**THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA PFSENSE**

* 1. Mô tả

Tường lửa PfSense là loại tường lửa mềm, miễn phí có chức năng kiểm soát lưu lượng mạng, thực hiện các hành động để bảo vệ an toàn cho mạng máy tính.

PfSense là tường lửa cấu hình cơ bản dựa trên dòng lệnh. Quản trị dựa trên chế độ đồ họa cho nên dễ dàng cho người quản trị có thể cấu hình, theo dõi hoạt động của mạng, đảm bảo an toàn cho mạng máy tính.

* 1. Chuẩn bị

− 01 máy ảo hệ điều hành Windows 7: Cài đặt ứng dụng Google Chrome

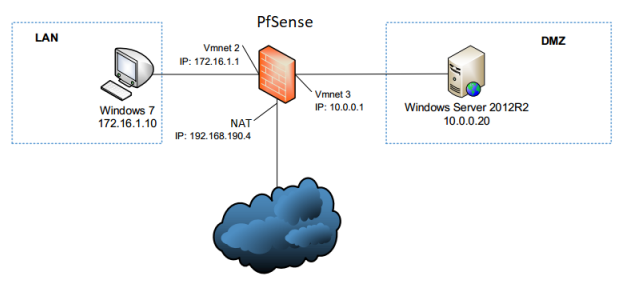
− 01 máy ảo hệ điều hành Windows Server 2012.

+ Đã cài dịch vụ web sử dụng máy chủ web IIS với trang web mặc định của Microsoft.

+ Đã cài phần mềm máy chủ thư điện tử (MDaemon V10).

− 01 máy ảo gốc.

* 1. Mô hình cài đặt



4. Các bước thực hiện

- Bước 1: Chuẩn bị các máy ảo

- Bước 2: Cài đặt tường lửa PfSense

- Bước 3: Cấu hình tường lửa cơ bản

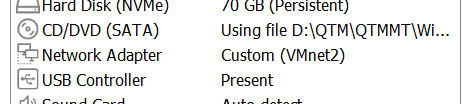
- Bước 4: Quản trị tường lửa bằng đồ họa

- Bước 5: Tạo tập luật theo kịch bản

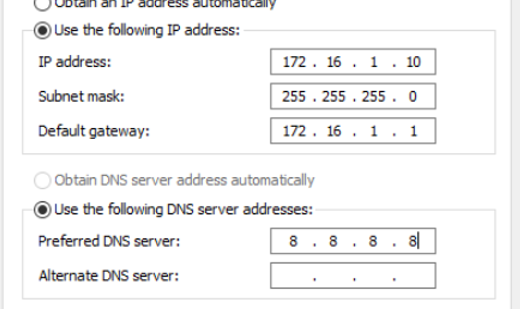
5. Chuẩn bị các máy ảo

a. Máy ảo Windows 7 với cấu hình như sau

- Cấu hình phần cứng: chú ý Vmnet2

****

- Cấu hình IP:

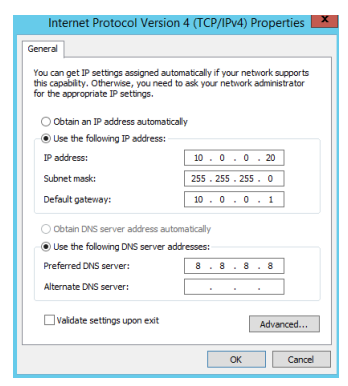


b. Máy ảo Server 2012

- Cấu hình phần cứng: chú ý Vmnet3

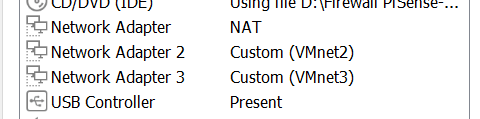


- Cấu hình mạng:



c. Máy ảo PfSense

- Cấu hình phần cứng:

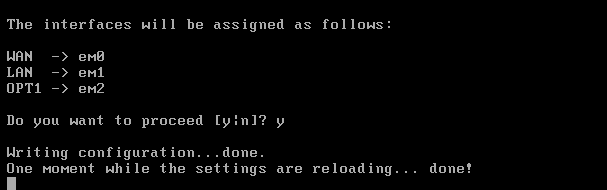


6. Cấu hình tường lửa cơ bản

em0: Cổng mạng kết nối Internet

em1: Cổng mạng kết nối LAN

em2: Cổng mạng kết nối DMZ

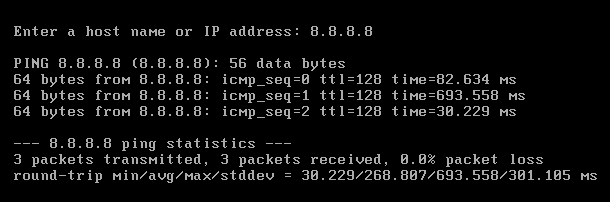


* Chọn y để thực hiện xử lý.
* Tiếp tục cấu hình địa chỉ IP cho mỗi cổng mạng tương ứng với mô hình đã cho.

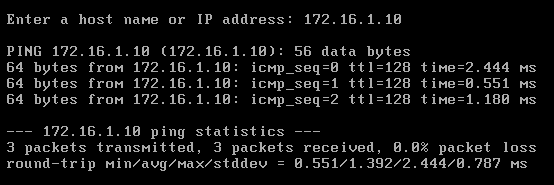


Kiểm tra kết nối tới các máy:

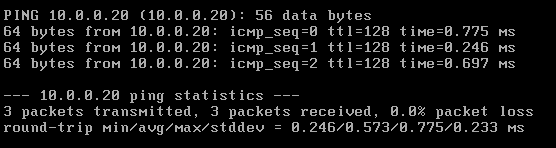
* Ping ra Internet



* Ping tới máy Windows 7



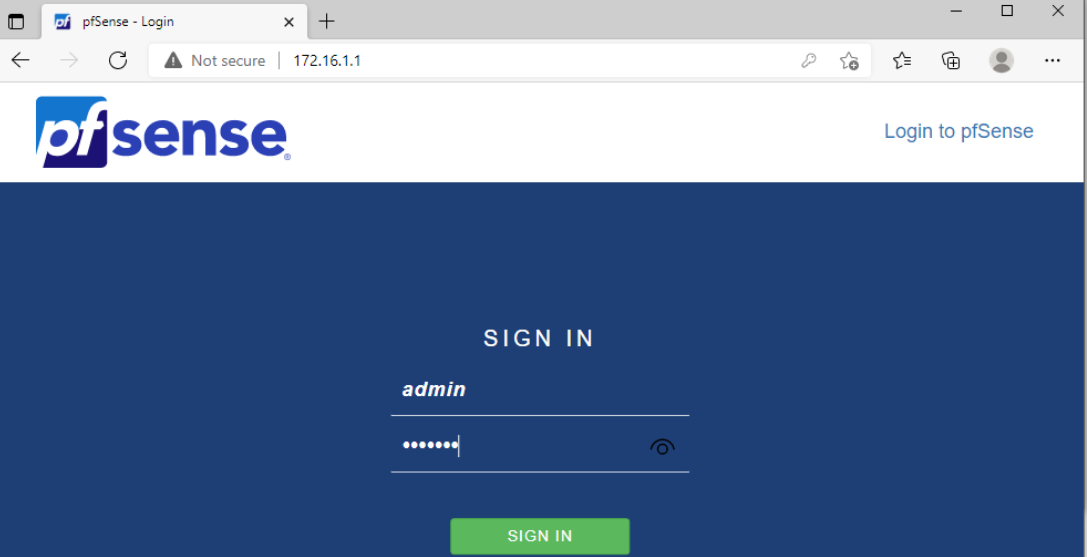
* Ping tới Server 2012



7. Quản trị tường lửa bằng đồ họa

Sau khi kết thúc quá trình cấu hình cơ bản xong, lúc này sử dụng trình duyệt web trên máy tính Windows 7 để truy cập và quản trị tường lửa qua giao diện đồ họa.

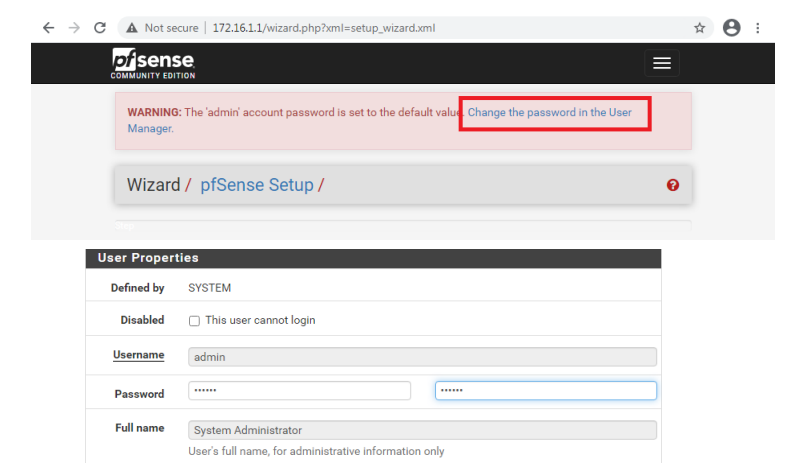
Tại máy Windows 7 sử dụng trình duyệt Google Chrome đã cài đặt truy cập theo đường dẫn: http://172.16.1.1



User: admin

Pass: pfsense

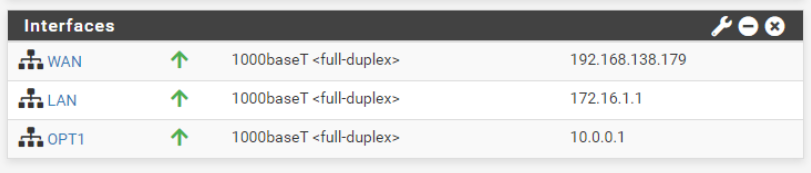
Công việc đầu tiên cần thay đổi mật khẩu cho tài khoản admin



Nhấn Save ở phía cuối trang để lưu và trở về giao diện quản trị.

Giao diện quản trị chung

Thông tin về cổng mạng



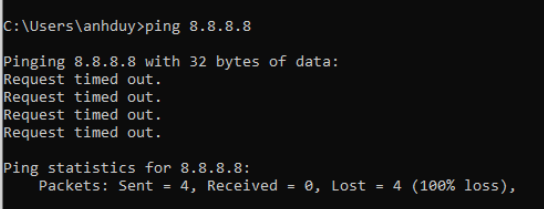
Chú ý: IP cổng WAN khác với IP trong mô hình đã cho vì để chế độ DHCP, trong môi trường máy ảo phải để chế độ này mới truy cập được Internet.

Trong thực tế IP cổng này là IP public là địa chỉ tĩnh.

**1.9. Tạo tập luật theo kịch bản**

**1.9.1. Kịch bản 1: Cho phép máy trạm trong mạng LAN Ping ra Internet**

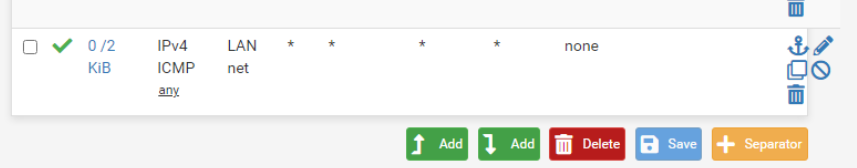
Trước khi thiết lập luật, kiểm tra Ping:



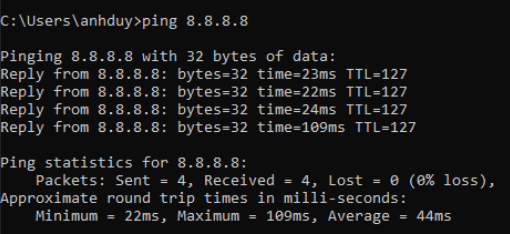
Kết quả đang bị chặn bởi tường lửa.

Chọn Add, đê thêm luật

Chọn Save để lưu cấu hình và Apply Changes để chạy luật. Kết quả



Ping kiểm tra lại, kết quả:

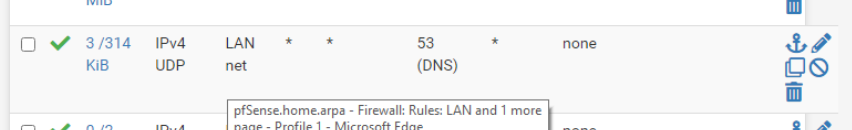


Như vậy sau khi thiết lập luật cho tường lửa, thì lúc này các gói tin ICMP đi qua tường lửa đều cho phép.

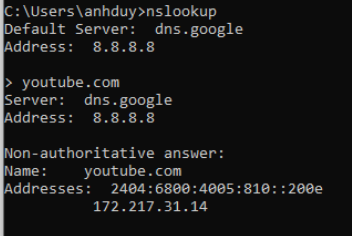
**1.9.2. Kịch bản 2: Cho phép máy tính trong mạng LAN truy vấn DNS ra Internet**

Chọn Add, đê thêm luật

Chọn Save để lưu cấu hình và Apply Changes để chạy luật. Kết quả



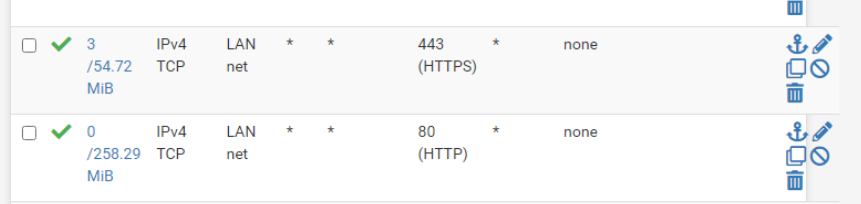
Kiểm tra kết quả, sử dụng giao diện dòng lệnh DOS, chạy lệnh: nslookup để kiểm tra:



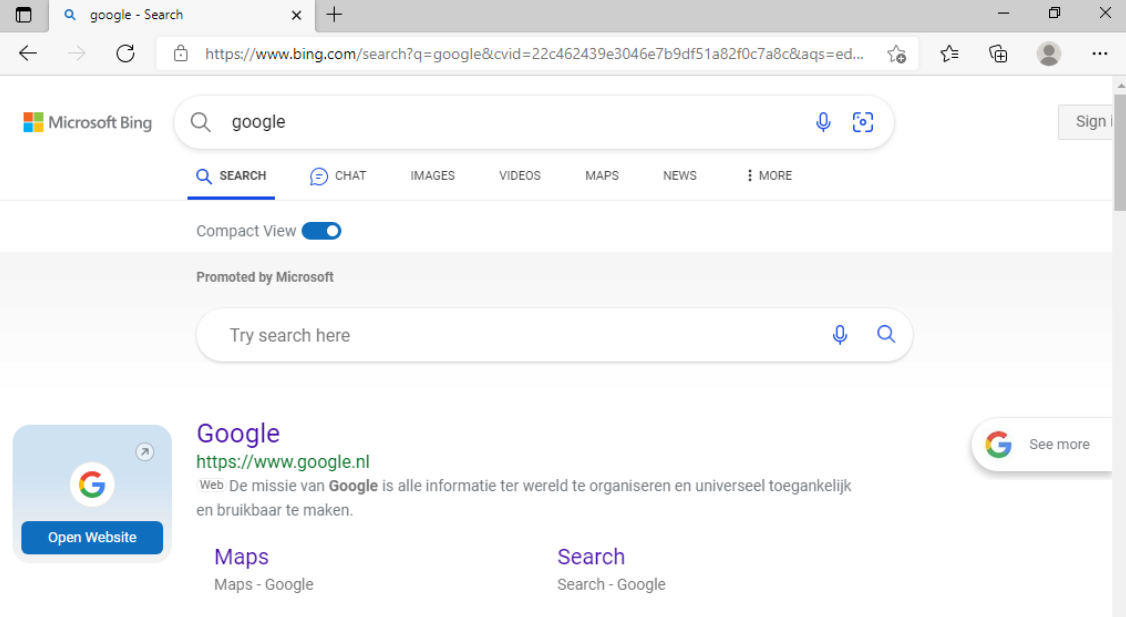
Có kết quả trả về địa chỉ IP tương ứng với tên miền

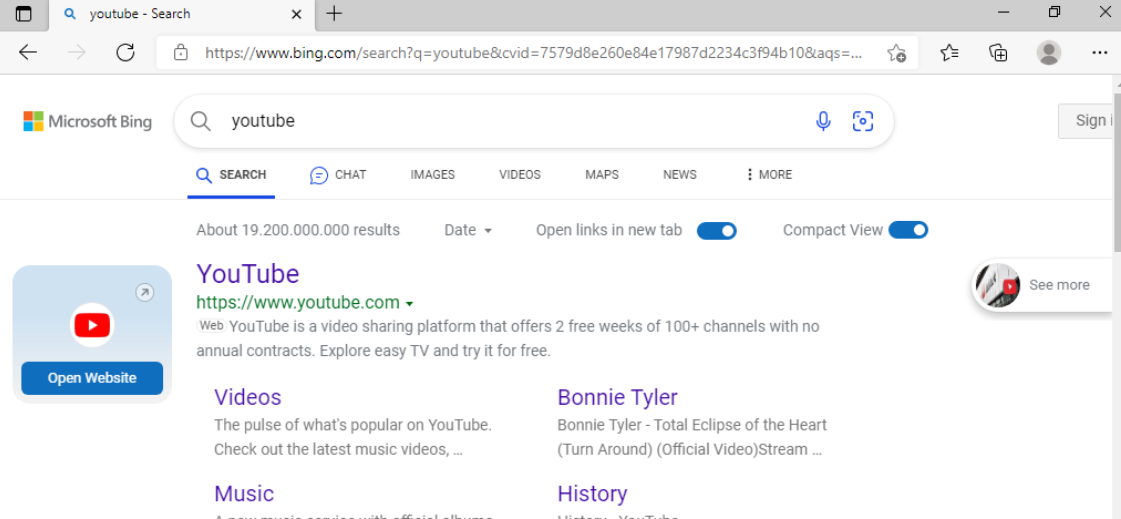
**1.9.3. Kịch bản 3: Cho phép máy tính trong mạng LAN truy cập website qua cổng 80, 443.**

Luật đã tạo như sau:



Kiểm tra kết quả truy cập website trên Windows 10:



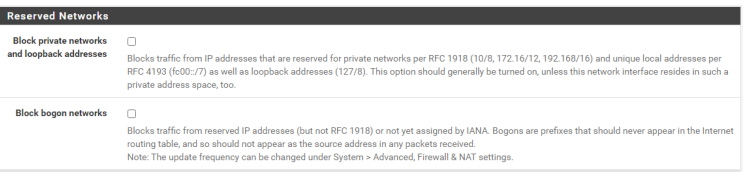


Kết quả thành công.

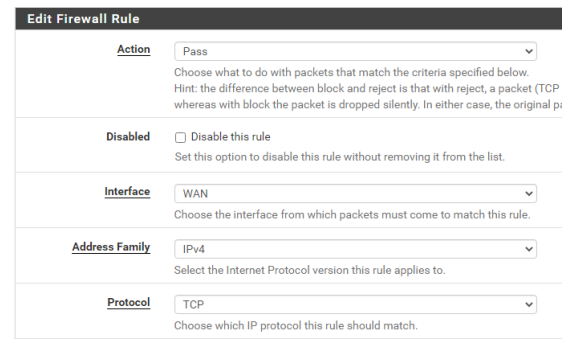
**1.9.4. Kịch bản 4: Cho phép máy tính ngoài Internet truy cập vào website trên máy chủ DMZ**

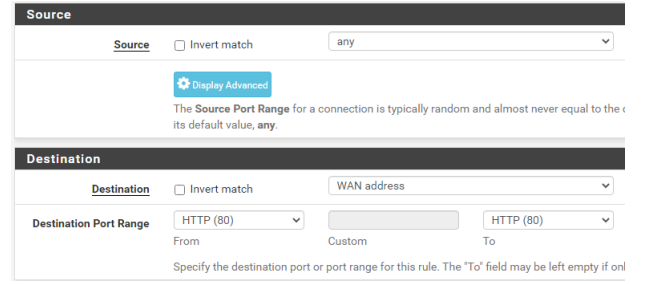
Tạo luật:

Chuyển qua giao diện cấu hình cho WAN. Bỏ 2 luật mặc định đã được tạo sẵn trong mạng WAN bằng cách vào phần setting bỏ 2 tùy chọn như sau

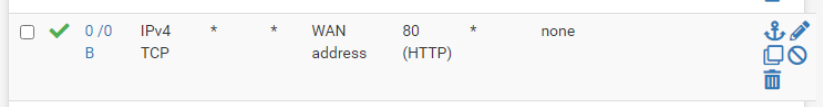


Lưu và thoát. Vào phần Add để tạo luật với các thông tin như sau:





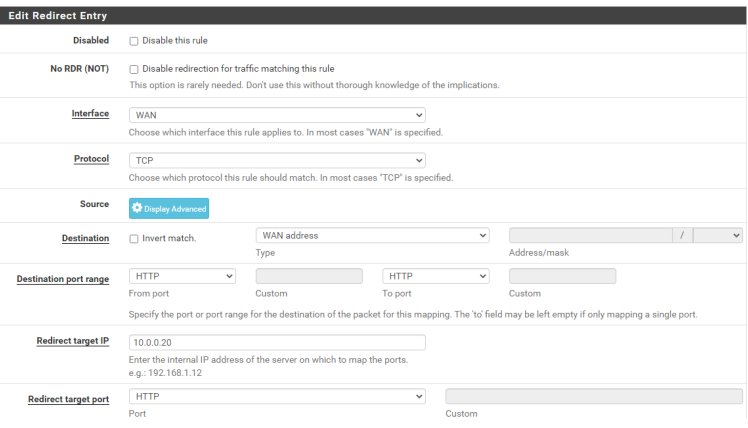
Lưu và thoát. Kết quả:



Để người dùng từ bên ngoài có thể truy cập được cần thực hiện NAT từ ngoài vào trong máy web server.

Vào Firewall → NAT

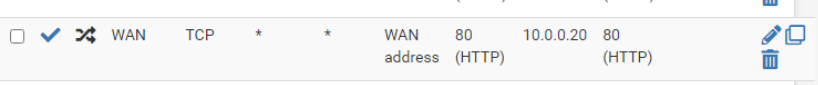
Để public các dịch vụ, chúng ta sử dụng NAT chế độ Port Forward. Chọn Add, tạo luật:



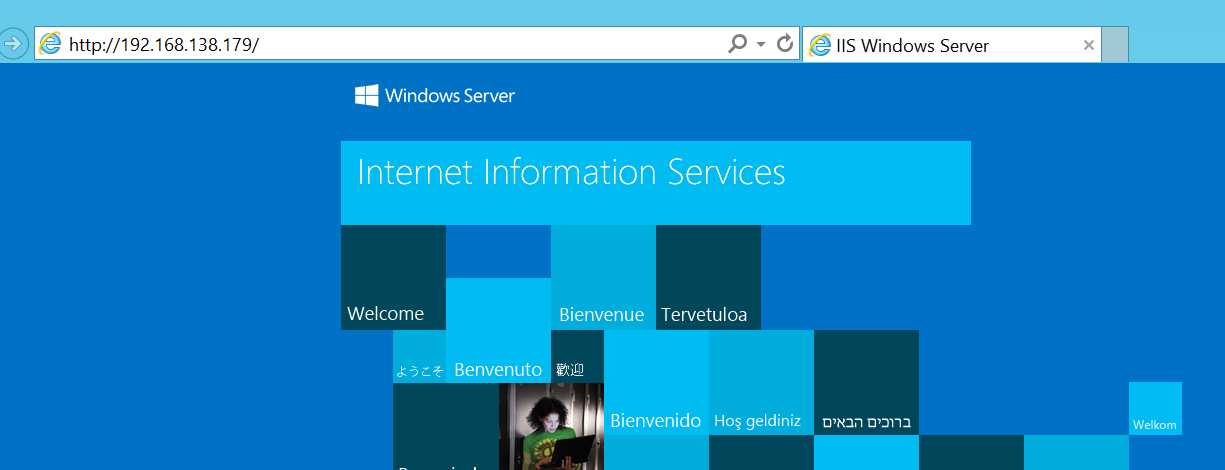
Chú ý: WAN address ở đây là địa chỉ của cổng mạng firewall kết nối ra Internet, theo cấu hình trong bài địa chỉ này là: 192.168.138.179. Máy trạm ở ngoài Internet (trong bài thực hành này sử dụng máy tính vật lý) truy cập vào website theo địa chỉ này.

Chọn lưu và Apply Change.

Kết quả:



Kiểm tra kết quả: Tại máy vật lý sử dụng trình duyệt web, truy cập vào địa chỉ như trên. (Máy vật lý và máy ảo kết nối với nhau qua cổng NAT của máy ảo).



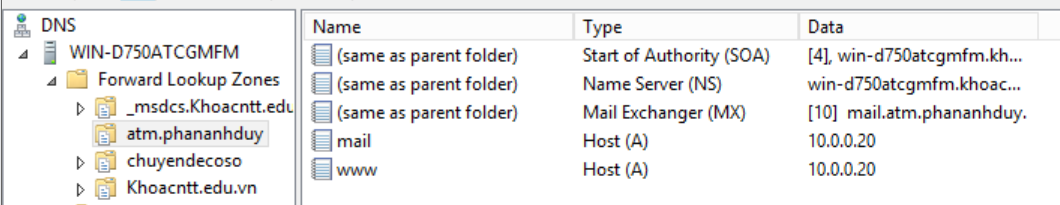
Kết quả thành công.

**1.9.5. Kịch bản 5: cho phép người dùng trong mạng LAN gửi và nhận mail với người dùng ngoài Internet sử dụng mail server trong DMZ.**

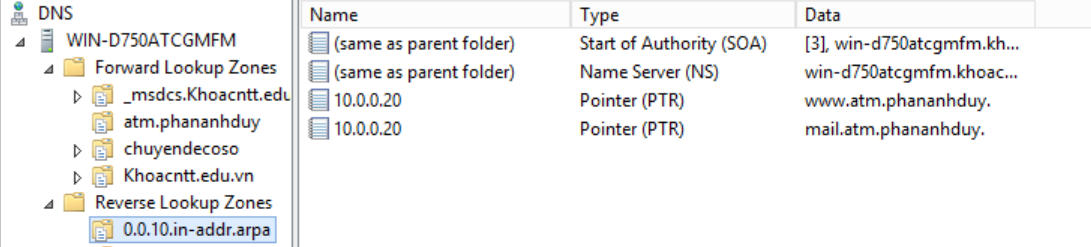
Cài đặt dịch vụ DNS trên máy chủ Windows Server 2012

Giao diện quản trị DNS xuất hiện:

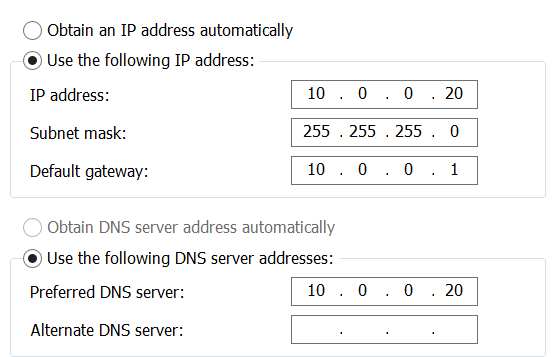
Chọn Forward Lookup Zone để tạo tên miền với IP tương ứng.



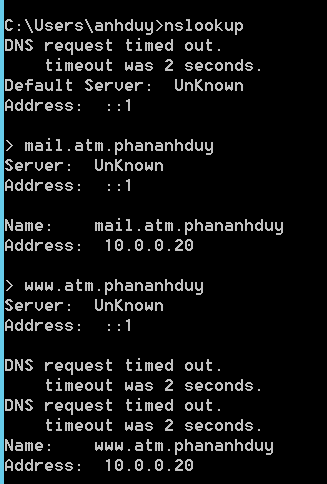
Chọn Reverse Lookup Zone để tạo phân giải ngược



Để kiểm tra dịch vụ DNS hoạt động đúng hay chưa cần sử dụng chương trình DOS (cmd) và lệnh nslookup. Trước tiên cần cấu hình lại địa chỉ IP của máy chủ DNS trong cấu hình mạng.

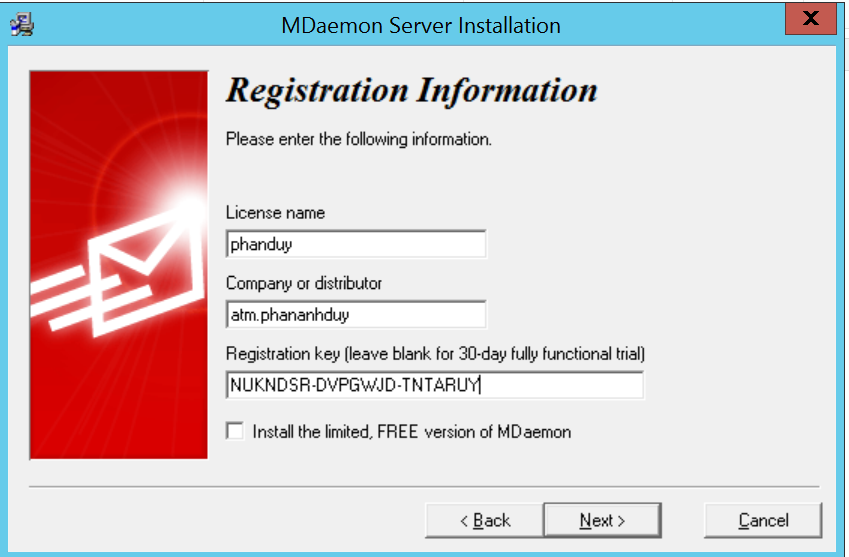


Kiểm tra:



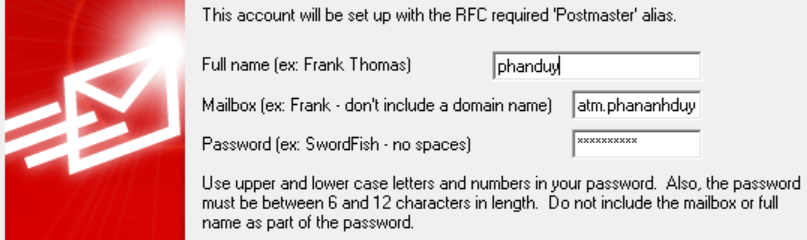
Kết quả truy vấn thành công.

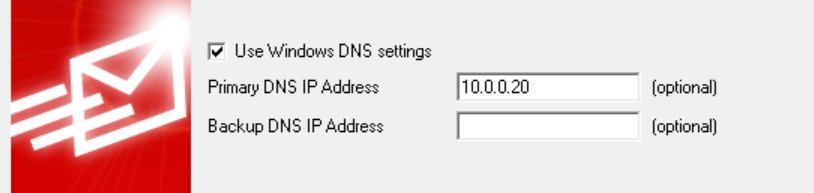
- Cài đặt dịch vụ mail trên máy chủ Windows Server 2012: Sao chép phần mềm máy chủ thư điện tử MDaemon V10 vào Server 2012. Thực hiện cài đặt và điền một số thông tin như sau:



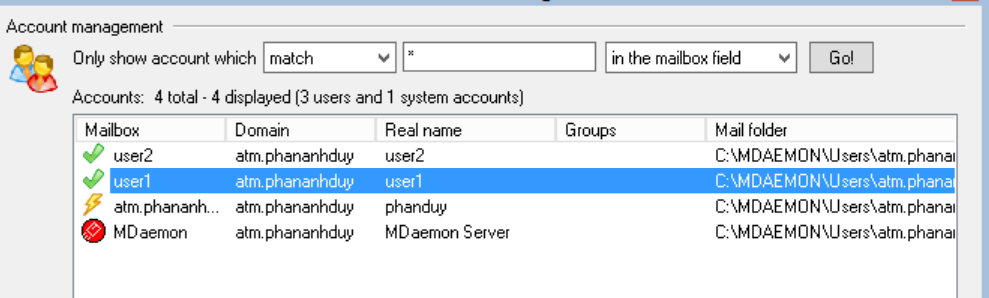
Domain Name: atm.phananhduy





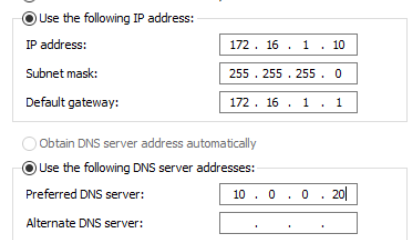


Sau khi cài đặt xong mail server, tạo các tài khoản người dùng mail. Vào mục Account → new account, với các thông tin

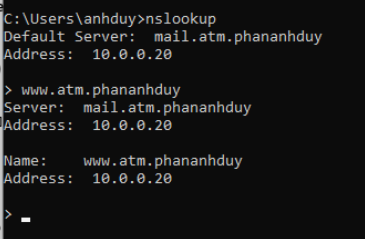


Sử dụng phần mềm Thunderbird Setup làm mail client cho tài khoản user2

Cài đặt và cấu hình như sau: Trước tiên phải chuyển IP DNS trên Windows 10 như sau

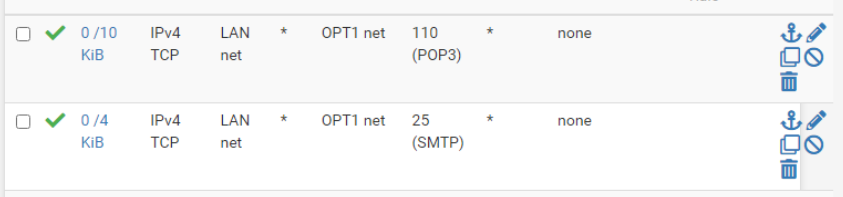


Sử dụng DOS (cmd) lệnh nslookup để truy vấn thử tên miền.

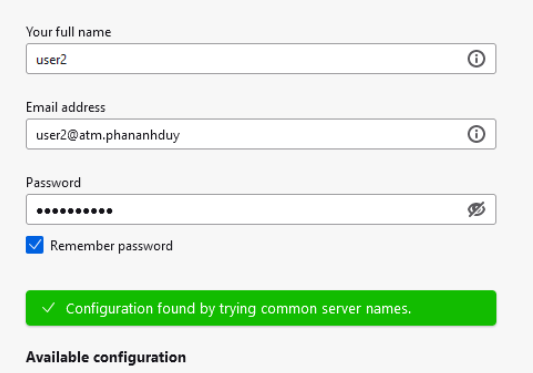


Kết quả thành công

Truy cập vào trình duyệt quản trị tường lửa, vào phần Rules → LAN và mở luật như sau:

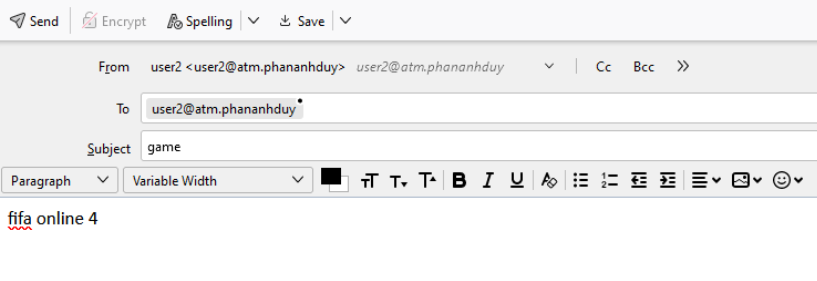


Kết quả: mail client truy vấn thành công

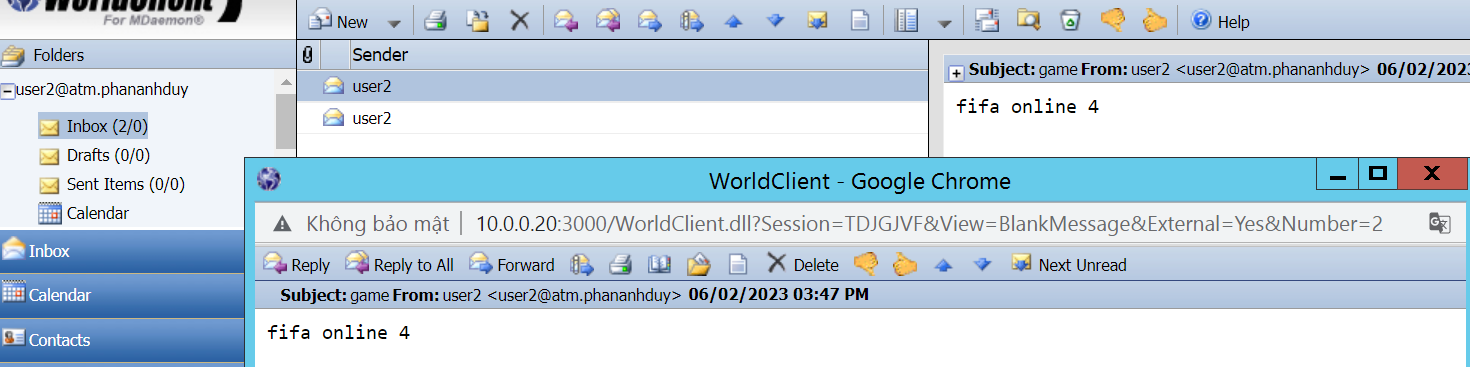


Nhấn Done để kết thúc cài đặt và thiết lập cho mail client.

- Kiểm tra quá trình gửi và nhận mail đã thành công hay chưa Tại phần mềm mail, với tài khoản user2 gửi và nhận thư cho chính nó để kiểm tra

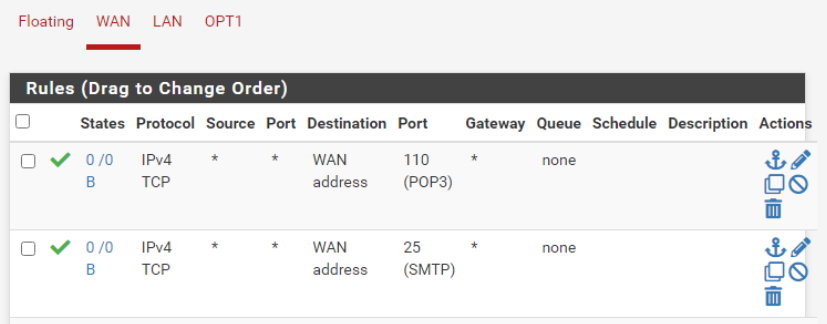


Kết quả:

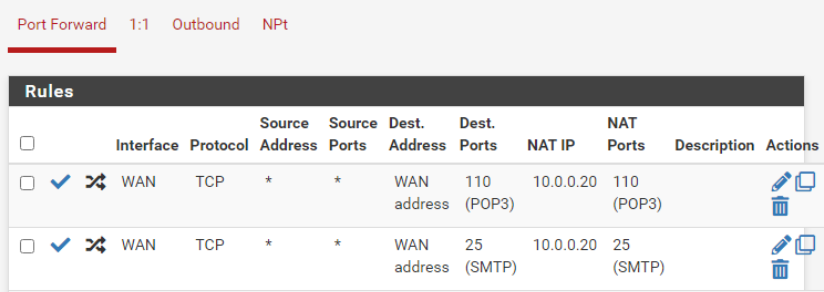


Đã gửi và nhận thư thành công.

Cấu hình luật để Public dịch vụ mail ra Internet:

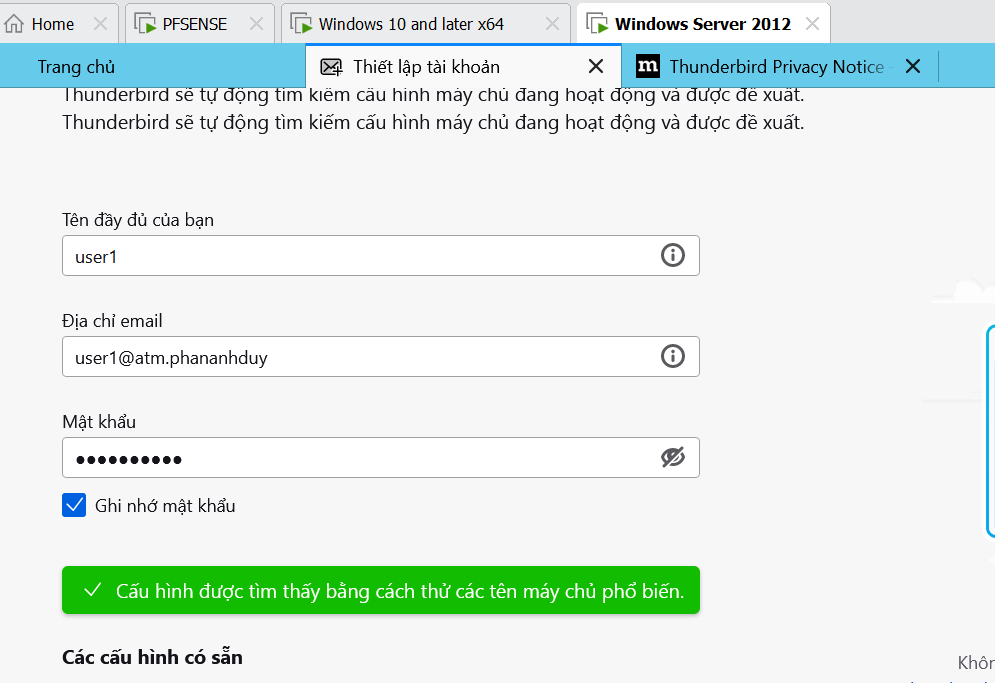


Cấu hình NAT:



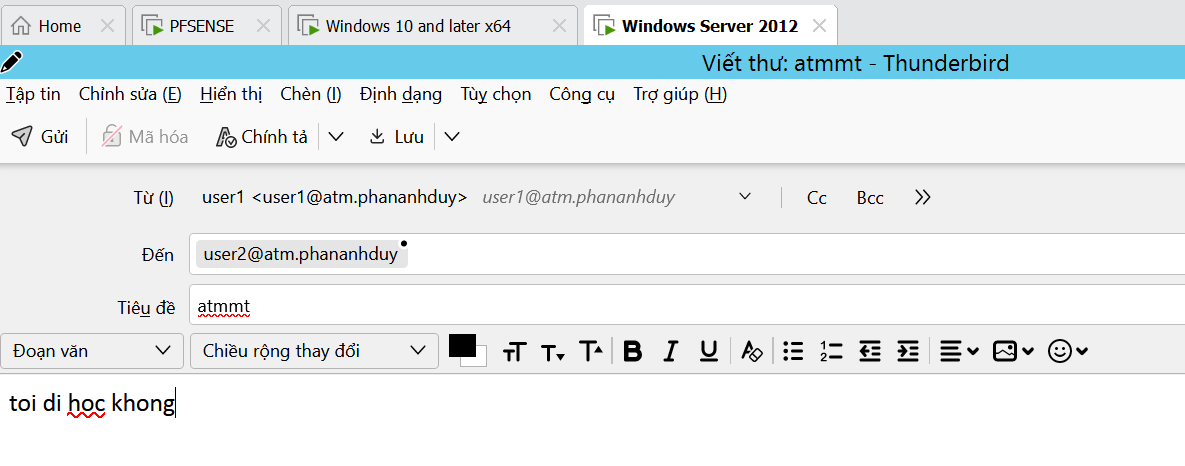
Cấu hình trên máy tính vật lý

Cài đặt phần mềm Thunderbirth và thiết lập giống như trong Win10

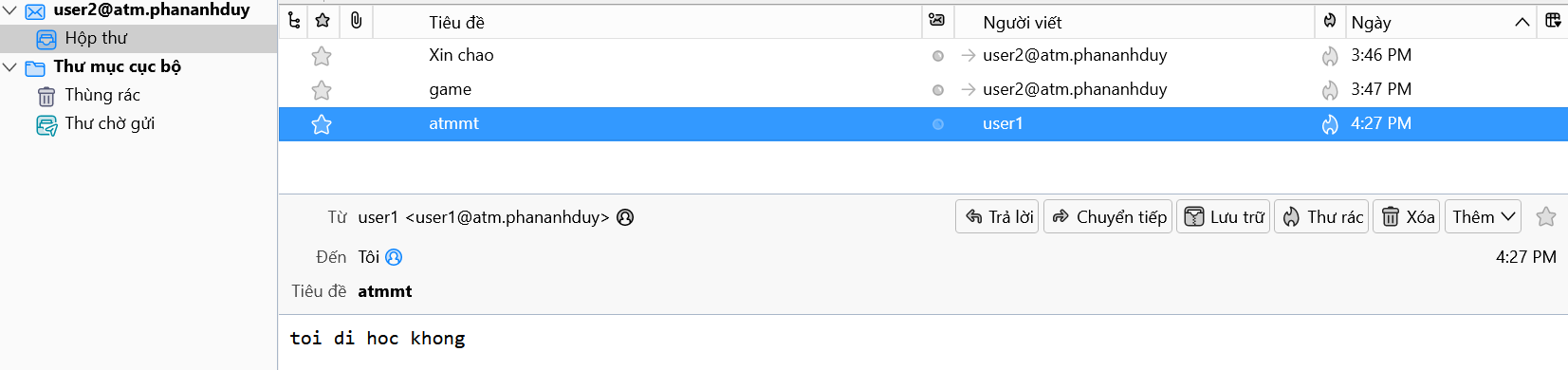


Kết quả thành công. Done để đóng của sổ cấu hình.

Sử dụng phần mềm mail client (user1) vừa cấu hình gửi thư cho user2:



Truy cập vào mail client trên Win 10 để kiểm tra:

****

Kết quả người dùng user2 trên Windows 10 đã nhận được mail từ người dùng user1 ngoài Internet qua máy chủ thư trong DMZ.

Kết luận: Cấu hình luật thành công trên tường lửa để cho phép người dùng gửi và nhận thư