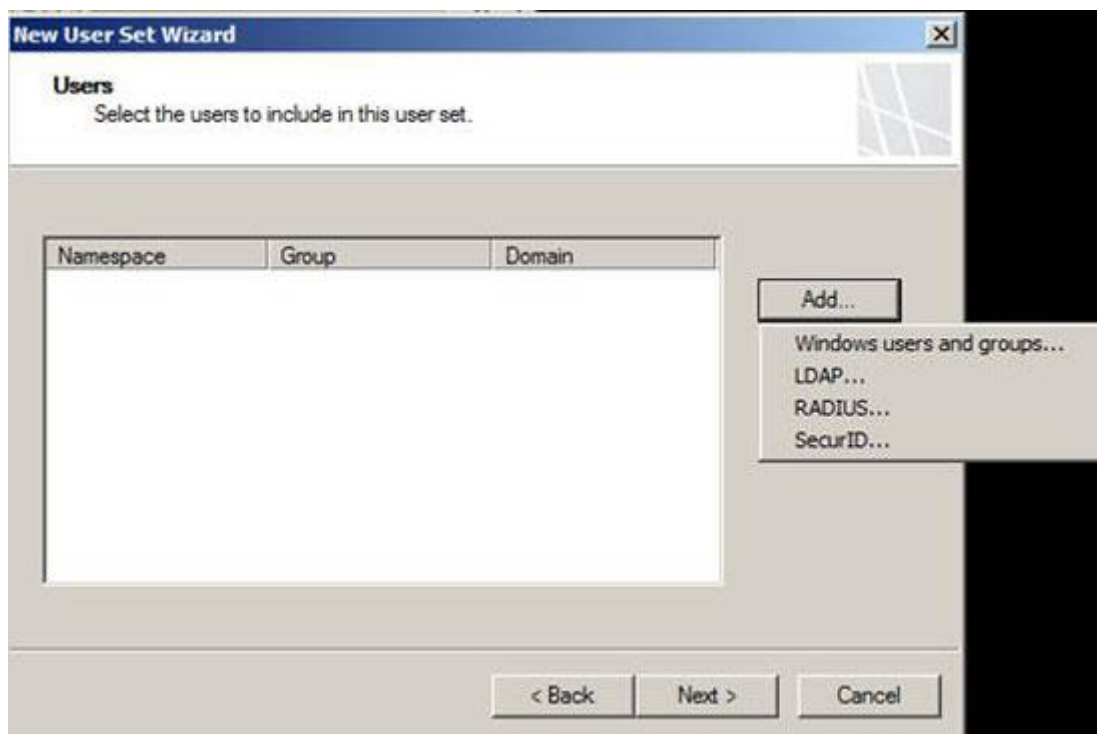
Hình 7  
[www.Key4VIP.info](http://www.Key4VIP.info)

Trong trang **Users**, khi kích **Add**, một menu sẽ xuất hiện. Menu này gồm có các nguồn nhận thực sau:

- **Windows users and groups** – Có nhiều người dùng và nhóm người dùng bên trong miền Active Directory hoặc một miền đích thực mà tường lửa TMG thuộc về nó.
- **LDAP** – Có nhiều người dùng và nhóm người dùng bên trong Active Directory và bạn có thể sử dụng khi tường lửa TMG không phải là một thành viên của miền. Cần lưu ý rằng TMG không hỗ trợ nhận thực LDAP cho Access Rules.
- **RADIUS** – Có người dùng có thể truy cập qua RADIUS. Lưu ý rằng bản thân RADIUS không hỗ trợ Group Membership, mặc dù vậy bạn có thể tạo một tập người dùng có chứa nhiều tài khoản có thể truy cập thông qua RADIUS, một thứ khá hiệu quả trong các nhóm đặc biệt trên tường lửa TMG. RADIUS được hỗ trợ cho các kết nối web gửi ra qua tường lửa TMG.
- **SecurID** – Có nhiều người dùng được định nghĩa bởi SecurID. Tuy nhiên SecurID không được hỗ trợ cho các kết nối gửi ra qua tường lửa TMG thông qua Access Rules.

Trong ví dụ này, tường lửa TMG đã gia nhập vào miền Active Directory, vì vậy chúng ta sẽ chọn **Windows users and groups**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

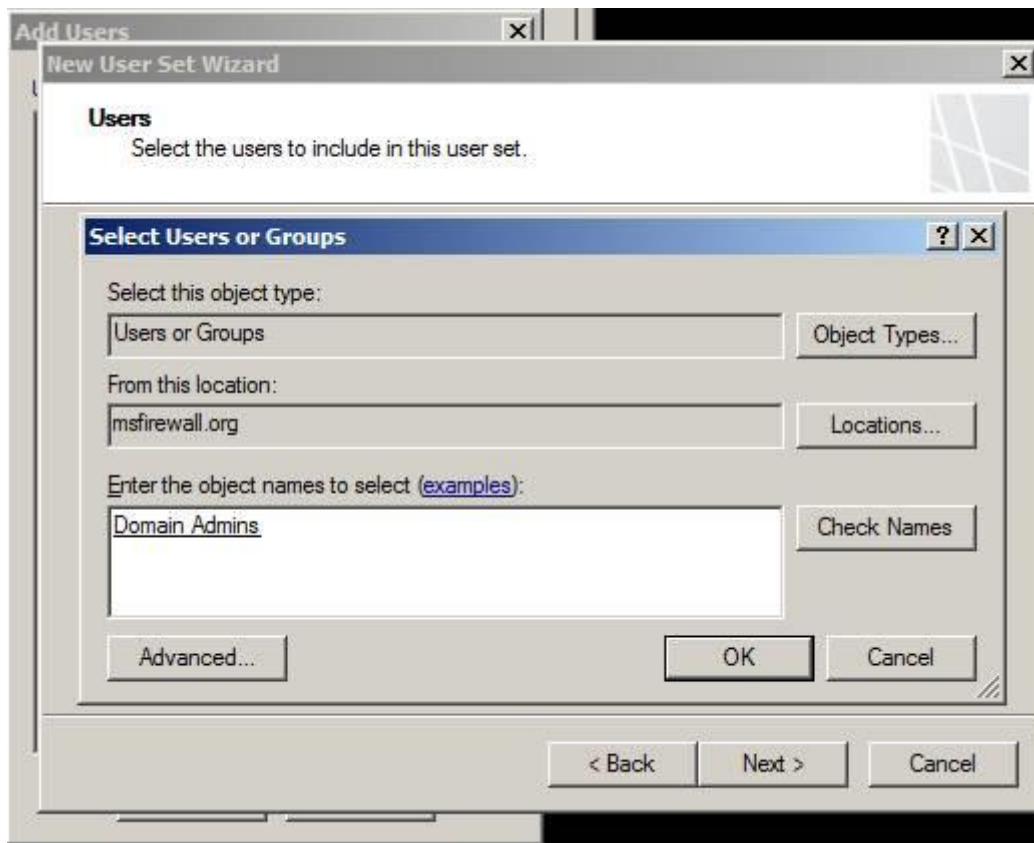


Hình 8

Bạn sẽ thấy xuất hiện hộp thoại **Select Users or Groups**. Chúng ta nhập **Domain Admins** vào trong hộp văn bản **Enter the object names to select** và kích **Check Names** sau đó kích **OK** để thêm nhóm Active Directory này vào tập người dùng.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

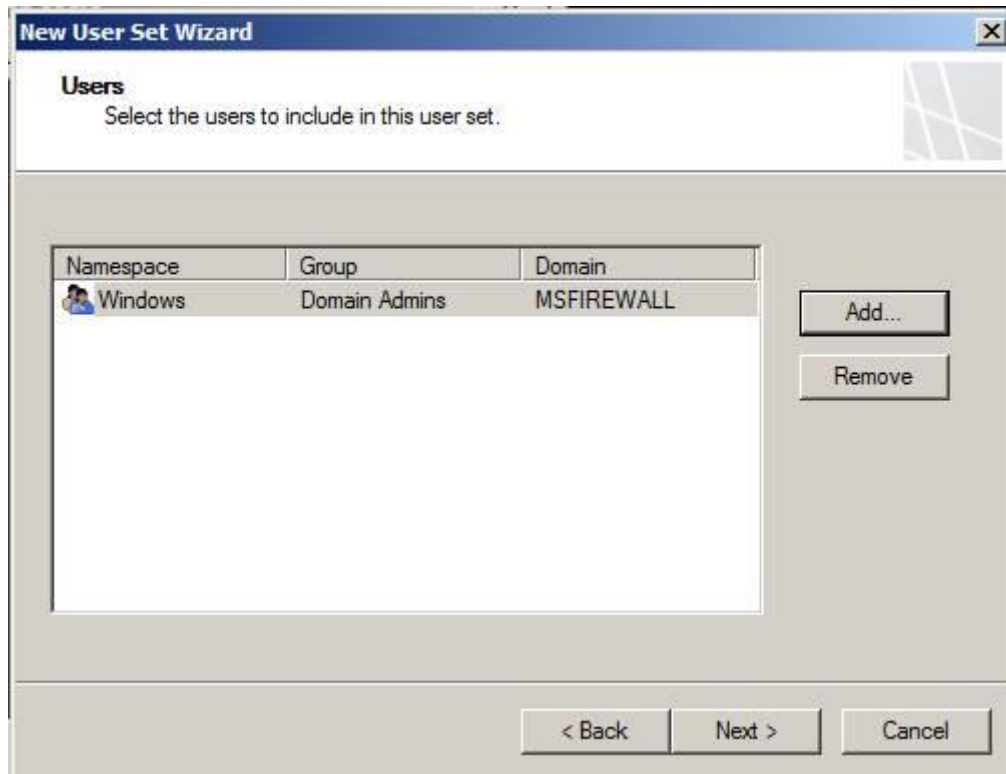


Hình 9

Bạn sẽ thấy tập người dùng mới trên trang **Users**. Có thể thêm nhiều người dùng nữa vào tập người dùng này nếu thích. Trong ví dụ này, chúng ta sẽ kích **Next** và không thêm bất cứ ai vào tập người dùng này.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 10

[www.Key4VIP.info](http://www.Key4VIP.info)

Trong trang **Completing the New User Set Wizard**, kích **Finish** để tạo tập người dùng mới.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 11  
[www.Key4VIP.info](http://www.Key4VIP.info)

Lúc này, bạn có thể tạo nhóm **Administrators** trong hộp thoại **Add Users** và có thể sử dụng nhóm này trong Access Rules và việc publish các rule.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

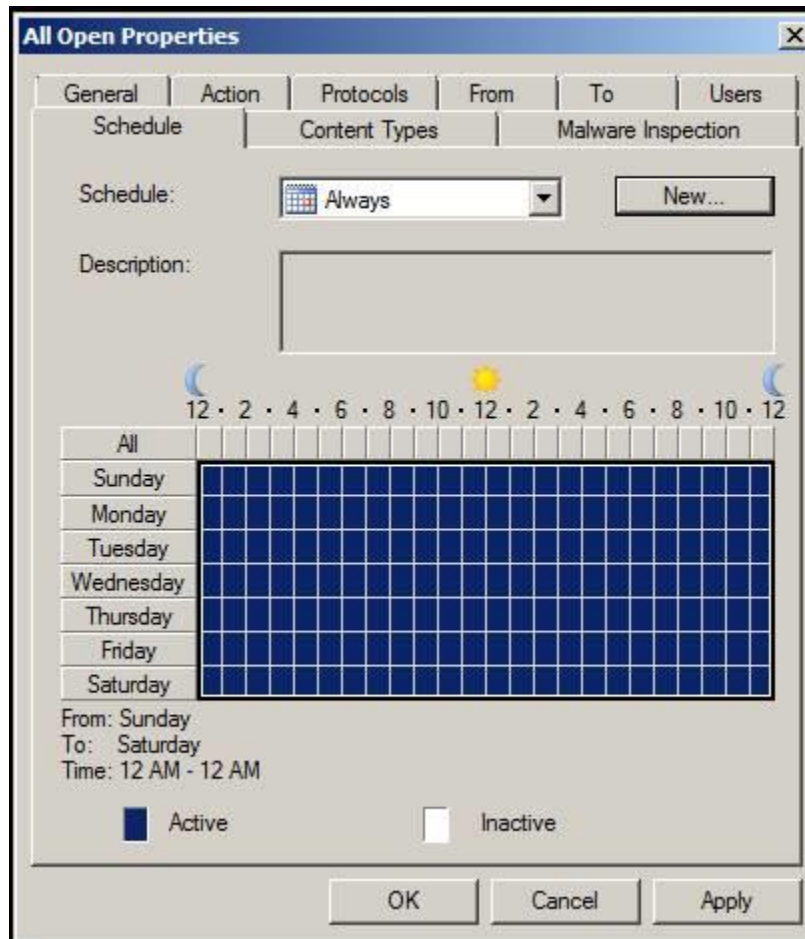


Hình 12

Trên tab **Schedule**, bạn có thể thiết lập một lịch trình cho rule để đặt thời gian rule sẽ được áp dụng. Lưu ý rằng khi bạn định nghĩa một lịch trình, lịch trình sẽ chỉ được áp dụng cho các kết nối mới đề phòng trường hợp người dùng đã kết nối trước khi lịch trình hết hạn, khi đó kết nối của người dùng sẽ không bị đứt. Mặc dù vậy, nếu một cố gắng kết nối mới hợp với rule nằm bên ngoài lịch trình, kết nối đó sẽ bị từ chối. Lịch trình mặc định luôn là **Always**, tuy nhiên có hai lịch trình đi kèm khác: **Weekends** và **Work hours**. Nếu không thích các lịch trình đi kèm này, bạn có thể kích nút **New** và tạo một lịch trình tùy biến.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

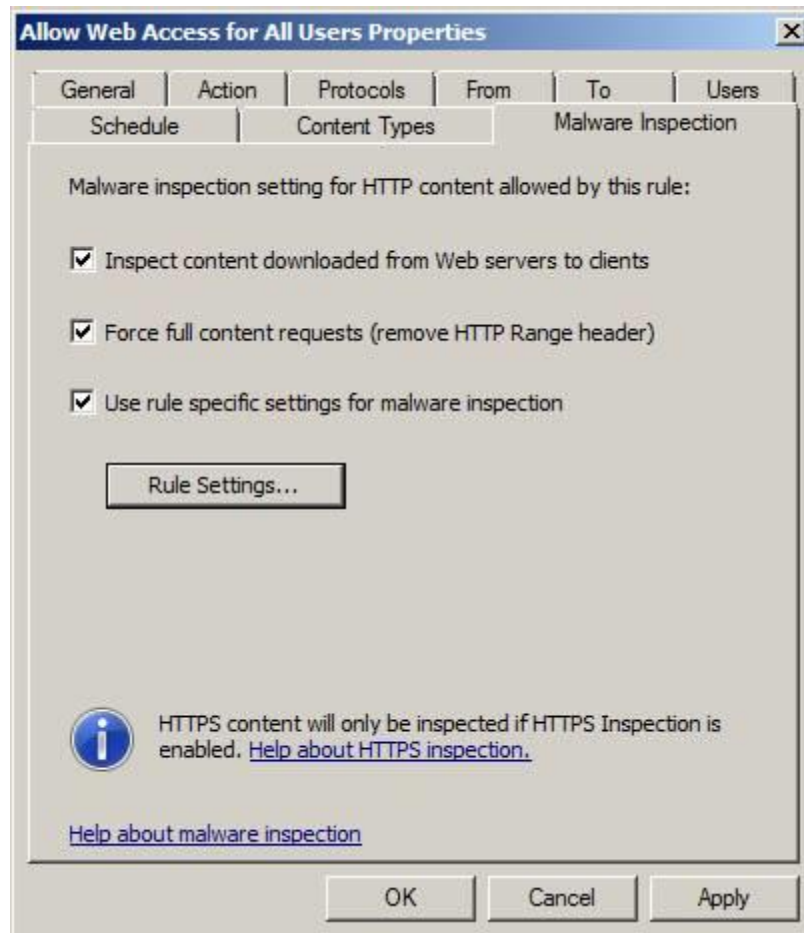




Hình 13

Tab **Malware Inspection** là một tab chỉ có sẵn trên tường lửa TMG. Có một vài tùy chọn trên tab này không được lộ diện trong Access Rule wizard:

- **Inspect content downloaded from web servers to clients** – Khi bạn kích hoạt tùy chọn này, tất cả các nội dung được download từ các máy chủ web sẽ được thanh tra malware bằng Microsoft AV engine đã được sử dụng bởi tường lửa TMG.
- **Force full content requests (remove HTTP Range header)** – Buộc tường lửa phải yêu cầu nội dung hoàn chỉnh để nó có thể được đánh giá một cách toàn bộ. Nếu chỉ đánh giá một dải nào đó, các mối nguy hiểm tiềm tàng có thể bị bỏ sót.
- **Use rule specific settings for malware inspection** – Bạn có thể tùy biến các thiết lập chống malware cho rule khi chọn tùy chọn này. Nếu chọn tùy chọn này, bạn cần kích nút **Rule Settings** để hoàn tất cấu hình tùy biến của mình.



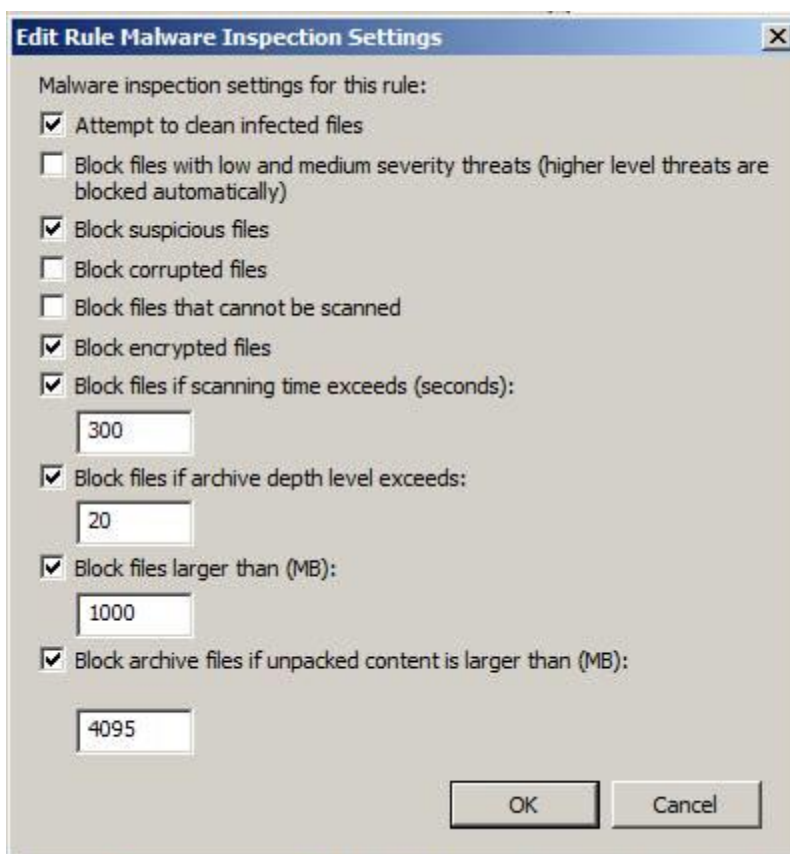
Hình 14

Trong trang **Edit Rule Malware Inspection Settings**, bạn có một số tùy chọn. Hình dưới thể hiện các thiết lập mặc định:

- **Attempt to clean the infected files** – Khi thiết lập này được kích hoạt, tường lửa TMG sẽ cố gắng làm sạch file trước khi chuyển tiếp nó đến người dùng. Nếu file không thể làm sạch, nó sẽ xóa file.
- **Block files with low and medium severity threats (higher level threats are blocked automatically)** – Tường lửa TMG mặc định sẽ không khóa các file ở mức nguy hiểm thông thường và thấp, bằng hệ thống phân loại của Microsoft AM engine.
- **Block suspicious files** – Tường lửa TMG sử dụng phương pháp suy nghiệm để xác định xem một file nào đó có phải là malware hay không. Khi tùy chọn này được chọn, file sẽ bị khóa nếu phương pháp suy nghiệm xác định file có thể là malware.
- **Block corrupted files** – Khi tùy chọn này được kích hoạt, các file được xác định là lỗi sẽ bị khóa.
- **Block files that cannot be scanned** – Khi tùy chọn này được kích hoạt, nếu Microsoft AV engine không thể quét file, file đó sẽ bị khóa.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

- **Block encrypted files** – Nếu file được mã hóa, Microsoft AV engine sẽ không thể đánh giá file và vì vậy, khi tùy chọn này được kích hoạt, nó sẽ khóa file.
- **Block files if scanning time exceeds (seconds)** – Khi tùy chọn này được kích hoạt, nó sẽ hạn chế thời gian Microsoft AV engine có thể đánh giá một file trước khi quyết định chuyển tiếp hoặc khóa nó. Giá trị mặc định là 5 phút.
- **Block files if archive level depth exceeds** - Khi tùy chọn này được kích hoạt, AV engine sẽ khóa các file vượt quá thiết lập về độ sâu lưu trữ ở đây. Giá trị mặc định là 20 mức.
- **Block files larger than (MB)** - Khi tùy chọn này được kích hoạt, nó sẽ khóa các file lớn hơn giá trị được liệt trong hộp văn bản, với giá trị mặc định là 1000MB (1GB). Tùy chọn này có thể được sử dụng để cải thiện hiệu suất trên tường lửa TMG, tuy nhiên bạn cần phải cẩn thận nếu không sẽ khóa các file mà người dùng cần vì khá nhiều người dùng thường làm việc với các file có dung lượng lớn.
- **Block archive files if unpacked content is large than (MB)** – Tùy chọn này thiết lập kích thước lớn nhất của một file được giải nén. Giá trị này được sử dụng để dự trữ bộ nhớ trong tường lửa TMG.



Hình 15

## Kết luận

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

Trong bài này, chúng tôi đã giới thiệu cho các bạn các chi tiết về Access Rules. Hầu hết trong số các tùy chọn mà bạn muốn cấu hình đều đã lộ diện trong Access Rule Wizard, tuy nhiên vẫn có một số tùy chọn quan trọng khác chỉ có thể truy cập sau khi bạn đã tạo rule, bằng cách truy cập vào hộp thoại Properties của rule. Chúng tôi hy vọng loạt bài gồm có hai phần này sẽ giúp ích được cho các bạn, nhất là những người mới làm quen với tường lửa TMG và các thông tin này sẽ giúp các bạn tạo các chính sách truy cập gửi ra phù hợp với tổ chức mình.

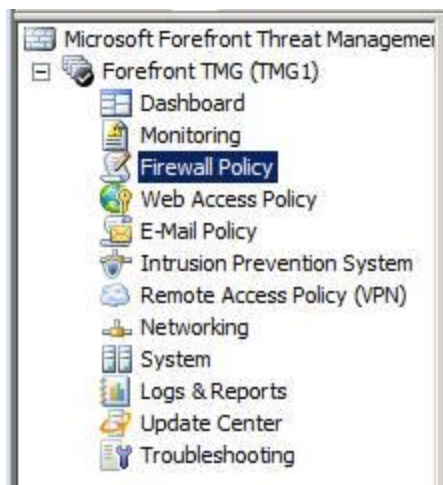
**Trong phần ba của loạt bài giới thiệu về TMG Access Rule, chúng tôi sẽ giới thiệu cho các bạn những vấn đề cơ bản về Web Publishing Rule.**

Web publishing là một thuật ngữ mà chúng ta sử dụng trong việc reverse proxy các website để người dùng bên ngoài có thể truy cập vào các website nằm bên trong tường lửa TMG. Lưu ý rằng có hai cách bạn có thể cho phép người dùng bên ngoài có thể sử dụng các website: web publishing và server publishing. Web publishing cho phép tường lửa TMG hành động như một reverse proxy, trong khi đó server publishing lại cung cấp các máy chủ web thông qua reverse NAT. Trong hai phương pháp này thì Web publishing là phương pháp được ưa thích hơn, với phương pháp này bạn có thể sử dụng ưu điểm của phương pháp tiền nhận thực và nhiều tính năng khác không có sẵn qua reverse NAT.

Để giới thiệu cho các bạn quá trình web publishing, chúng ta hãy bắt đầu bằng cách publish một HTTP site đơn giản nằm phía sau tường lửa TMG. Site cơ bản này không yêu cầu SSL và cũng không yêu cầu nhận thực. Về sau, chúng ta sẽ đi xem xét một số ví dụ phức tạp hơn, trong đó bạn có thể sử dụng SSL và nhận thực.

[Key4VIP.info](http://www.Key4VIP.info)

Để bắt đầu, hãy kích nút **Firewall Policy** trong panel bên trái của giao diện điều khiển TMG firewall, như thể hiện trong hình 1 bên dưới.



Hình 1

Trong panel bên phải của giao diện, kích **Tasks Tab**. Sau đó trên Tasks Tab, kích liên kết **Publish Web Sites** được thể hiện như trong hình 2 bên dưới.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 2

Thao tác này sẽ làm xuất hiện trang **Welcome to the New Web Publishing Rule Wizard**. Trên trang này, hiển thị trong hình 3, bạn cần đặt tên cho rule. Trong hộp văn bản **Web publishing rule name**, lấy ví dụ, chúng ta nhập vào tên *HTTP Web Server* và sau đó kích **Next**.

[Key4VIP.info](http://www.Key4VIP.info)

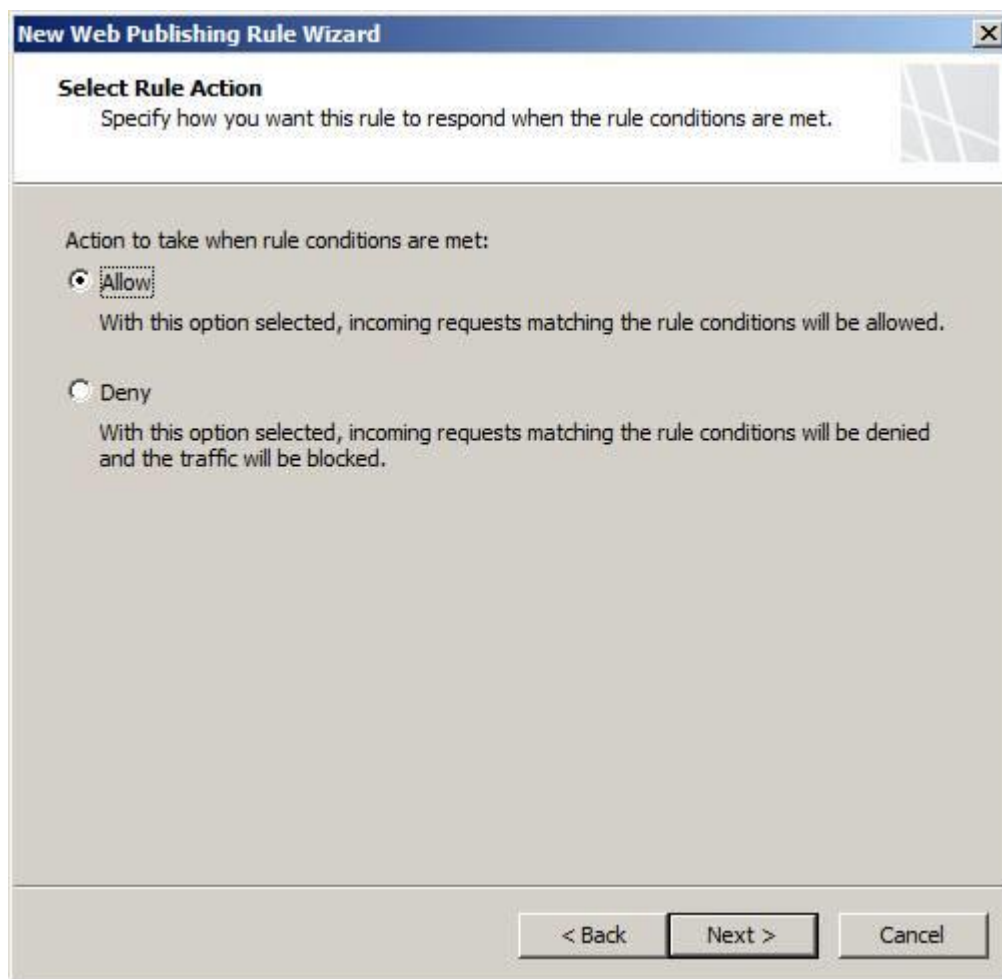
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 3

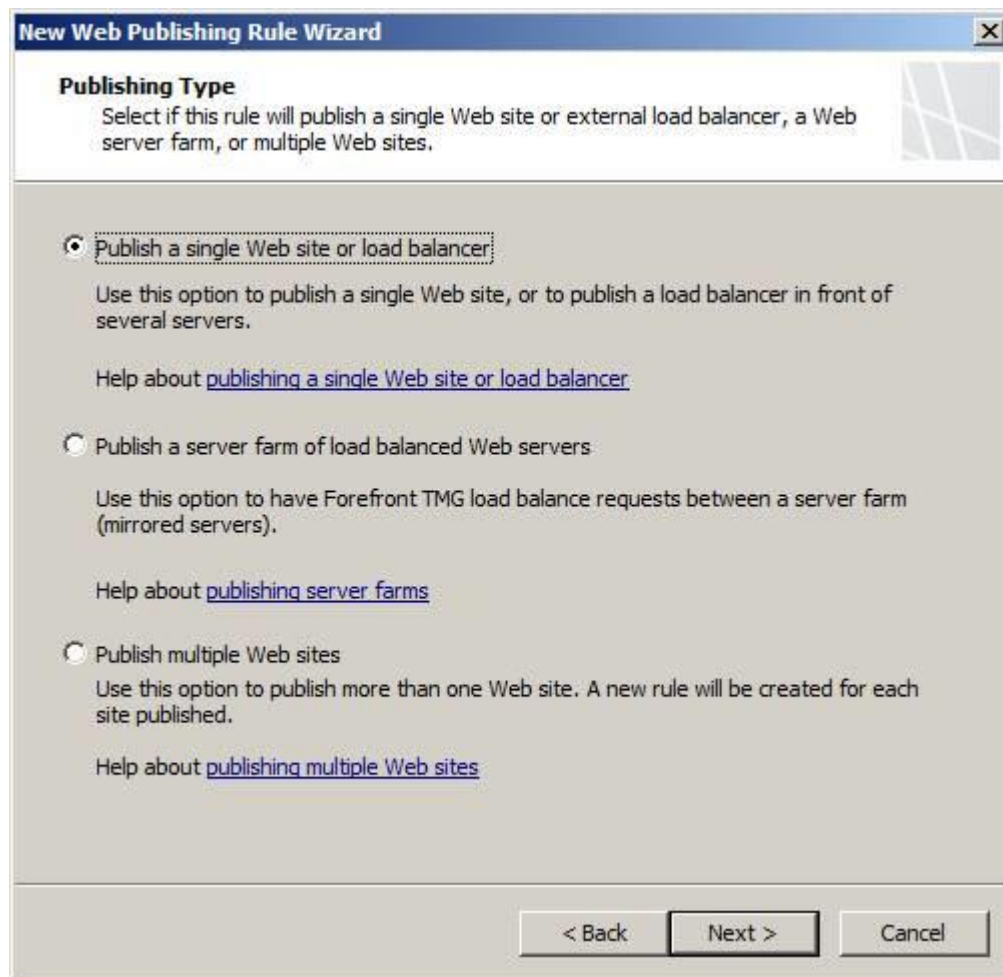
Trong trang **Select Rule Action**, như thể hiện trong hình 4, bạn có thể cấu hình rule là Allow hoặc Deny cho kết nối. Trong ví dụ này, chúng ta sẽ chọn **Allow**. Tùy chọn Deny được sử dụng cho các trường hợp sử dụng đặc biệt; bạn cũng có thể tạo các rule web publishing để cho phép các kết nối đến một website nào đó nằm phía sau tường lửa TMG.





Hình 4

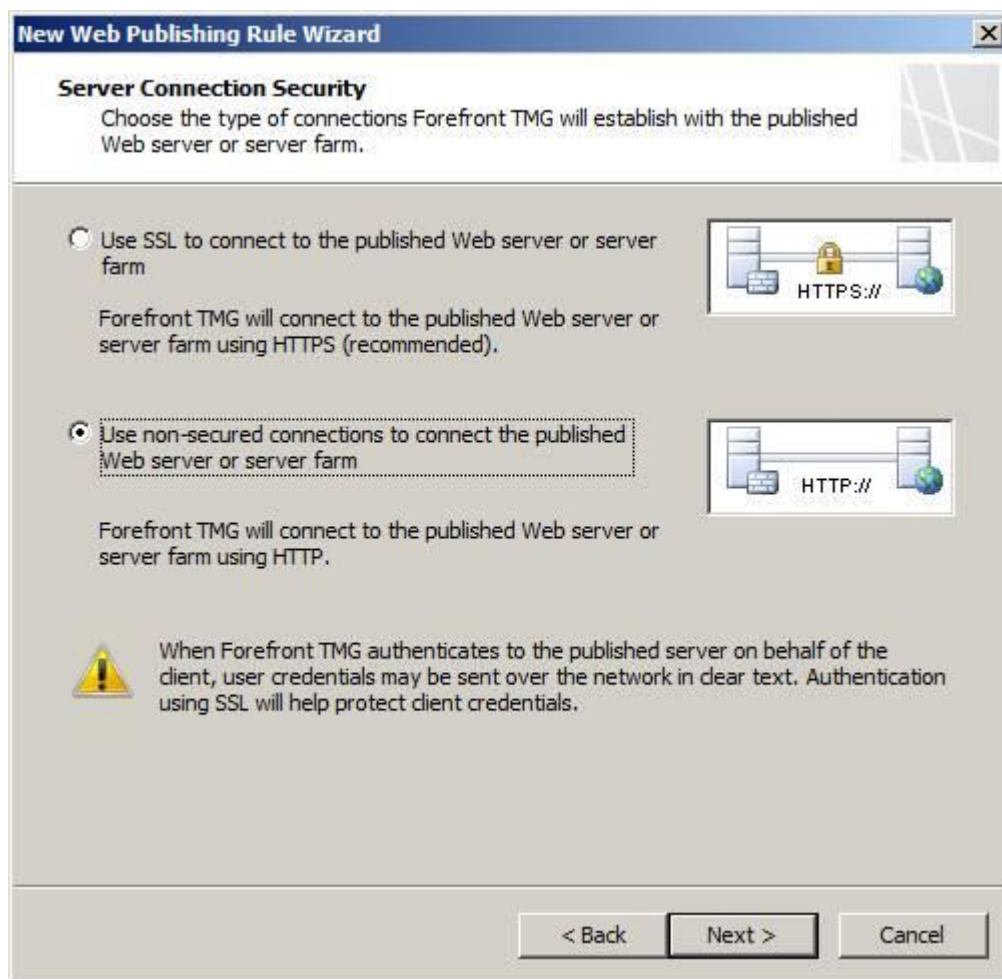
Trong trang **Publishing Type**, như thể hiện trong hình 5, bạn chọn một trong số ba kịch bản tương ứng với môi trường máy chủ web của mình. Trong ví dụ này, do muốn publish một web server nằm phía sau tường lửa TMG, vì vậy chúng ta chọn tùy chọn **Publishing a single Web site or load balancer** và kích **Next**.



Hình 5

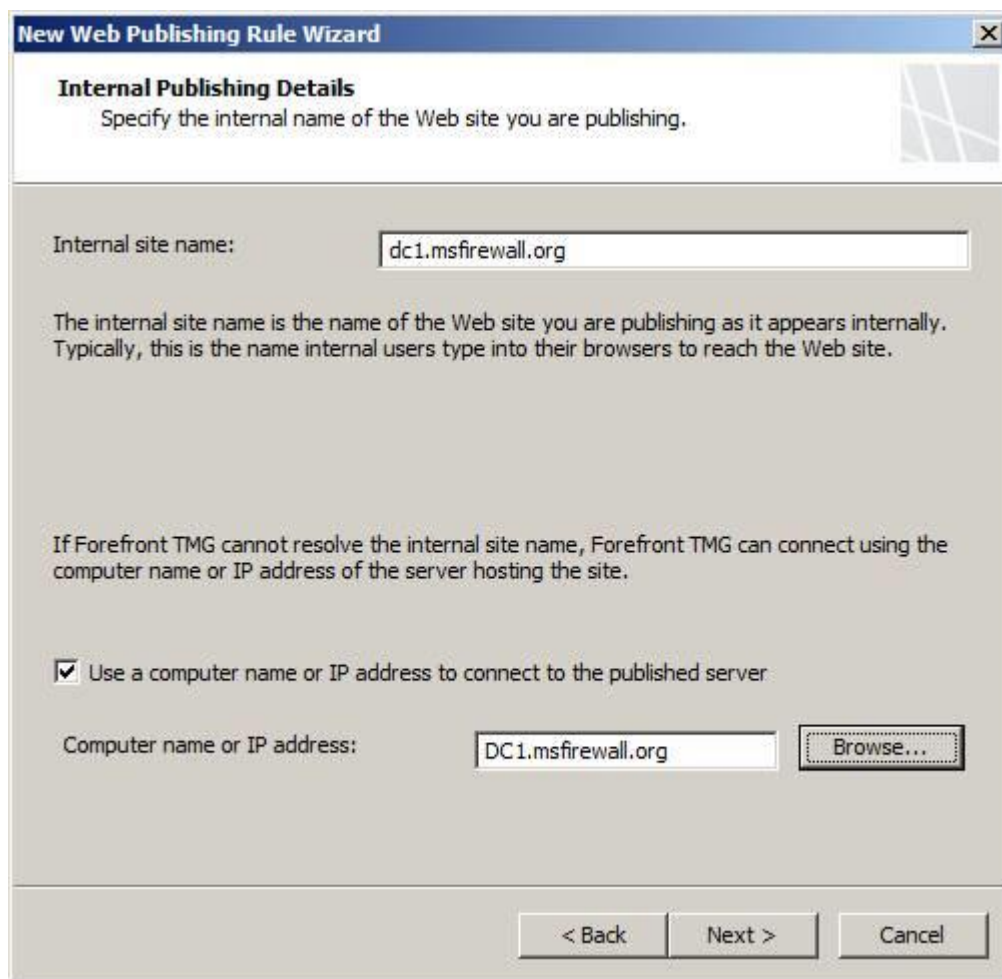
Trong trang **Server Connection Security**, thể hiện trong hình 6, bạn phải chọn xem tường lửa TMG có cần sử dụng SSL để kết nối với máy chủ web hay không. Trong kịch bản này, chúng ta không yêu cầu SSL giữa tường lửa TMG và máy chủ web, vì vậy hãy chọn tùy chọn **Use non-secured connections to connect the published Web server or server farm**.

Cần nhớ rằng để kết nối an toàn nhất, bạn nên sử dụng SSL.



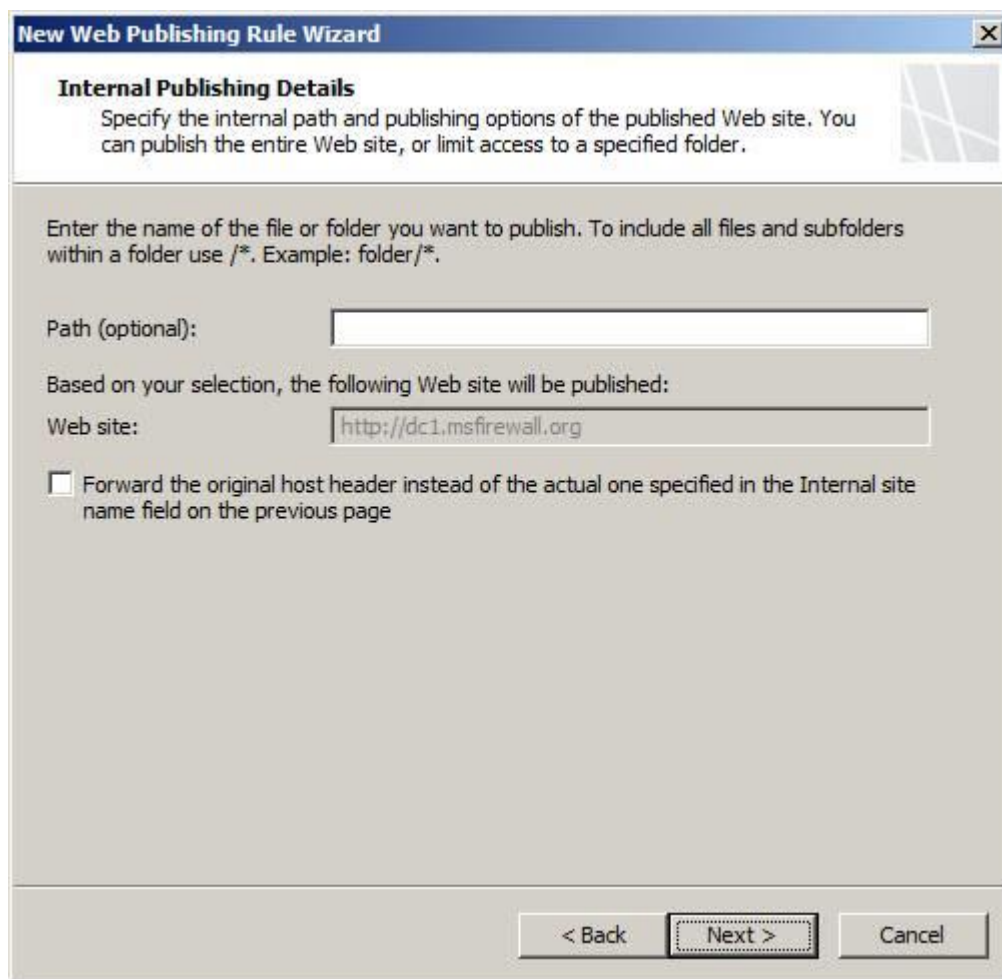
Hình 6

Trong trang **Internal Publishing Details**, hiển thị trong hình 7, bạn sẽ được yêu cầu định nghĩa tên máy chủ trong mạng nội bộ. Trong ví dụ này, chúng ta nhập vào Fully Qualified Domain Name (FQDN) của máy chủ trong mạng nội bộ đang hosting website, đó là **dc1.msfirewall.org**. Bạn cũng có tùy chọn kích hoạt hộp kiểm **Use a computer name or IP address to connect to the published server**, sau đó nhập vào tên hoặc địa chỉ IP khác của máy chủ. Tùy chọn này cho phép tường lửa TMG tìm máy chủ nếu nó đang sử dụng một tên khác không giống tên bạn nhập trong hộp *Internal site name*. Sau khi nhập vào các thông tin này, kích **Next**.



Hình 7

Trong trang **Internal Publishing Details**, hiển thị trong hình 8, bạn có thể nhập vào đường dẫn để hạn chế người dùng truy cập vào một file hoặc thư mục nào đó trên máy chủ web. Trong ví dụ này, do muốn cho phép truy cập toàn bộ site nên chúng ta không nhập đường dẫn nào ở đây. Sau khi thực hiện xong các lựa chọn ở đây, kích **Next**.



The screenshot shows a Windows XP-style dialog box titled "New Web Publishing Rule Wizard". The "Internal Publishing Details" tab is selected. The text inside says: "Specify the internal path and publishing options of the published Web site. You can publish the entire Web site, or limit access to a specified folder." Below this, there is a text box for "Path (optional):" which is empty. Another text box for "Web site:" contains the text "http://dc1.msfirewall.org". A checkbox labeled "Forward the original host header instead of the actual one specified in the Internal site name field on the previous page" is unchecked. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Hình 8

Trên trang **Public Name Details**, hình 9, nhập vào tên của website mà người dùng sẽ truy cập. Đây là tên mà người dùng sử dụng để truy cập site. Để thực hiện điều này, chọn tùy chọn **This domain name (type below)** từ danh sách sổ xuống *Accept requests for*. Sau khi chọn tùy chọn đó, nhập vào tên mà người dùng sẽ truy cập site trong hộp văn bản *Public name*. Trong ví dụ này, người dùng sẽ sử dụng tên **www.msfirewall.org** để truy cập site, vì vậy chúng ta sẽ nhập tên đó vào hộp văn bản. Tiếp nữa, chúng ta sẽ có tùy chọn nhập vào đường dẫn, tuy nhiên chúng ta không thực hiện công việc đó mà hãy kích **Next**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

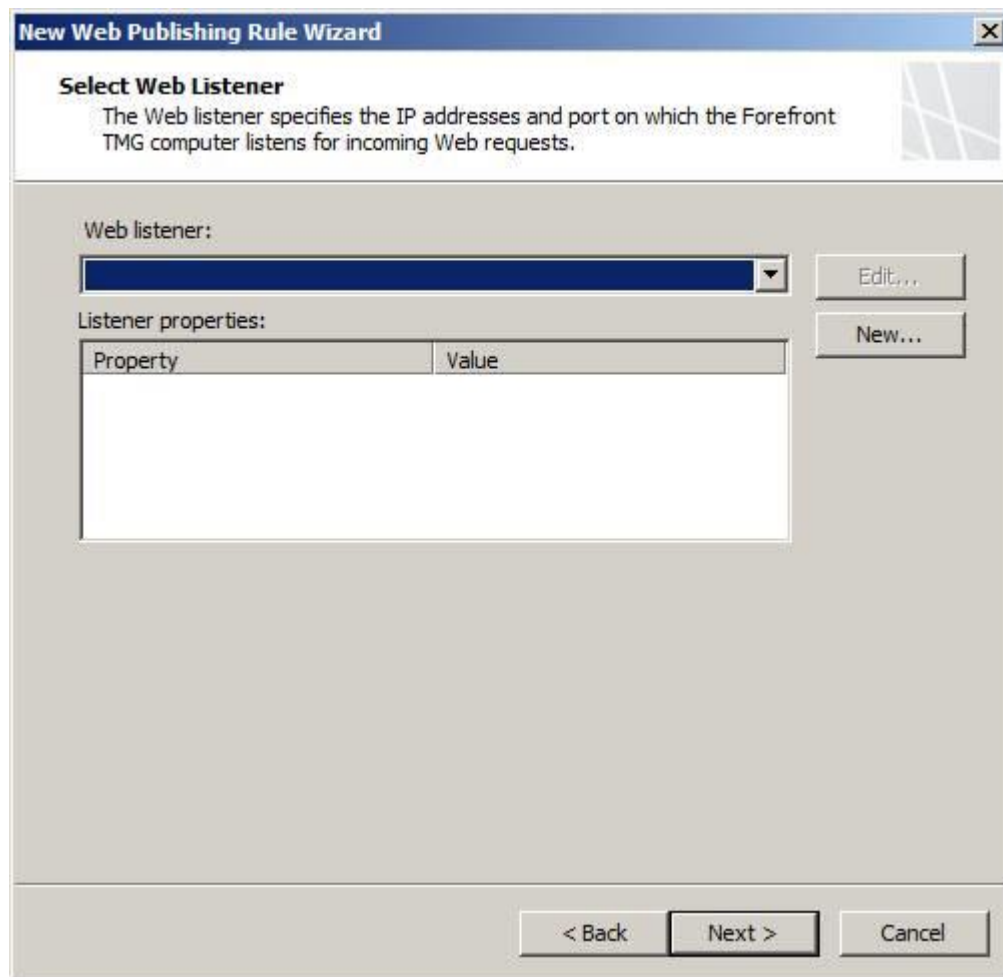
The screenshot shows the 'New Web Publishing Rule Wizard' dialog box, specifically the 'Public Name Details' step. The title bar reads 'New Web Publishing Rule Wizard'. Below the title bar, the section 'Public Name Details' is followed by the instruction: 'Specify the public domain name (FQDN) or IP address users will type to reach the published site.' The main area contains several input fields: 'Accept requests for:' with a dropdown menu showing 'This domain name (type below):'; 'Public name:' with a text box containing 'www.msfirewall.org' and an example 'Example: www.contoso.com'; 'Path (optional):' with an empty text box; and 'Site:' with a text box containing 'http://www.msfirewall.org/'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Hình 9

Trong trang **Select Web Listener**, hình 10, chọn bộ lắng nghe web listener sẽ được sử dụng để chấp nhận các kết nối từ người dùng bên ngoài để truy cập vào website. Trong ví dụ của chúng tôi, chưa có bộ lắng nghe nào được thiết lập, vì vậy không có lựa chọn nào trong hộp chọn sổ xuống. Để tạo một bộ lắng nghe HTTP web listener mới, kích nút **New**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

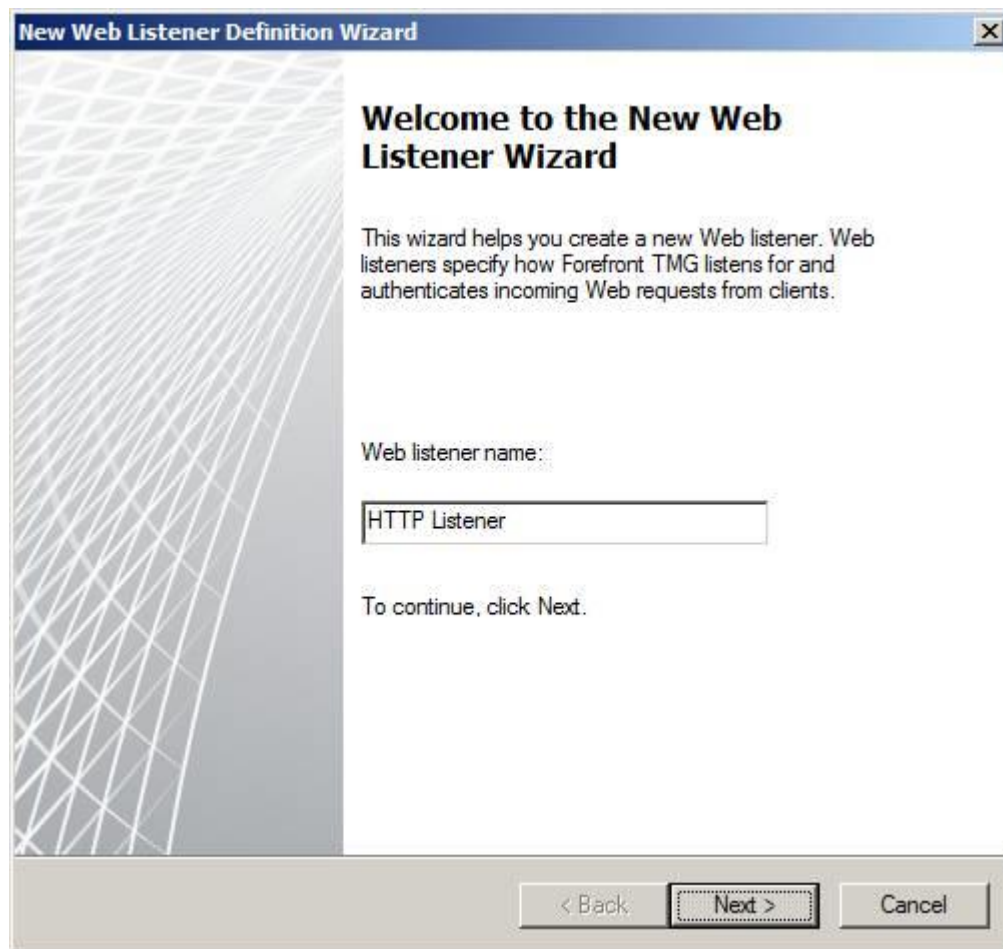




Hình 10

Thao tác này sẽ làm xuất hiện trang *Welcome to the New Web Listener Wizard*, hình 11. Ở đây chúng ta nhập tên cho bộ lắng nghe web listener trong hộp văn bản *Web listener name* (chúng ta sẽ sử dụng tên **HTTP Listener**) và sau đó kích **Next**.

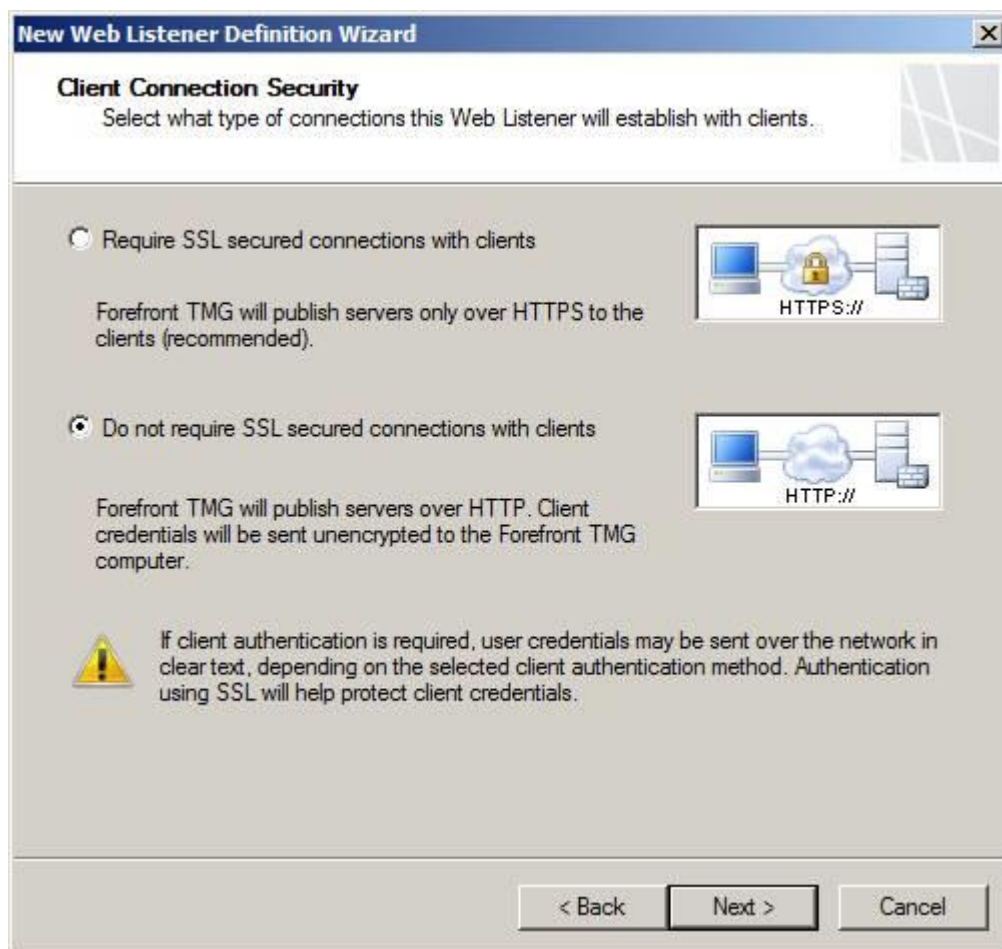
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 11

Trong trang *Client Connection Security*, hình 2, bạn phải chỉ định muốn hay không muốn sử dụng SSL để kết nối với tường lửa TMG. Trong ví dụ này, chúng ta muốn publish một site HTTP đơn giản, do đó hãy chọn **Do not require SSL secured connection with clients** và kích **Next**.

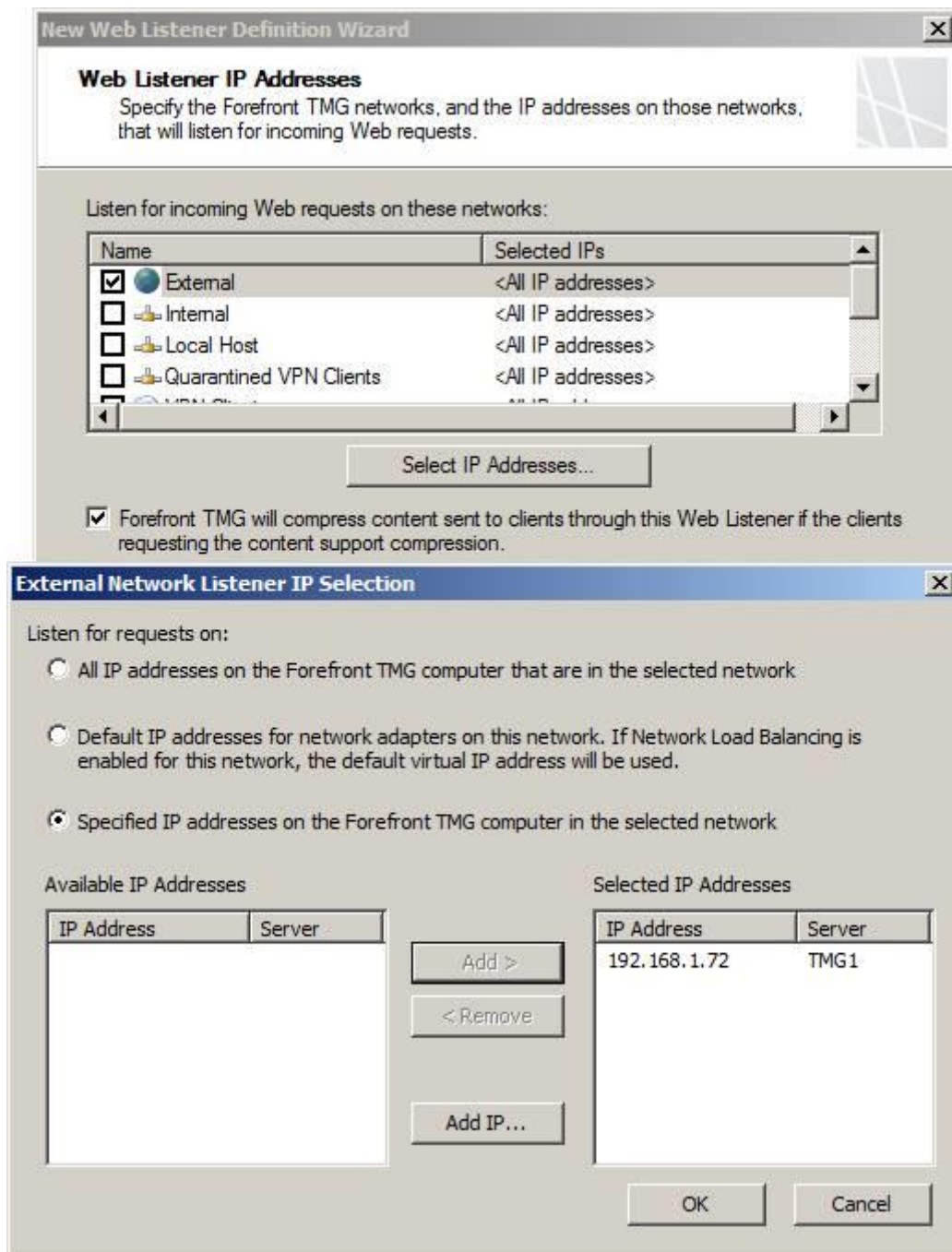
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 12

Trong trang *Web Listener IP Addresses*, hình 13, chọn mạng mà bạn muốn tường lửa TMG chấp nhận các kết nối đến website. Trong hầu hết các trường hợp, khi publish một website cho người dùng bên ngoài, bạn nên chọn mạng **External** mặc định để chấp nhận các kết nối gửi đến. Nếu bạn có nhiều địa chỉ IP được ràng buộc với giao diện ngoài, bạn có thể kích **Select IP Addresses** và sau đó chọn địa chỉ IP cụ thể mà bạn muốn chấp nhận các kết nối; trong hầu hết các trường hợp, bạn nên thực hiện điều này thay vì chấp nhận các kết nối trên tất cả địa chỉ IP có thể được cấu hình trên giao diện ngoài của tường lửa TMG. Trong ví dụ này, chúng ta chỉ có một địa chỉ IP trên giao diện ngoài, tuy nhiên chúng ta sẽ chọn một địa chỉ IP cụ thể đó trong trường hợp cần add thêm nhiều địa chỉ IP vào giao diện ngoài trong tương lai.

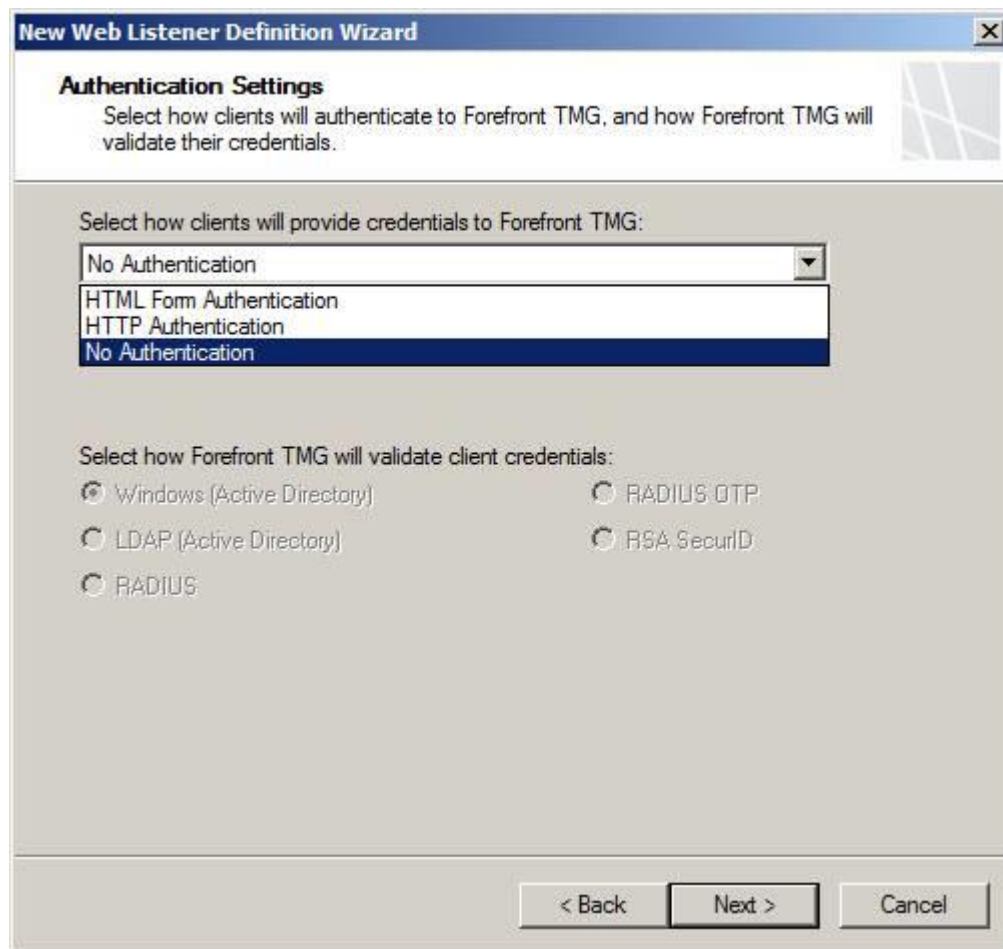
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 13

Trong trang **Authentication Settings**, hình 4, chọn kiểu thông tin sẽ được sử dụng để kết nối tới tường lửa TMG nhằm truy cập site. Kiểu nhận thực này thường được gọi là tiền nhận thực vì người dùng nhận thực với tường lửa TMG trước khi nhận thực với máy chủ web. Trong ví dụ này, chúng ta không yêu cầu nhận thực vì vậy hãy chọn tùy chọn **No Authentication** và kích **Next**.

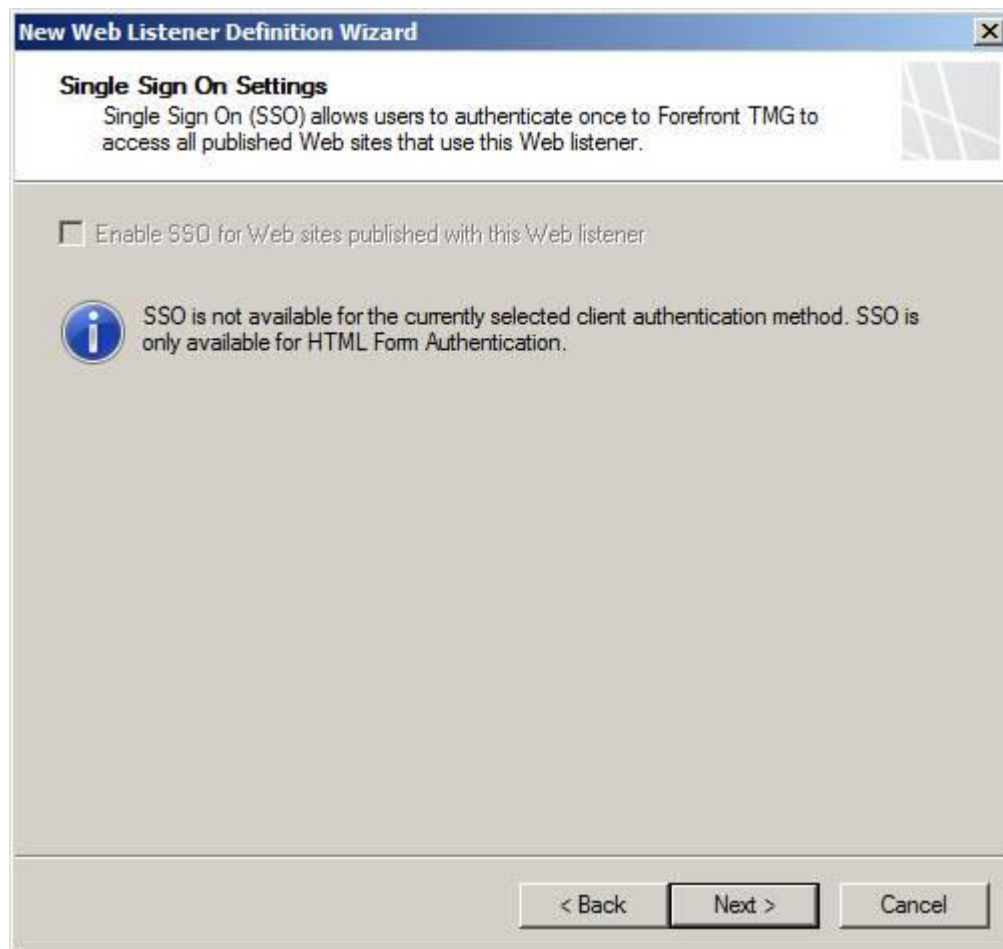
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 14

Trong trang *Single Sign On Settings*, hình 15, bạn có thể cấu hình bộ lắng nghe web listener để hỗ trợ cơ chế đăng nhập một lần (single sign-on) cho tất cả các site được publish qua bộ lắng nghe này. Mặc dù vậy, để cơ chế đăng nhập một lần làm việc, người dùng phải đăng nhập. Do chúng ta không yêu cầu nhận thực trong ví dụ này do đó cơ chế đăng nhập là không cần thiết, vậy hãy chuyển sang phần tiếp theo bằng cách kích **Next**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

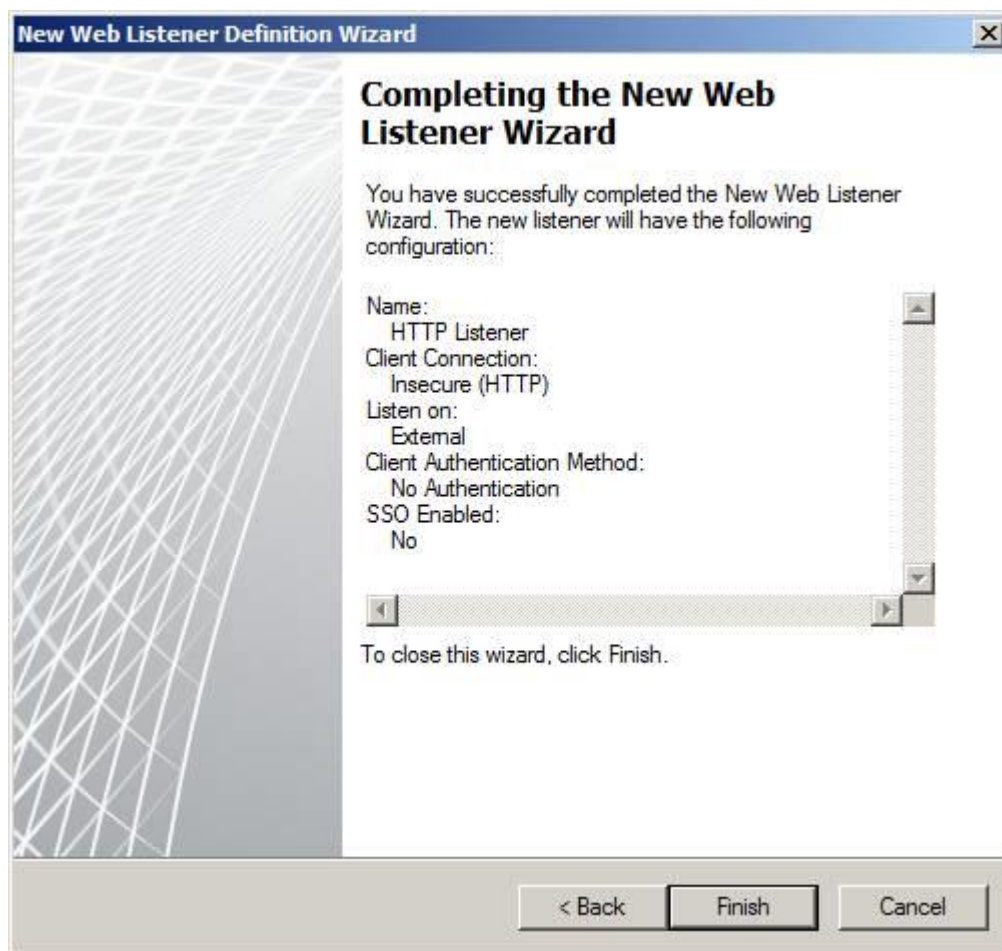


Hình 15

Sau khi kích **Next** bạn sẽ thấy xuất hiện trong cuối cùng của web listener wizard, hình 16. Ở đây chúng ta sẽ xem xét lại các thiết lập trên trang *Completing the New Web Listener Wizard* và kích **Finish**.

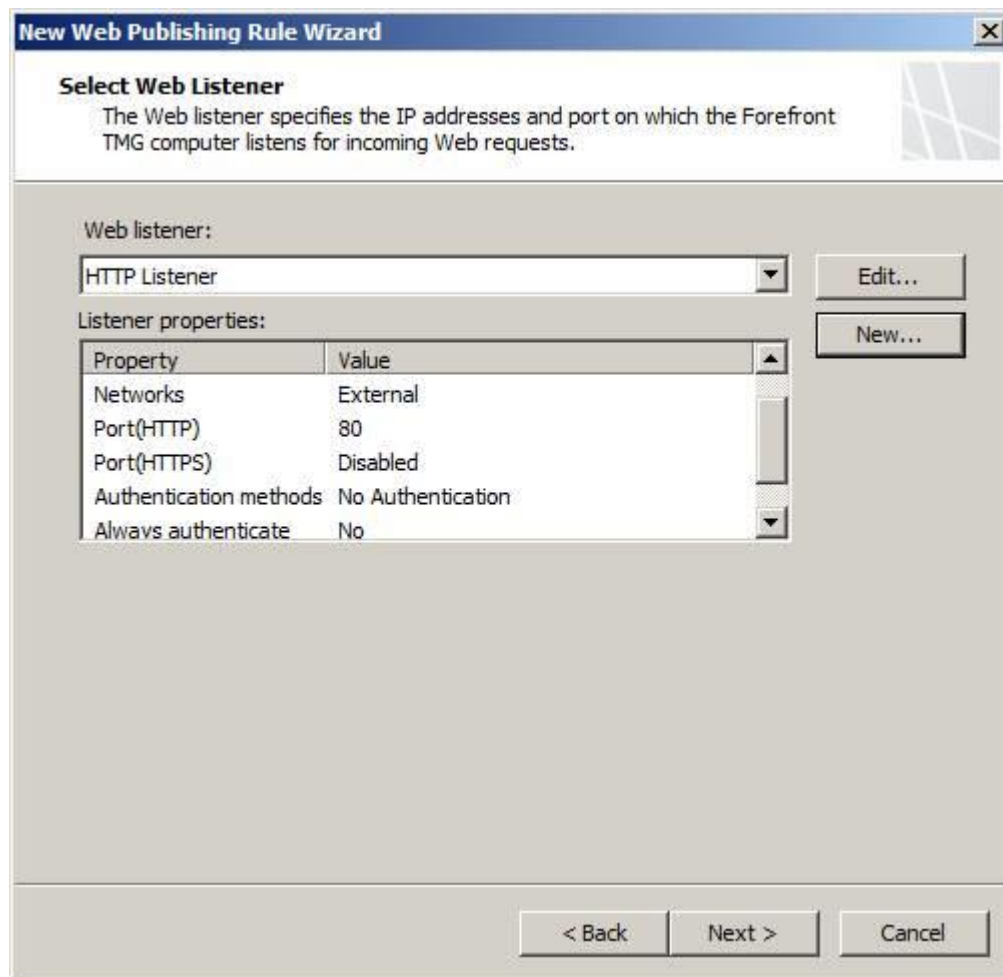
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..





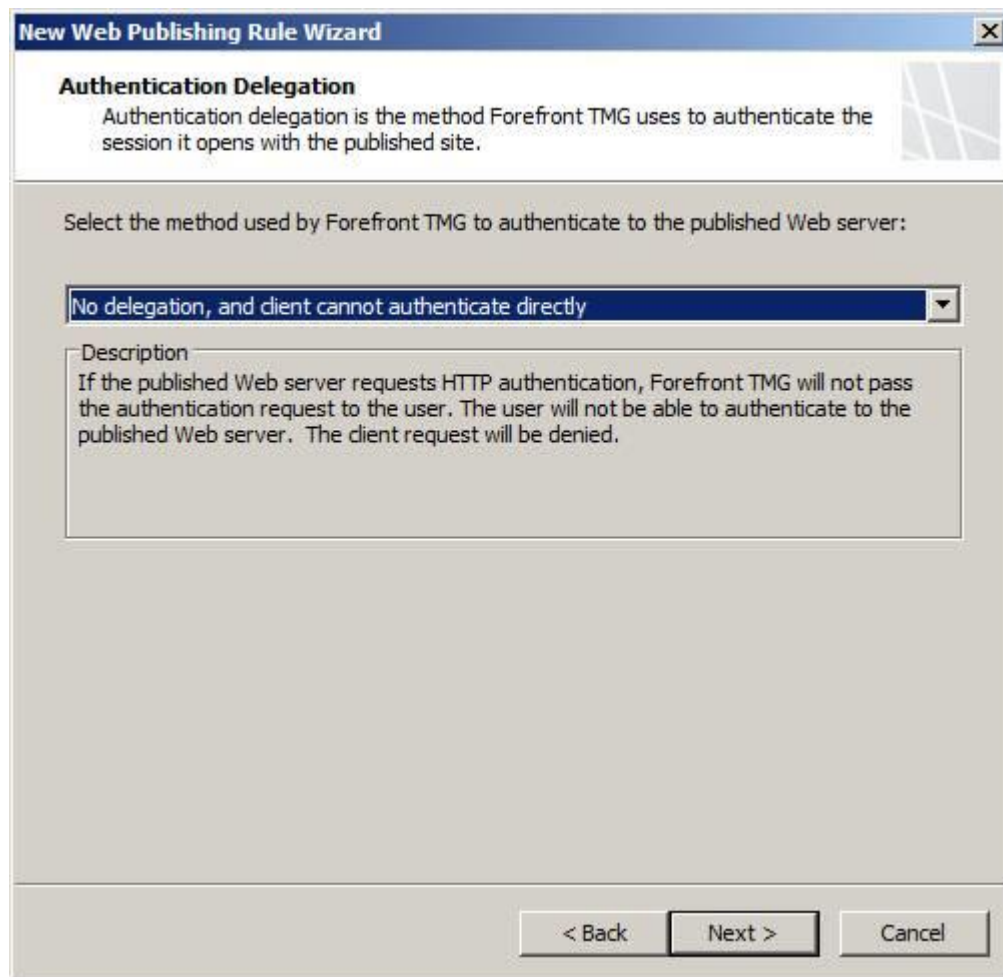
Hình 16

Giờ đây chúng ta hãy quay trở về wizard gốc. web listener mới lúc này sẽ xuất hiện trong trang **Select Web Listener** như được thể hiện trong hình 17, ở đây bạn có thể thấy một số thông tin chi tiết về Web Listener. Có một số tùy chọn bổ sung để bạn có thể cấu hình trên web listener. Ngoài ra bạn có thể truy cập chúng bằng cách kích nút **Edit**. Chúng tôi sẽ giới thiệu về vấn đề này trong phần sau. Còn giờ đây, chúng ta hãy tiếp tục bằng cách kích **Next**.



Hình 17

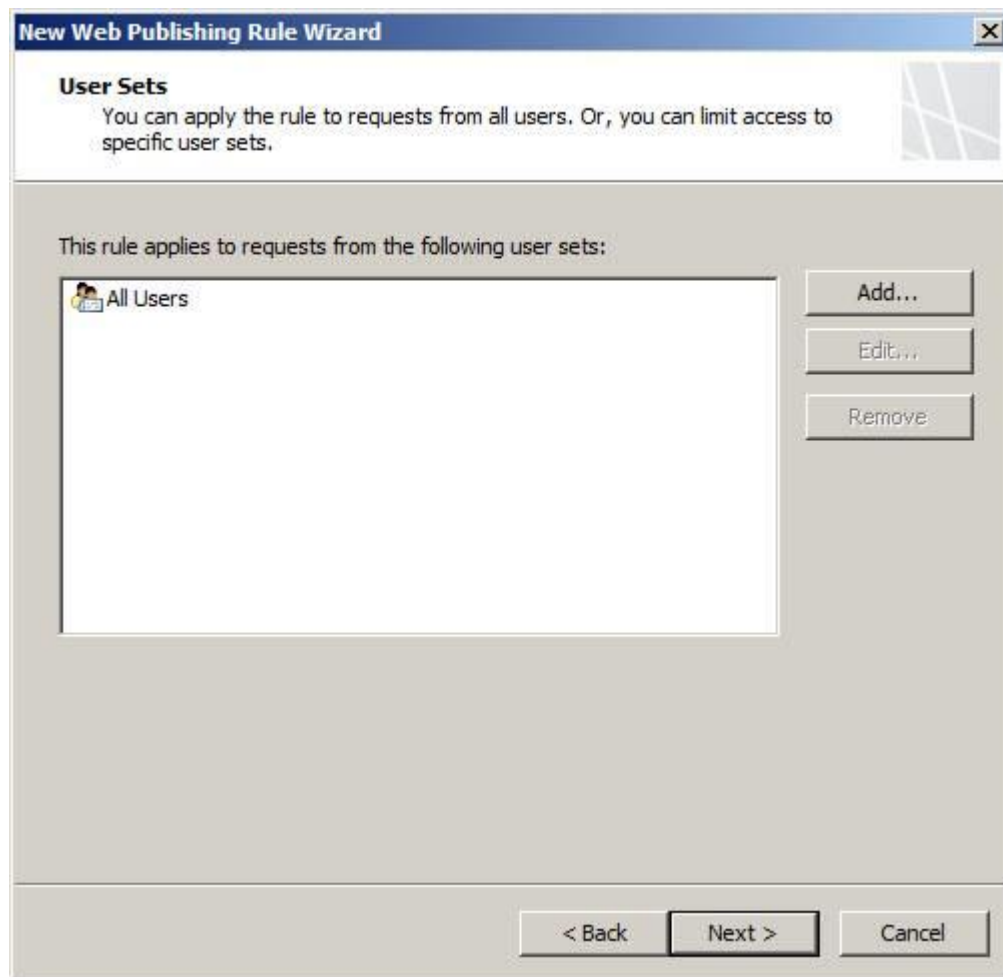
Trong trang **Authentication Delegation**, hình 18, bạn cấu hình cách TMG firewall ủy nhiệm chứng chỉ cho website đã được publish. Điều này có nghĩa người dùng sẽ chỉ cần nhận thực một lần với tường lửa TMG. Trong ví dụ này, chúng ta không yêu cầu nhận thực, do đó không có lý do gì để ủy nhiệm các tiêu chuẩn, chúng ta sẽ chọn tùy chọn **No delegation, and client cannot authenticate directly** và kích **Next**.



Hình 18

Trong trang **User Sets**, hình 19, chọn người dùng hoặc nhóm người dùng được phép truy cập vào website đã được publish. Để kích hoạt tùy chọn này, bạn phải yêu cầu người dùng nhận thực để họ sẽ được nhận dạng. Do không yêu cầu nhận thực trong ví dụ này nên chúng ta sẽ sử dụng nhóm mặc định, đó là **All Users**. Trong ngữ cảnh của TMG firewall, “all users” không có nghĩa là tất cả người dùng đã được nhận thực; nó có nghĩa là người dùng mặc danh – vì vậy khi cho phép truy cập “all users”, bạn đang cho phép người dùng không nhận thực có thể truy cập site.

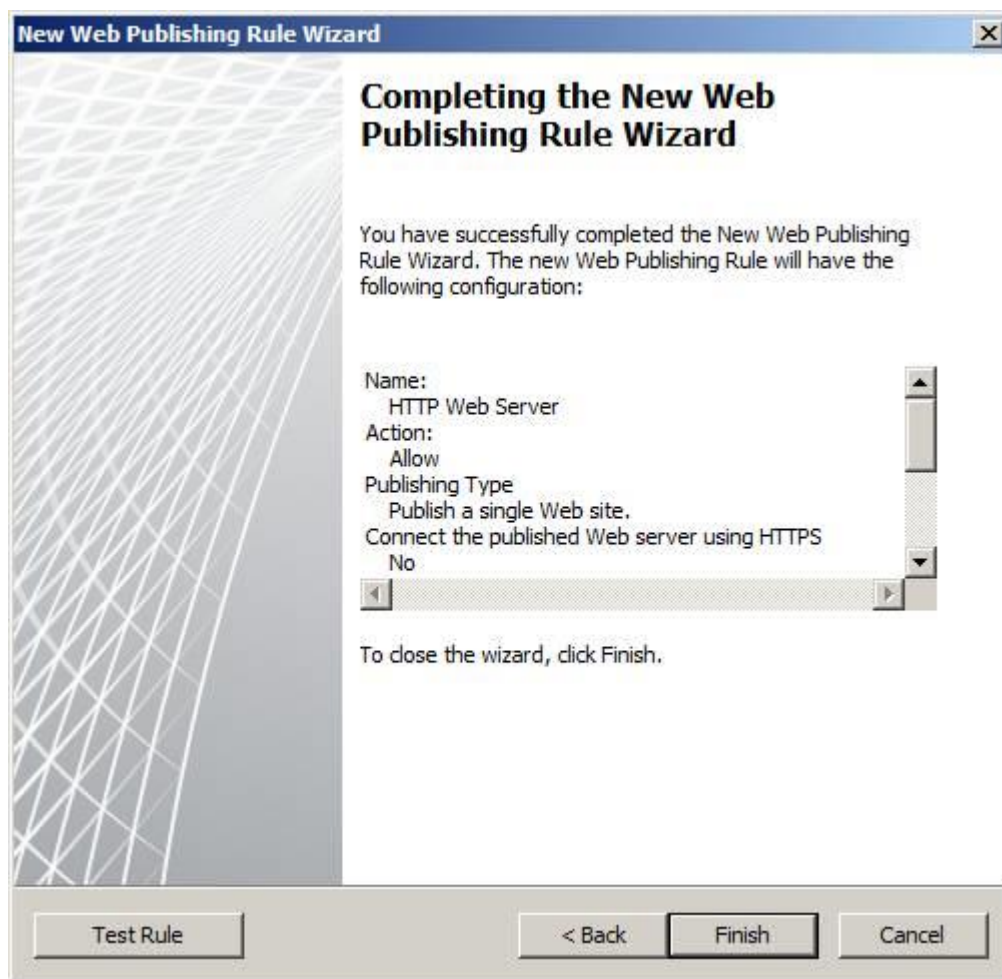
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 19

Chúng ta sẽ đánh giá lại các thiết lập trong trang *Completing the New Web Publishing Rule Wizard* như được hiển thị trong hình 20, sau đó kích nút **Test Rule**.

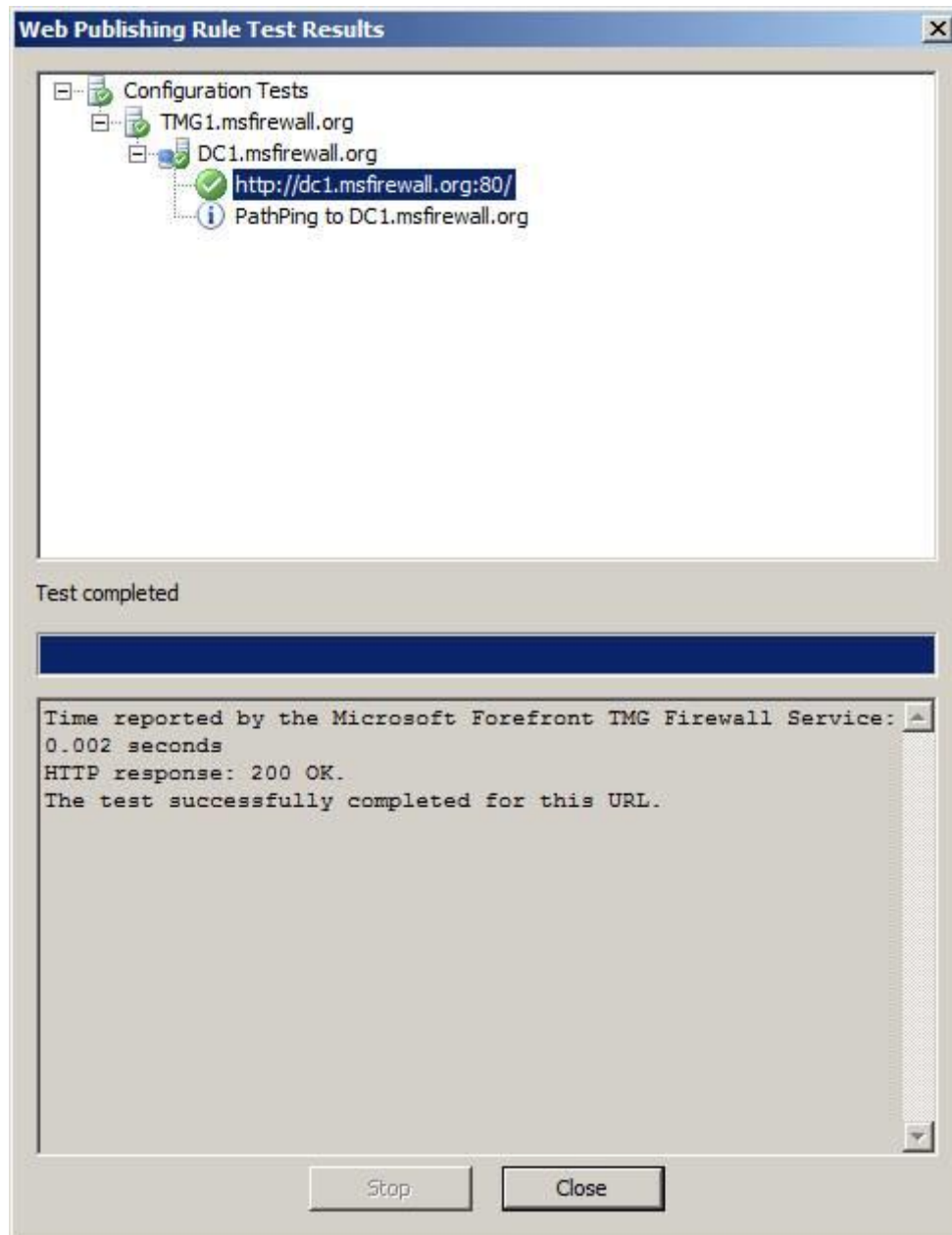
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 20

Nút **Test Rule** cho phép bạn thấy liệu website có thể truy cập từ TMG firewall hay không. Như những gì bạn có thể thấy trong hình 21 bên dưới, khi kích nút Test Rule, TMG sẽ cố gắng kết nối với máy chủ web bằng kết nối HTTP và nó thực hiện hành động ping đường dẫn (PathPing) đến máy chủ web. Như những gì trong hình, tường lửa TMG đã có thể kết nối đến máy chủ web và PathPing đã diễn ra thành công.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 21

Lúc này bạn có thể thấy rule mới trong danh sách các rule tường lửa. Để kích hoạt rule, bạn phải kích nút **Apply**, như thể hiện trong hình 22 bên dưới.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

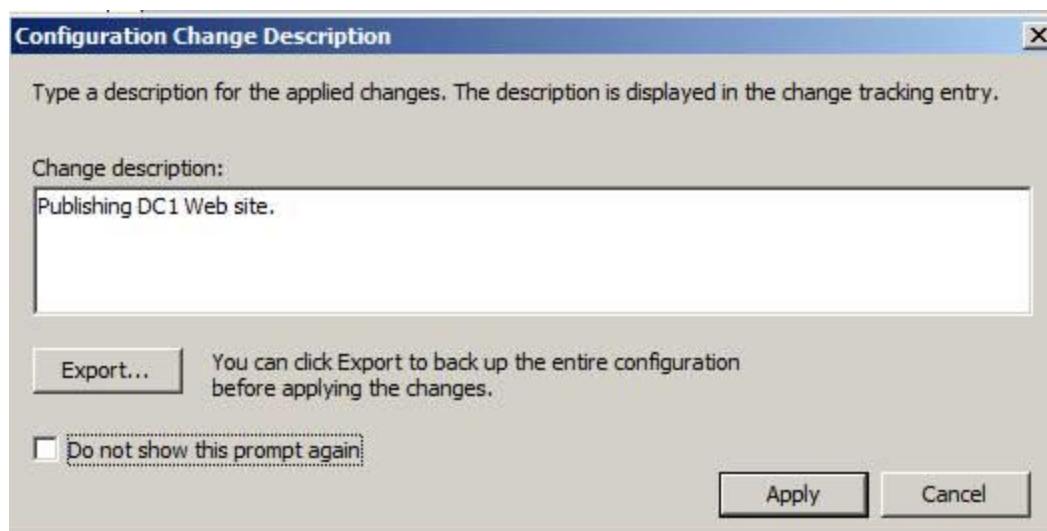


[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 22

Hộp thoại *Configuration Change Description*, như thể hiện trong hình 23, bạn có thể nhập vào bình luận về thay đổi mà mình đã thực hiện trong chính sách tường lửa. Tường lửa TMG sẽ lưu các thông tin này để bạn có thể sử dụng nó như một phần của hệ thống quản lý thay đổi, mục đích hỗ trợ cho việc khắc phục sự cố sau này. Sử dụng hộp thoại này, bạn cũng có thể export cấu hình tường lửa để có thể khôi phục cấu hình về điểm trước khi thực hiện thay đổi. Kích **Apply** để lưu các thay đổi.



Hình 23

Cấu hình lúc này sẽ được lưu và bạn có thể thấy các kết quả trong hộp thoại **Saving Configuration Changes**, hình 24. Lưu ý rằng các kết nối khách đang tồn tại sẽ được đánh giá lại theo chính sách mới. Đây là điểm mới đối với tường lửa TMG – với tường lửa ISA, chính sách tường lửa chỉ được áp với các kết nối mới.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 24

## Kết luận

[Key4VIP.info](http://www.Key4VIP.info)

Trong phần này, chúng tôi đã giới thiệu cho các bạn một số cơ bản của việc web publishing với TMG. Trong phần, chúng ta đã tạo một web publishing rule, một bộ lắng nghe HTTP web listener đơn giản. Cuối phần tạo rule, chúng ta đã sử dụng nút test để xác định xem website có khả năng reachable hay không. Trong phần tiếp theo của loạt bài này, chúng ta sẽ tạo một SSL web site có yêu cầu nhận thực. Trong phần đó, bạn sẽ biết một số tùy chọn nâng cao khi tạo các web publishing rule.

**Trong phần tiếp theo của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn một số khái niệm được sử dụng trong mạng có tường lửa TMG firewall - TMG firewall Network và TMG firewall Network Rule.**

Trong loạt bài giới thiệu những vấn đề cơ bản của tường lửa TMG, chúng tôi đã giới thiệu cho các bạn về các rule truy cập và các rule cho web publishing. Trong phần tiếp theo này chúng tôi sẽ giới thiệu cho các bạn về các mạng TMG và các rule mạng. Tường lửa TMG chắc chắn là một trong những tường lửa trực quan hơn. Bạn không cần phải nhớ các câu lệnh mà thay vào đó là sử dụng giao diện người dùng có thiết kế khá chuyên nghiệp.

## Tạo một TMG Firewall Network

Mô hình kết nối mạng có tường lửa TMG dựa trên khái niệm TMG firewall “Network”, với chữ N viết hoa. Một TMG firewall Network là một bộ sưu tập các địa chỉ IPv4 không thuộc về bất cứ TMG

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

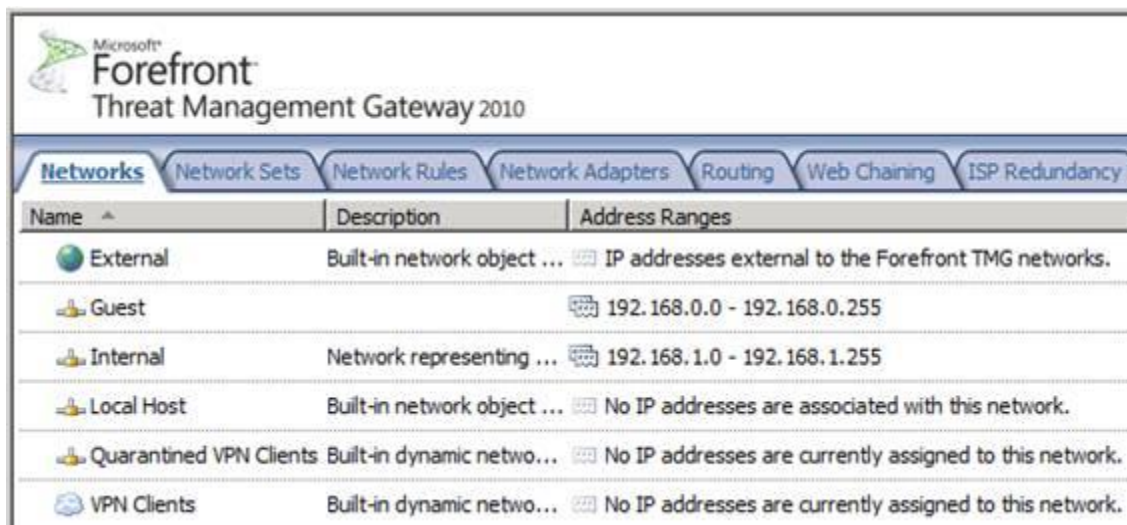
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

firewall Network nào khác. NIC kết nối chính tường lửa TMG với các địa chỉ IP đó được coi là “root” của TMG firewall Network.

Giả sử rằng bạn có một TMG firewall có hai NIC. Một giao diện được kết nối với Internet và đó là giao diện External mặc định, nó được kết nối với External Network mặc định. Một NIC khác được kết nối với một mạng subnet khác, đó là Internal Network mặc định. Nếu subnet nằm trong dải 10.0.0.0.-10.0.0.255 thì mạng Internal Network mặc định của bạn được định nghĩa bằng các địa chỉ đó và NIC kết nối với subnet đó là “root” của Internal Network mặc định.

Trong hình 1 bên dưới, bạn có thể thấy tab **Networks** trong nút **Network** ở panel bên trái của giao diện TMG firewall. Có 5 mạng TMG firewall mặc định ở đây:

- **External.** Mạng External Network mặc định gồm có tất cả các địa chỉ IP không nằm trong mạng TMG firewall khác.
- **Internal.** Mạng Internal Network mặc định được định nghĩa khi bạn cài đặt tường lửa. Internal Network mặc định điển hình là một mạng gồm có các bộ điều khiển miền (domain controller) hoặc máy chủ DNS mà tường lửa TMG cần để thực hiện các hoạt động cơ bản.
- **Local Host.** Local Host Network được định nghĩa bởi các địa chỉ IP ràng buộc với tất cả giao diện mạng trên các NIC của tường lửa TMG.
- **Quarantined VPN Clients.** Quarantined VPN Clients Network là một mạng được tạo động, gồm có tất cả các địa chỉ IP của máy khách VPN hiện đang được cách ly.
- **VPN Clients.** VPN Clients Network là một mạng được tạo động khác gồm có các địa chỉ IP của tất cả các máy khách VPN hiện không được cách ly.



Hình 1

Nếu muốn có nhiều hơn hai NIC trong một tường lửa TMG, bạn cần phải tạo các mạng mới để hỗ trợ các NIC này.

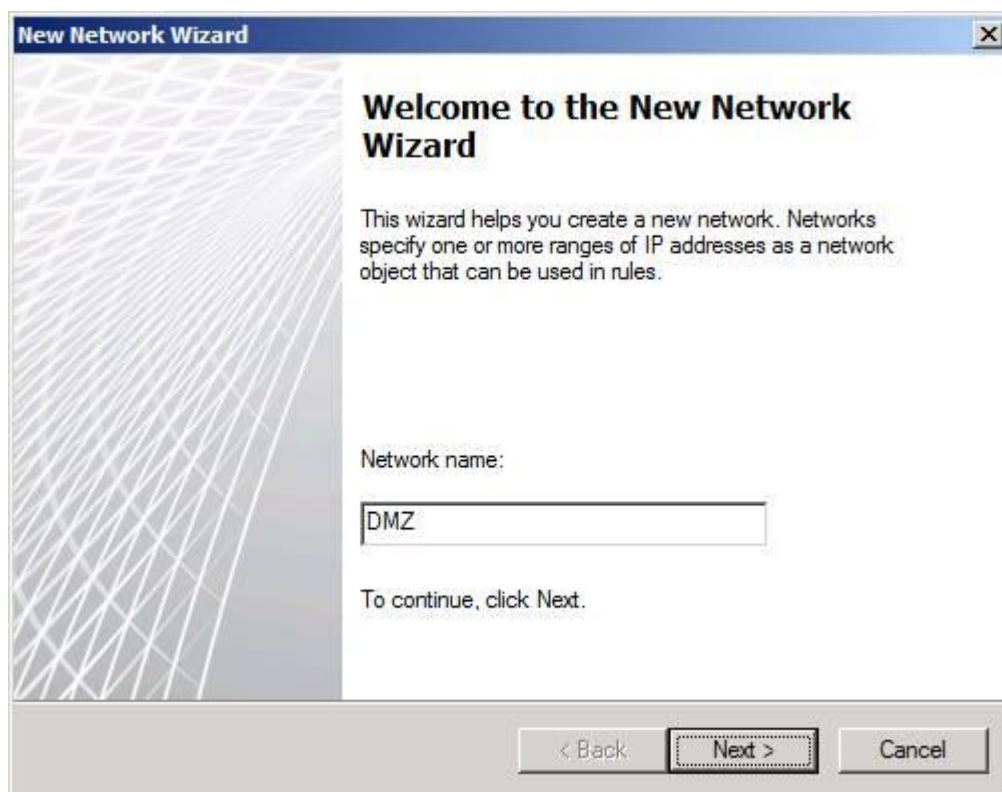
**Lưu ý:**

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

Bạn có thể có thêm nhiều NIC trên cùng một mạng tường lửa TMG, tuy nhiên chúng ta sẽ không đề cập đến kịch bản đó trong bài này.

Để tạo một mạng tường lửa TMG mới, hãy kích liên kết **Create a New Network** trong phần panel bên phải của giao diện điều khiển. Thao tác này sẽ làm xuất hiện **Welcome to the New Network Wizard**, xem thể hiện trong hình 2 bên dưới. Trong trang này, bạn cần phải gán tên cho mạng. Trong ví dụ trong bài, chúng tôi đã đặt tên cho mạng là **DMZ** và kích **Next**.



Hình 2

Trong trang **Network Type**, bạn phải chỉ cho wizard về kiểu mạng mà bạn muốn tạo. Đây là các lựa chọn mà bạn cần chọn:

- **Internal Network** – Internal Network là một mạng được bảo vệ bởi tường lửa TMG. Khi tạo một Internal Network, bạn sẽ có một số tùy chọn cấu hình cụ thể cho mạng đó, chẳng hạn như các thiết lập web proxy mà các máy khách trên mạng sử dụng. Chúng ta sẽ đề cập đến vấn đề này sau.
- **Perimeter Network** – Mạng Perimeter Network cũng tương tự như mạng Internal Network dưới dạng các tùy chọn có sẵn cho bạn sau khi mạng được hoàn tất. Trong thực tế, không có sự khác biệt trong thực hiện giữa Perimeter Network và Internal Network, chỉ định “kiểu” làm cho nó trở nên dễ dàng hơn trong việc phân biệt mạng nào mà bạn cho là mạng bên trong, mạng nào được xem là DMZ.

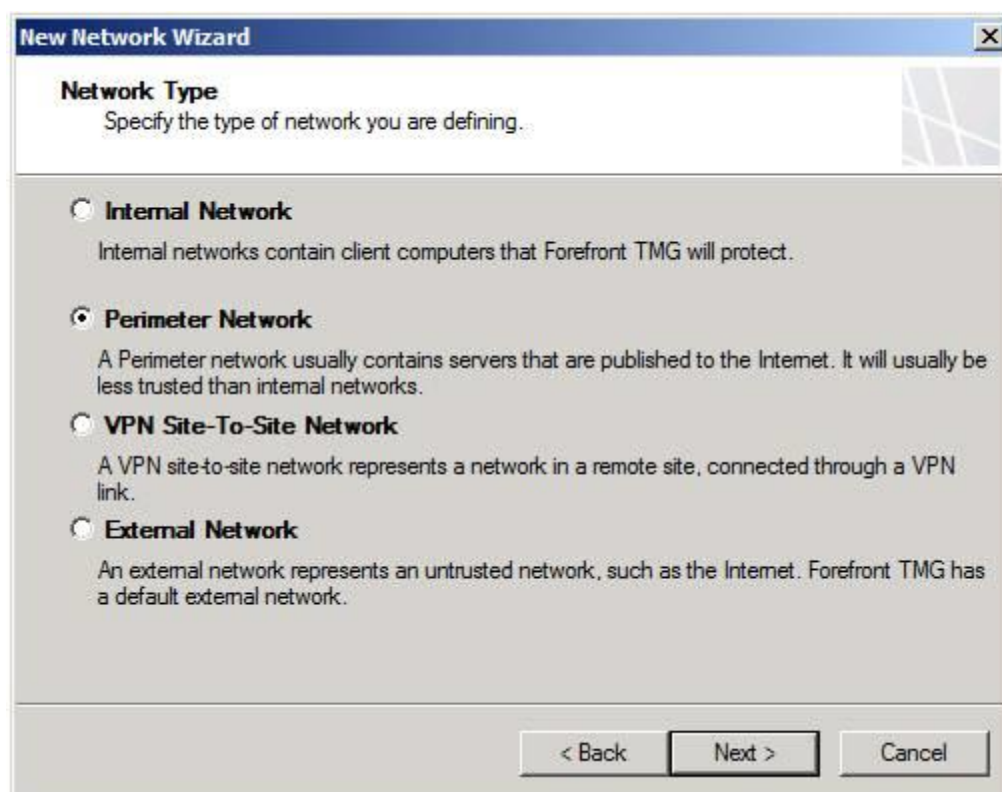
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

- **VPN Site-to-Site Network** – Đây là kiểu mạng đặc biệt mà TMG sử dụng để kết nối hai mạng với nhau qua Internet, sử dụng các router VPN.
- **External Network** – Mạng External Network là một mạng không có các tùy chọn có trong các mạng Internal và Perimeter, và không được coi như một mạng được bảo vệ bởi TMG; nó cho phép bạn kết nối với các tài nguyên bên ngoài tổ chức, tuy nhiên không thể *reach* (vớ tới) qua cổng mặc định trên mạng External Network mặc định.

Trong ví dụ này, chúng ta sẽ tạo một mạng DMZ vì vậy hãy chọn tùy chọn **Perimeter Network** như thể hiện trong hình 3 và kích **Next**.



Hình 3

Trong trang **Network Addresses**, bạn cần cấu hình các địa chỉ IP được sử dụng để định nghĩa mạng. Có nhiều địa chỉ có thể *reach* trực tiếp bởi NIC kết nối với mạng mà bạn đang tạo. Có ba cách có thể add địa chỉ để định nghĩa một mạng:

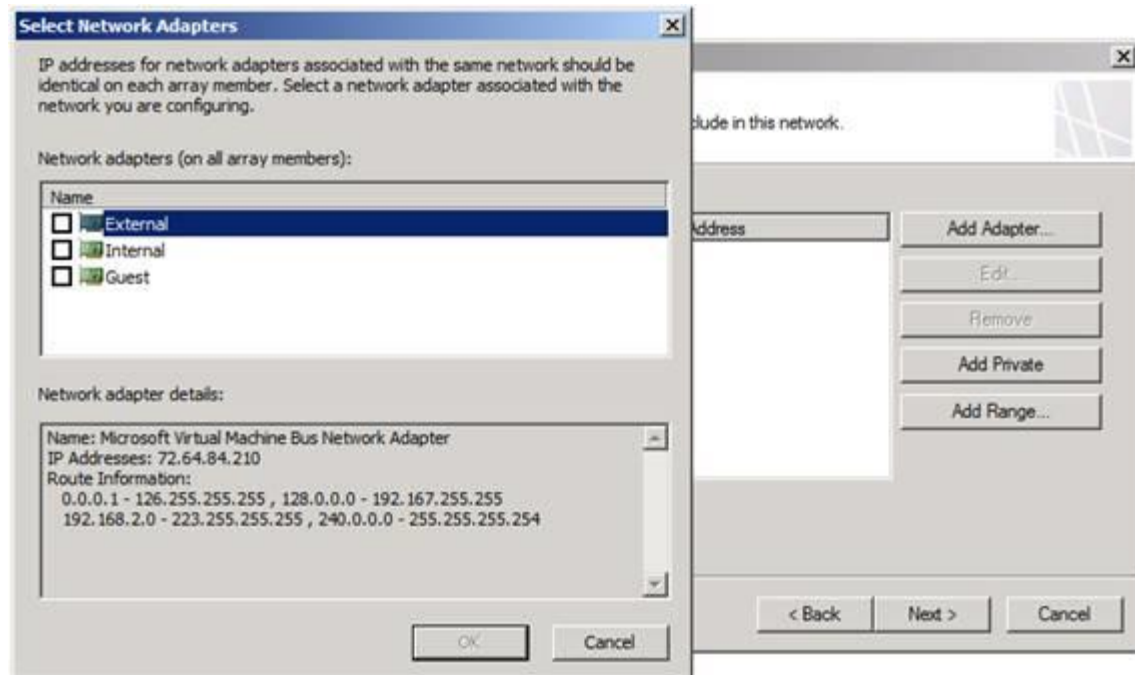
- **Add Adapter** – Đây là cách tốt nhất cho việc add địa chỉ. Nếu bạn cấu hình bảng định tuyến trên tường lửa TMG trước khi tạo mạng, tùy chọn này sẽ tự động bao hàm tất cả các địa chỉ có thể *reach* bởi NIC trên mạng mà bạn đang định nghĩa.
- **Add Private**. Tùy chọn này cho phép dễ dàng add một bộ các địa chỉ IP riêng để định nghĩa một mạng mới của bạn.
- **Add Range**. Tùy chọn này cho phép bạn chỉ định một dải địa chỉ IP nào đó để định nghĩa cho mạng của bạn. Bạn thường phải sử dụng tùy chọn này nếu chưa cấu hình bảng định tuyến trên

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

tường lửa TMG; trong trường hợp đó, tất cả địa chỉ có thể với trực tiếp bởi NIC đều không được bao hàm khi bạn sử dụng tùy chọn **Add Adapter**.

Trong ví dụ này, chúng ta sẽ chọn NIC (**Guest**) (chúng tôi đã đặt lại tên các NIC để dễ dàng phân biệt hơn) là root của mạng DMZ đang tạo. Xem thể hiện trong hình 4.



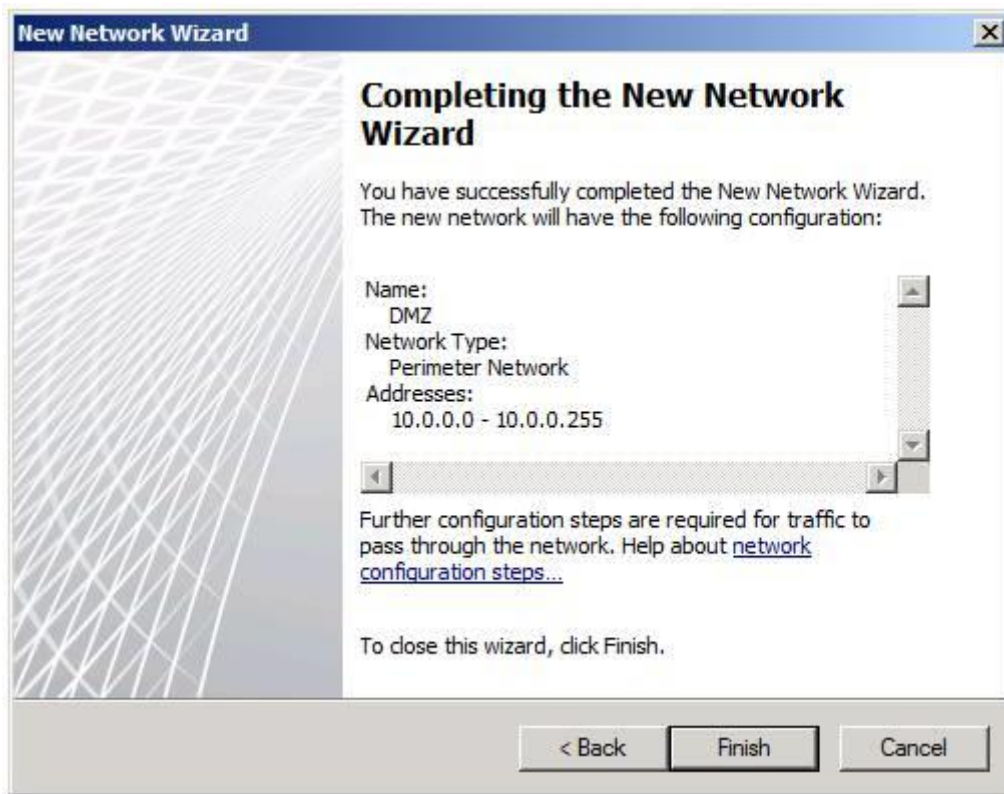
Hình 4

Xem lại các lựa chọn trên trang **Completing the New Network Wizard**, trang bạn có thể thấy trong hình 5 và kích **Finish**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Key4VIP.info Hình 5

Tại đây, mạng mới đã được tạo xong. Mặc dù vậy, không có nhiều thứ bạn thực hiện lúc này cho tới khi tạo một Network Rule.

### Tạo một TMG Firewall Network Rule

Mạng được kết nối với các mạng khác bằng các rule mạng (Network Rule). Nếu không có rule nào để kết nối một mạng với một mạng khác sẽ không có lưu lượng truyền tải giữa các mạng. Khi bạn kết nối một mạng với một mạng khác, bạn cần phải định nghĩa mối quan hệ tuyến giữa các mạng. Mối quan hệ tuyến có thể là NAT hoặc có thể là Route. Một mối quan hệ tuyến có nghĩa rằng các gói từ một mạng nguồn nào đó đến một mạng đích sẽ được định tuyến, giống như bất cứ một kết nối được định tuyến nào. Nếu bạn chọn quan hệ NAT, các kết nối từ mạng nguồn sẽ được NAT đến mạng đích, với địa chỉ IP chính trên NIC gần nhất với mạng đích thay cho địa chỉ IP nguồn gốc của host trên mạng nguồn.

Để tạo một rule mới, kích tab **Network Rules** trong nút **Networks** trong giao diện tường lửa. Sau đó kích liên kết **Create a Network Rule** trong panel phải của giao diện. Trang đầu tiên bạn thấy sẽ là **Welcome to the New Network Rule Wizard**, như những gì thể hiện trong hình 6 bên dưới. Đầu tiên bạn cần gán tên cho rule trong hộp thoại **Network rule name**. Trong ví dụ này chúng tôi đã đặt tên cho rule là **Internal to DMZ**, đây là rule sẽ kết nối mạng Internal Network mặc định với mạng DMZ Network mới. Kích **Next**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

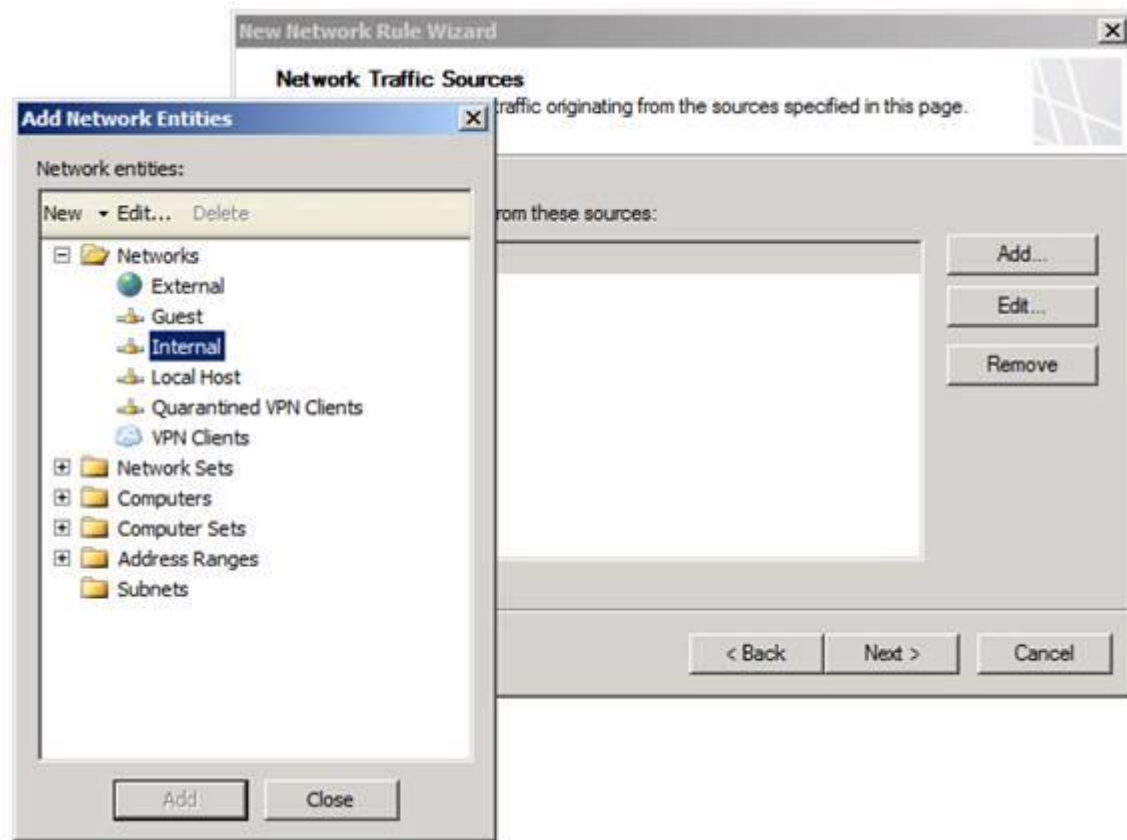
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Key4VIP.info

Trong hộp thoại **Network Traffic Sources**, bạn cần thiết lập mạng nguồn cho rule mạng. Trong ví dụ này, chúng tôi đã chọn mạng **Internal** mặc định làm mạng nguồn. Kích **Add** và sau đó trong hộp thoại **Add Network Entities** kích đúp **Internal**, xem thể hiện trong hình 7. Kích **Close** và tiếp sau đó kích **Next**.

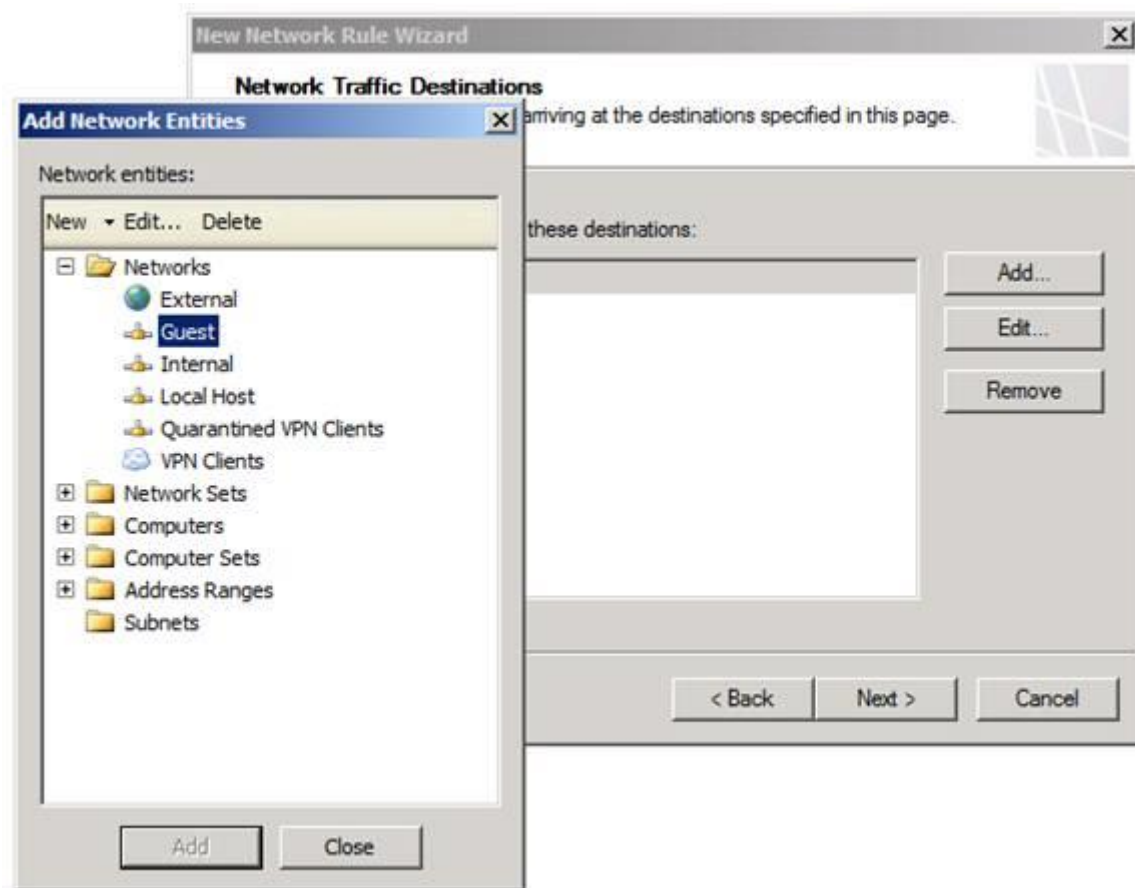
[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 7

Trong trang **Network Traffic Destinations**, thiết lập phía đích đến của rule. Trong ví dụ này chúng tôi đã chọn mạng **Guest** (đó là một mạng DMZ Network) làm phía đích của Network Rule. Kích nút **Add** và chọn DMZ Network từ danh sách **Networks** trong hộp thoại **Add Network Entities**, xem thể hiện trong hình 8, sau đó kích **Next**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

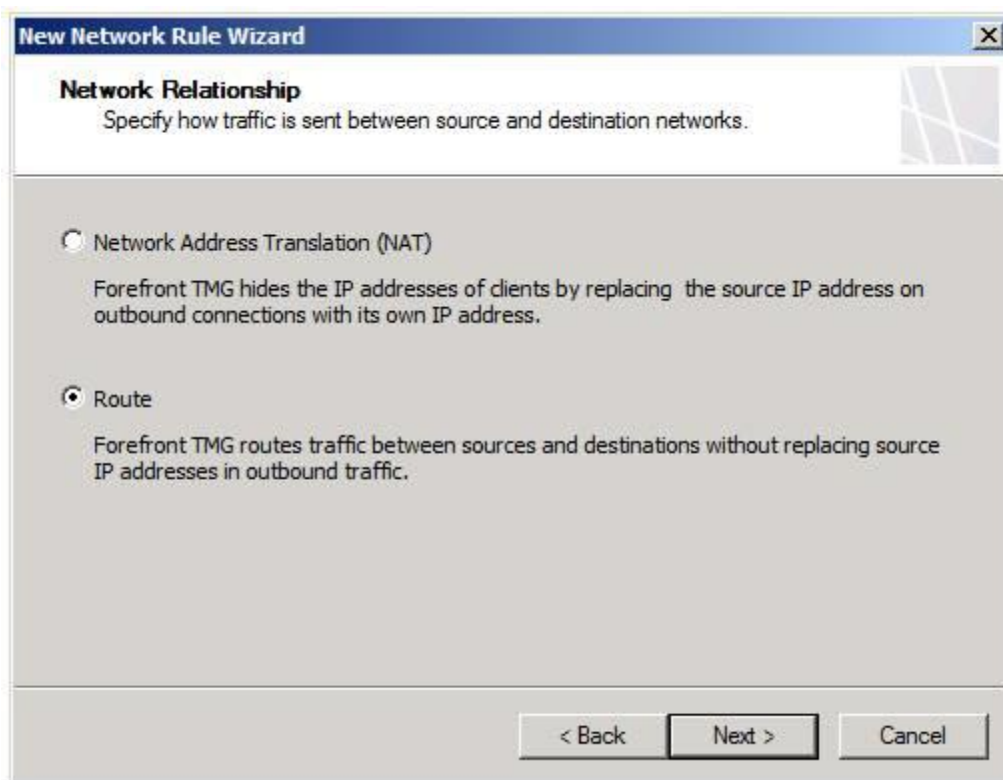


Hình 8

Trong trang **Network Relationship**, hình 9, chọn mối quan hệ tuyến giữa mạng nguồn và đích. Trong ví dụ này, chúng tôi đã chọn tùy chọn **Route** và kích **Next**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Key4VIP.info

Trang cuối cùng của wizard là **Completing the New Network Rule Wizard** như thể hiện trong hình 10. Kiểm tra các thiết lập của bạn và kích **Finish**.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



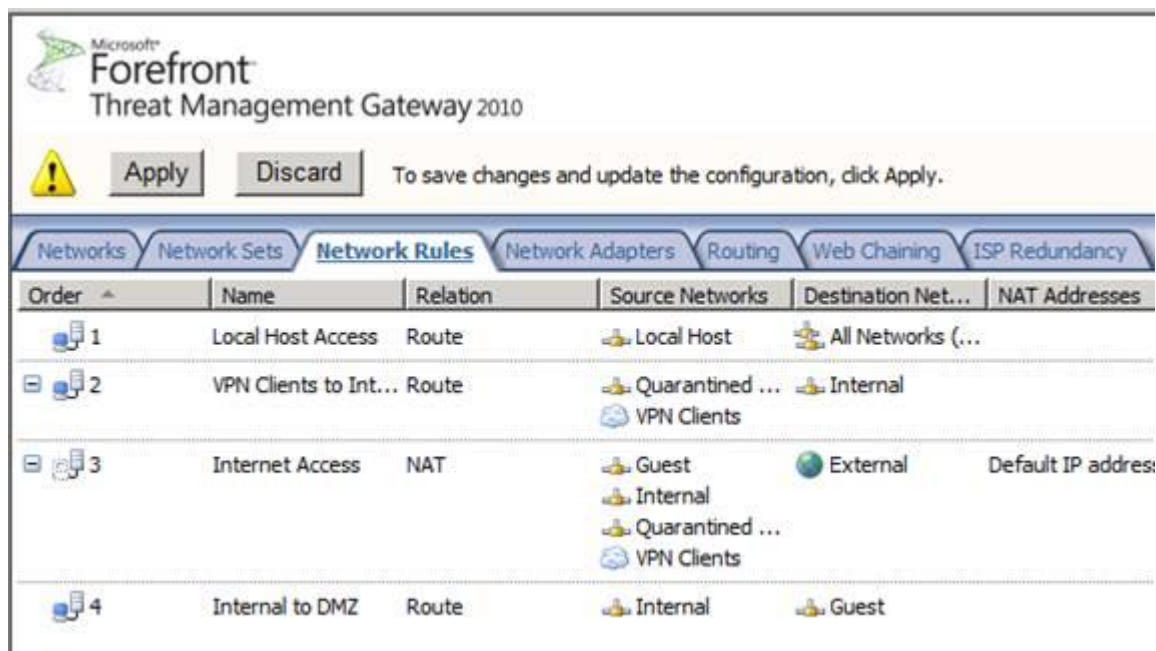
Hình 10  
[Key4VIP.info](http://www.Key4VIP.info)

Bạn có thể thấy rule mạng mới trong danh sách Network Rule trong trang **Network Rules**, như những gì bạn thấy trong hình 11. Network Rules được đánh giá theo thứ tự - vì vậy nếu thấy có sự dè dặt trong một số rule bạn có thể di chuyển rule mà bạn muốn được đánh giá cao hơn lên trên trong danh sách bằng cách kích phải vào nó và kích lệnh **Move Up**. Sau khi rule cần chuyển đã nằm ở vị trí mong muốn, hãy kích nút **Apply** để lưu cấu hình vào chính sách tường lửa.

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..



Hình 11

## Kết luận

Trong bài này chúng tôi đã giới thiệu được cho các bạn một số khái niệm cơ bản được sử dụng trong kết nối mạng có tường lửa TMG - TMG firewall Network và TMG firewall Network Rule. Nếu chưa từng sử dụng nhiều hơn hai NIC trong một tường lửa TMG, bạn sẽ không bao giờ cần phải nghĩ đến chủ đề này. Tuy nhiên nếu quyết định muốn nâng tường lửa TMG lên mức cao hơn, bạn có thể cài đặt nhiều NIC trong tường lửa và tạo các mạng tường lửa TMG mới. Có một điều quan trọng cần nhớ ở đây là bạn không thể sử dụng các mạng đó cho tới khi tạo rule để kết nối các mạng đó với nhau xong. Khi các mạng được kết nối thông qua rule nào đó, sự truyền thông sẽ được cho phép giữa các mạng này.

Trong phần tiếp theo của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn các tùy chọn mặc định có sẵn trong cấu hình mạng khi tạo một mạng Internal hoặc Perimeter.

Đóng gói Ebook bởi [www.Key4VIP.info](http://www.Key4VIP.info)

*Văn Linh (Theo Isaserver)*

[www.Key4VIP.info](http://www.Key4VIP.info) Bán key Windows Server 2003,2008,2012 và các bản R2 bảo hành Vĩnh Viễn  
Bán key SQL,Exchange Server,TMG,SharePoint,Kaspersky ( Client+ Server),Windows 7,8.1,Bitdefender..