

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 02
TRIỂN KHAI TƯỜNG LỬA PFSENSE

Người xây dựng bài thực hành:

ThS. Cao Minh Tuấn

HÀ NỘI, 2021

MỤC LỤC

Mục lục	2
Thông tin chung về bài thực hành	3
Chuẩn bị bài thực hành	4
Đối với giảng viên	4
Đối với sinh viên	4
THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA PfSense.....	5
1.1. Mô tả.....	5
1.2. Chuẩn bị	5
1.3. Mô hình cài đặt.....	5
1.4. Các bước thực hiện.....	5
1.5. Chuẩn bị các máy ảo	6
1.6. Cài đặt tường lửa PfSense	10
1.7. Cấu hình tường lửa cơ bản	12
1.8. Quản trị tường lửa bằng đồ họa.....	14
1.9. Tạo tập luật theo kịch bản	16
<i>1.9.1. Kịch bản 1: Cho phép máy trạm trong mạng LAN Ping ra Internet....</i>	<i>17</i>
<i>1.9.2. Kịch bản 2: Cho phép máy tính trong mạng LAN truy vấn DNS ra Internet</i>	<i>18</i>
<i>1.9.3. Kịch bản 3: Cho phép máy tính trong mạng LAN truy cập website qua cổng 80, 443.....</i>	<i>19</i>
<i>1.9.4. Kịch bản 4: Cho phép máy tính ngoài Internet truy cập vào website trên máy chủ DMZ</i>	<i>20</i>
<i>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.</i>	<i>23</i>

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Thiết lập và cấu hình tường lửa PfSense.

Học phần: An toàn mạng máy tính

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

Máy tính vật lý có cấu hình tối thiểu: RAM 4GB, 50 HDD

- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA PFSENSE

1.1. Mô tả

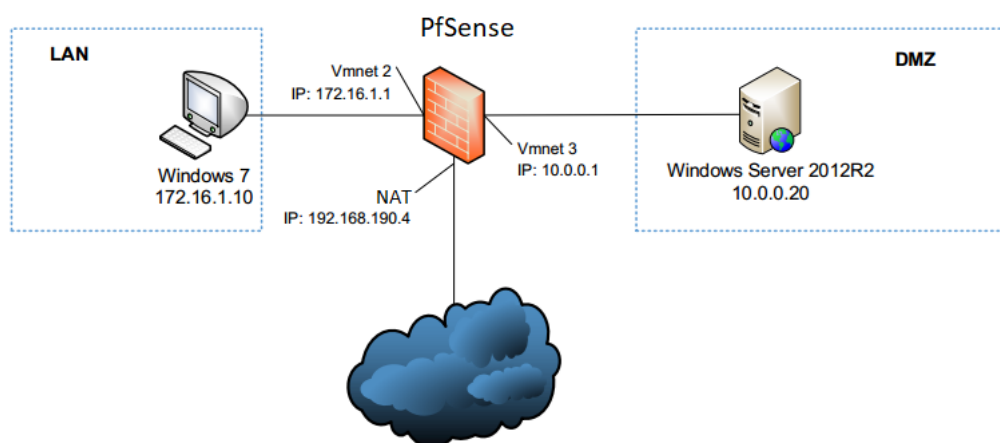
Tường lửa PfSense là loại tường lửa mềm, miễn phí có chức năng kiểm soát lưu lượng mạng, thực hiện các hành động để bảo vệ an toàn cho mạng máy tính.

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.

1.2. 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.

1.3. Mô hình cài đặt



1.4. Các bước thực hiện

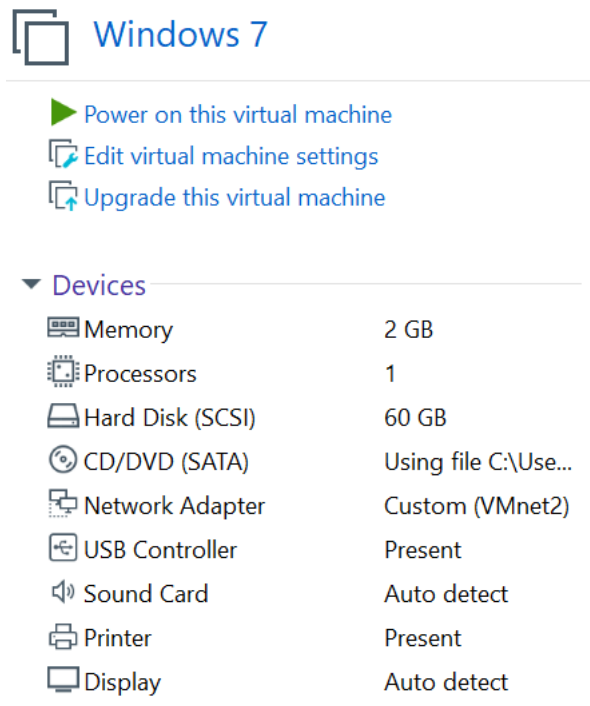
- Bước 1: Chuẩn bị các máy ảo
- Bước 2: Cài đặt tường lửa PfSense
- Bước 3: Cấu hình tường lửa cơ bản

- Bước 4: Quản trị tường lửa bằng đồ họa
- Bước 5: Tạo tập luật theo kịch bản

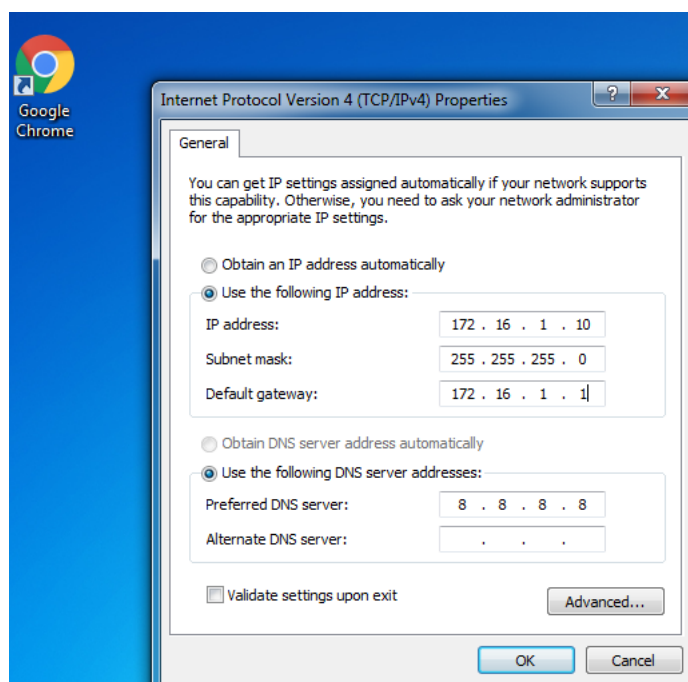
1.5. Chuẩn bị các máy ảo

1. Máy ảo Windows 7 với cấu hình như sau

- Cấu hình phần cứng: chú ý **Vmnet2**

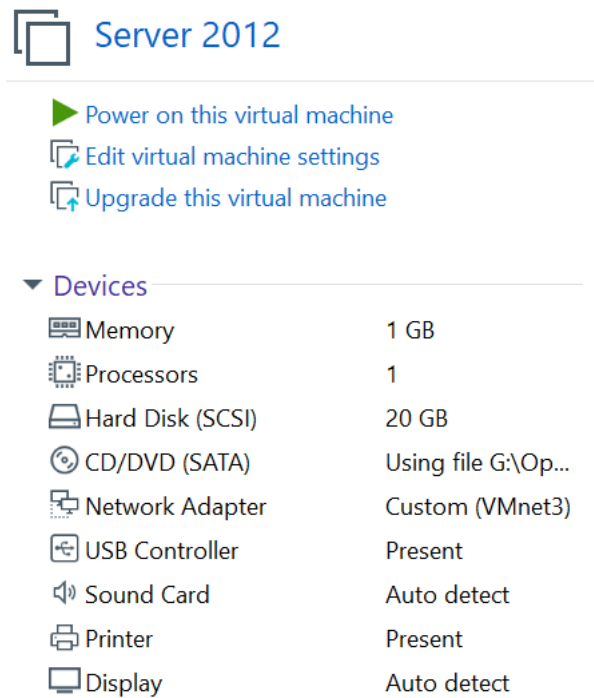


- Cài đặt trình duyệt Google Chrome
- Cấu hình IP:

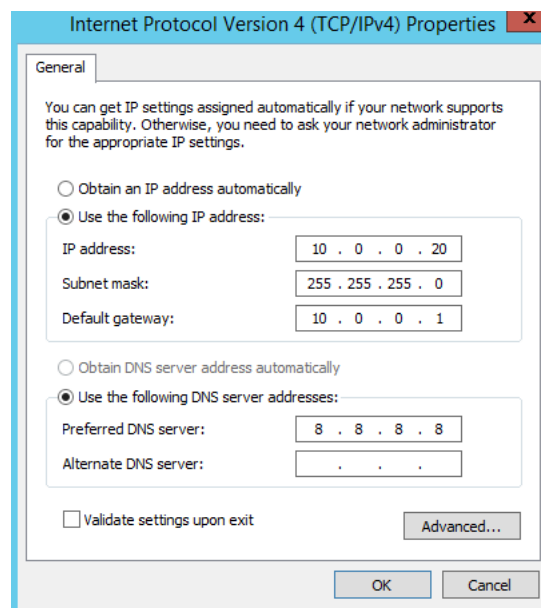


2. Máy ảo Server 2012

- Cấu hình phần cứng: chú ý **Vmnet3**



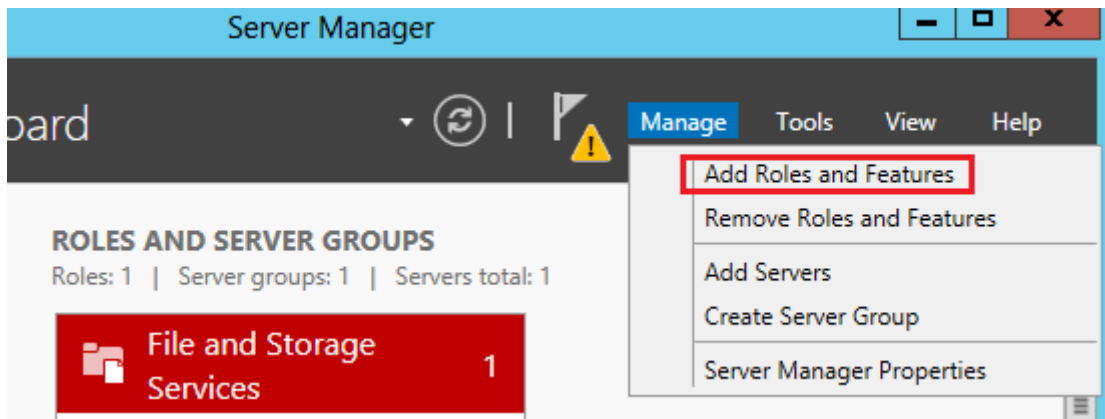
- Cấu hình mạng:



- Cài đặt máy chủ web IIS

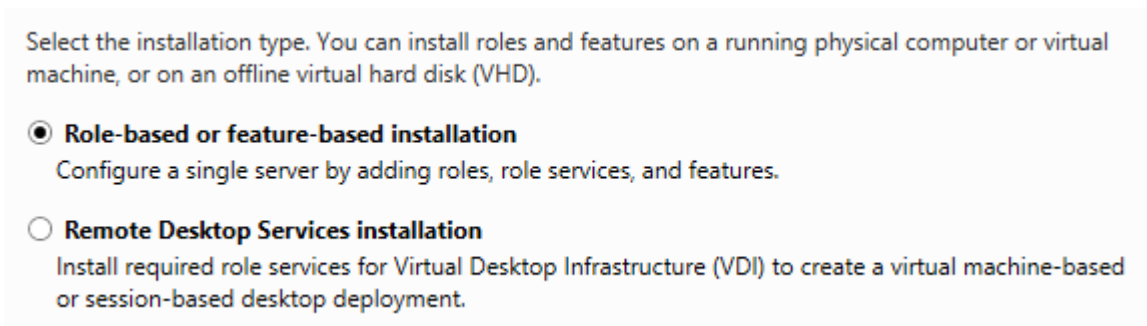
Truy cập theo đường dẫn để cài đặt dịch vụ

Server Manager → Manage → Add Roles and Features



Cửa sổ Add Roles and Features xuất hiện chọn Next để bắt đầu quá trình cài đặt.

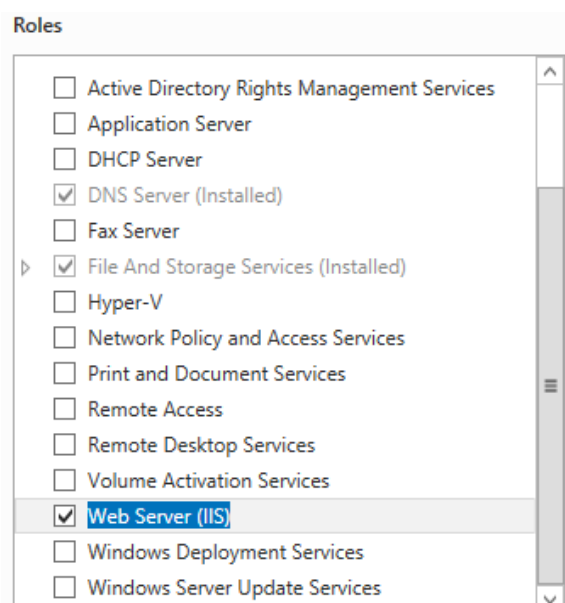
Trong lựa chọn Select installation type → chọn Role-based or feature-based installation để cài đặt các dịch vụ và tính năng cho máy chủ.



Chọn Next để tiếp tục cài đặt.

Trong tùy chọn Select destination server → Chọn Select a server from the server pool.

Tiếp tục lựa chọn dịch vụ



Chọn Next để tiếp tục.

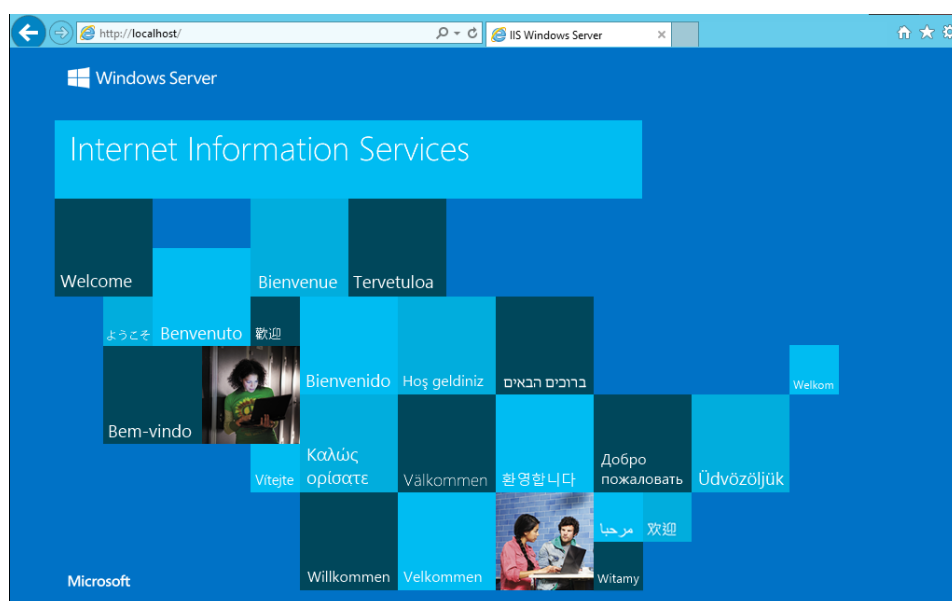
Trong mục Select features để mặc định → chọn Next để tiếp tục.

Các bước tiếp theo để mặc định → Install

Quá trình cài đặt thành công.

Để kiểm tra dịch vụ web, sử dụng trình duyệt Internet Explorer trên Server 2012. Truy cập theo đường dẫn:

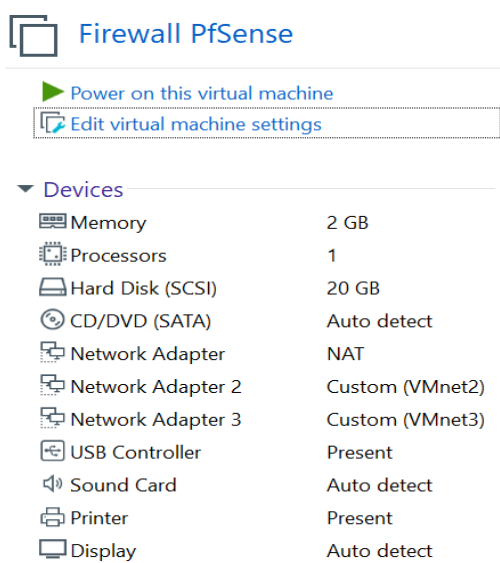
<http://localhost>



Nội dung hiển thị như trên thì dịch vụ web đã hoạt động.

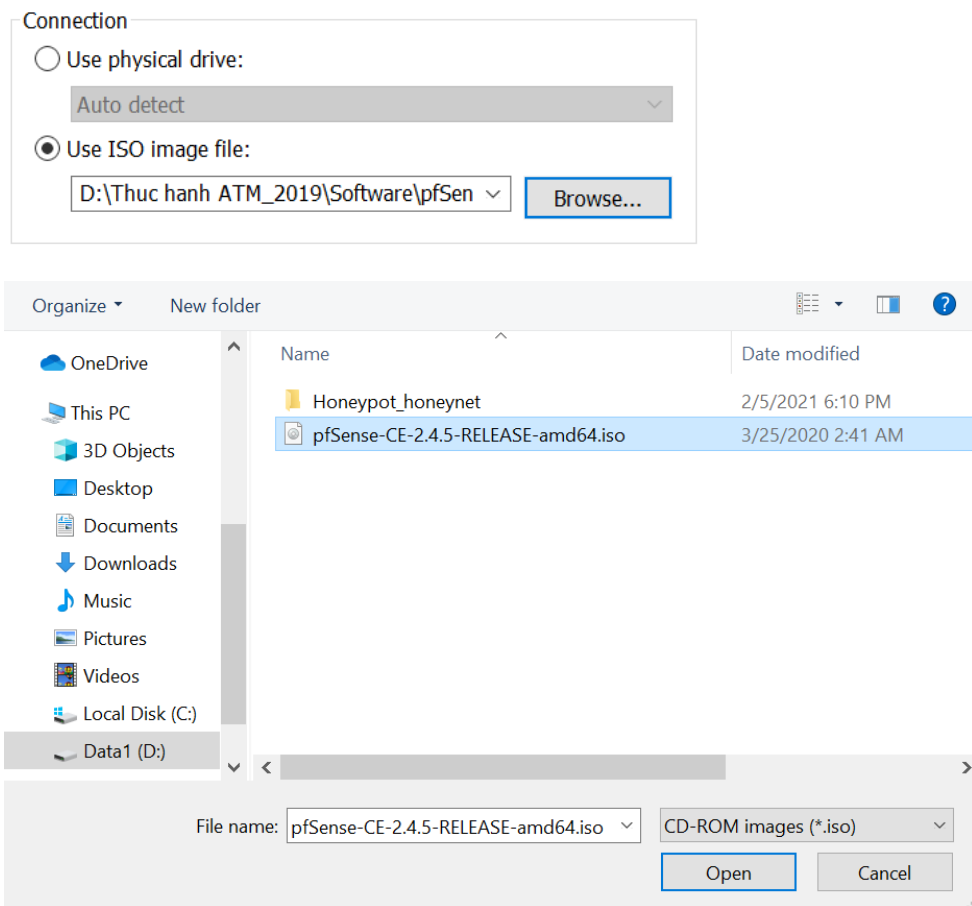
3. Máy ảo PfSense

- Cấu hình phần cứng:



- Chèn đĩa cài đặt

Từ giao diện trên chọn CD/DVD → trở tới nơi lưu trữ hệ điều hành PfSense



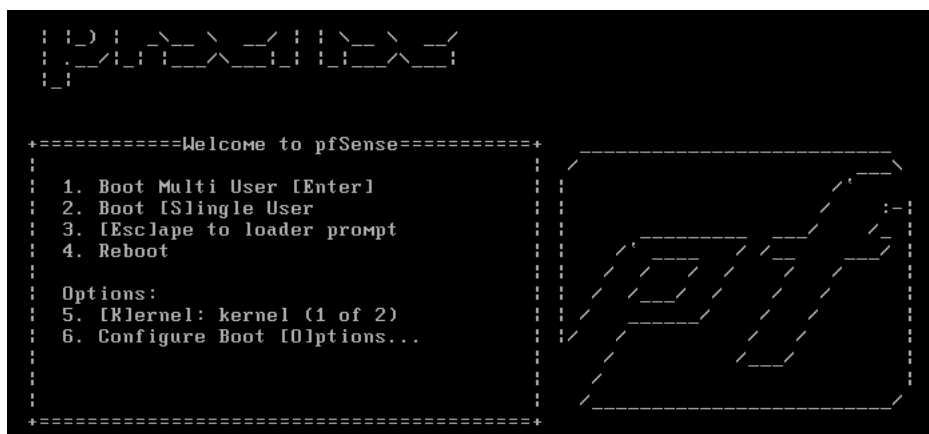
Nhấn Open để lựa chọn hệ điều hành.

Chọn OK để hoàn tất cấu hình phần cứng.

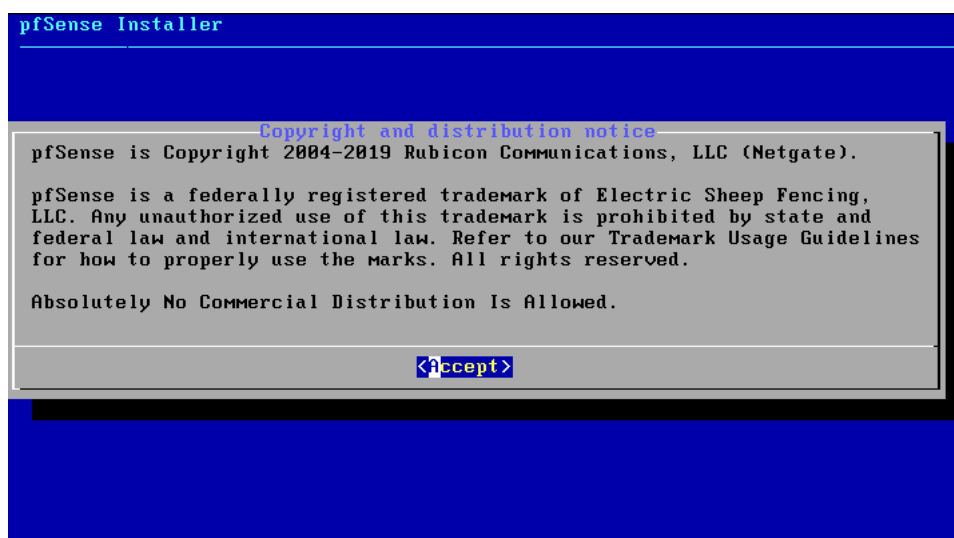
1.6. Cài đặt tường lửa PfSense

Sau khi cấu hình phần cứng cho máy ảo PfSense xong, khởi động máy ảo.

Quá trình cài đặt bắt đầu



Quá trình diễn ra mặc định



Quá trình tiếp theo để mặc định và nhấn Enter để cài đặt.

Giao diện cuối cùng chọn



Chọn No để bỏ qua chế độ kiểm tra.

Chọn Reboot để khởi động lại tường lửa sau khi đã cài đặt xong.

1.7. Cấu hình tường lửa cơ bản

Sau khi khởi động lại tường lửa, bắt đầu cấu hình cơ bản:

```
Valid interfaces are:

le0      08:0c:29:e8:a1:02 (down) AMD PCnet-PCI
le1      08:0c:29:e8:a1:0c (down) AMD PCnet-PCI
le2      08:0c:29:e8:a1:16 (down) AMD PCnet-PCI

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y|n]? █
```

Cấu hình mạng LAN ảo, chọn n để bỏ qua.

Lựa chọn cổng mạng tương ứng với các phân vùng mạng

```
Enter the WAN interface name or 'a' for auto-detection
(le0 le1 le2 or a): le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 le2 a or nothing if finished): le1

Enter the Optional 1 interface name or 'a' for auto-detection
(le2 a or nothing if finished): le2█
```

Le0: Cổng mạng kết nối Internet

Le1: Cổng mạng kết nối LAN

Le2: Cổng mạng kết nối DMZ

```
The interfaces will be assigned as follows:

WAN   -> le0
LAN   -> le1
OPT1  -> le2

Do you want to proceed [y|n]? y█
```

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.

```
WAN (wan)      -> le0      -> v4/DHCP4: 192.168.190.129/24
LAN (lan)      -> le1      -> v4: 172.16.1.1/24
OPT1 (opt1)    -> le2      -> v4: 10.0.0.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Chọn 2 để cấu hình

Chú ý: ở trong môi trường ảo hóa này IP cổng WAN nên để mặc định.

Tiếp tục cấu hình cho cổng LAN

```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - static)
2 - LAN (le1 - static)
3 - OPT1 (le2)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

Chú ý muốn quản trị tường lửa PfSense qua giao diện web thì phải thực hiện bước sau đây:

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Kết quả:

```
The IPv4 LAN address has been set to 172.16.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://172.16.1.1/

Press <ENTER> to continue.
```

Tương tự cấu hình IP cho cổng mạng DMZ qua OPT1

```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - static)
2 - LAN (le1 - static)
3 - OPT1 (le2)

Enter the number of the interface you wish to configure: 3

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 31):
> 24
```

Kết quả cuối cùng sau khi cấu hình cơ bản:

```
*** Welcome to pfSense 2.4.5-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.190.129/24
LAN (lan)       -> le1      -> v4: 172.16.1.1/24
OPT1 (opt1)    -> le2      -> v4: 10.0.0.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Kiểm tra kết nối tới các máy:

Ping ra Internet

```
Enter a host name or IP address: 8.8.8.8

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=24.511 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=26.601 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=24.846 ms
```

Ping tới máy Windows 7

```
Enter a host name or IP address: 172.16.1.10

PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.510 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.796 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.943 ms
```

Ping tới Server 2012

```
Enter a host name or IP address: 10.0.0.20

PING 10.0.0.20 (10.0.0.20): 56 data bytes
64 bytes from 10.0.0.20: icmp_seq=0 ttl=128 time=0.379 ms
64 bytes from 10.0.0.20: icmp_seq=1 ttl=128 time=0.834 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=128 time=0.778 ms
```

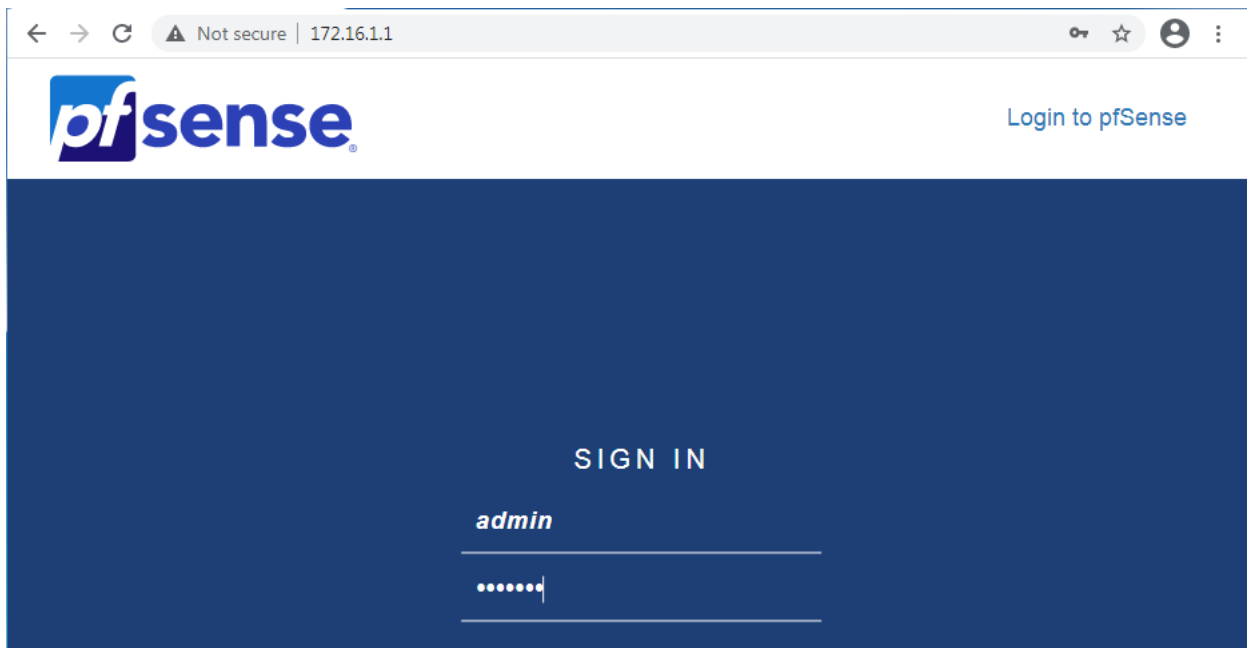
Kết quả cấu hình mạng thành công.

1.8. 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:

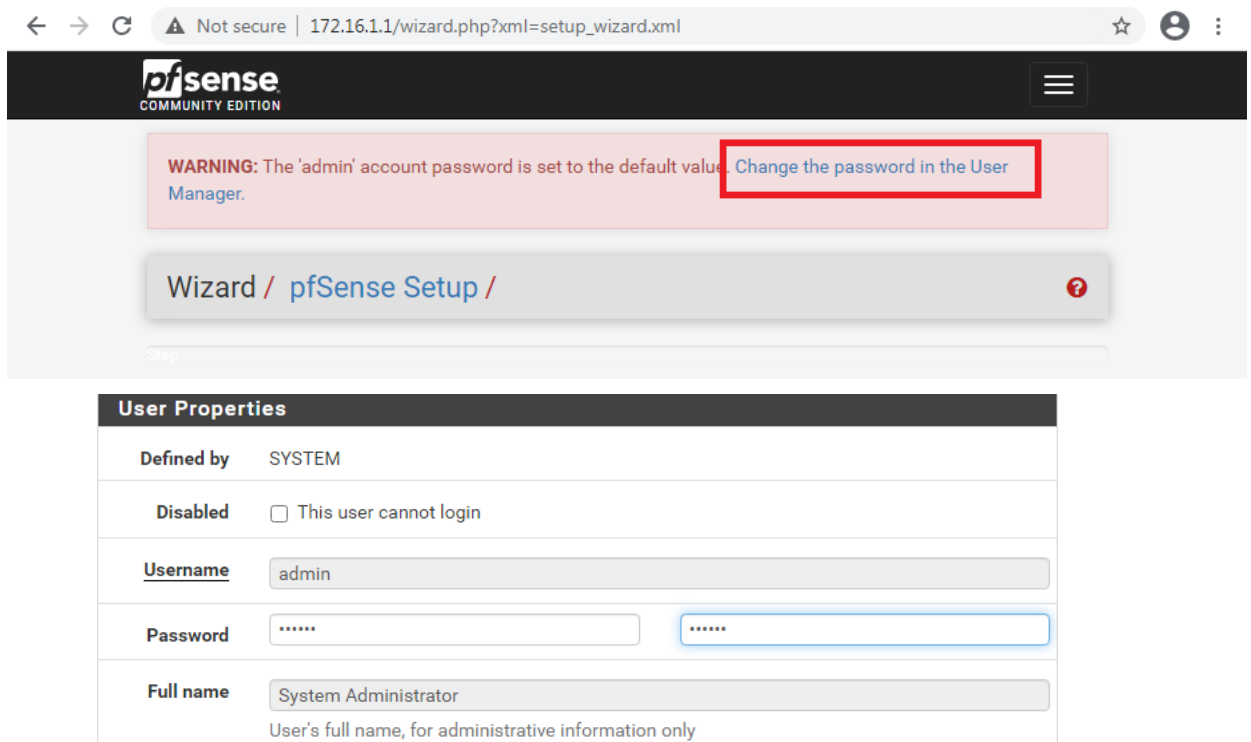
<http://172.16.1.1>



User: admin

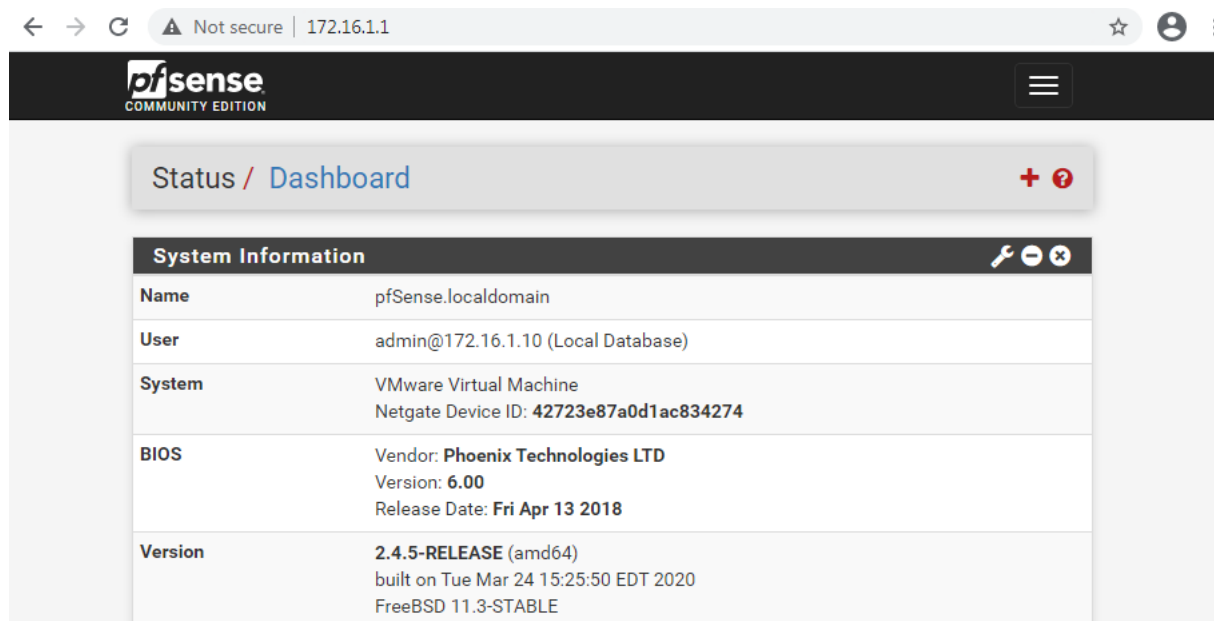
Pass: pfsense

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

Interfaces			
WAN	↑	autoselect	192.168.190.129
LAN	↑	autoselect	172.16.1.1
OPT1	↑	autoselect	10.0.0.1

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.

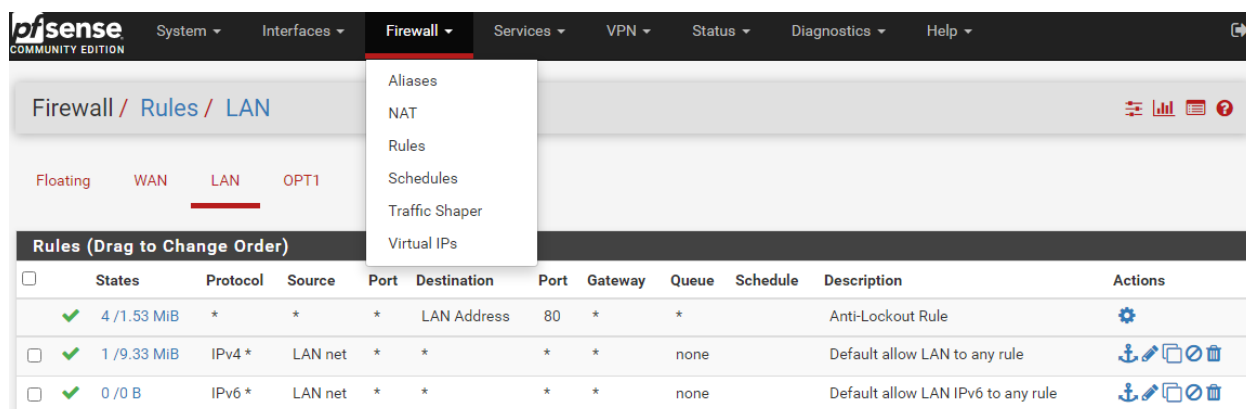
Trong thực tế IP cổng này là IP public là địa chỉ tĩnh.

1.9. Tạo tập luật theo kịch bản

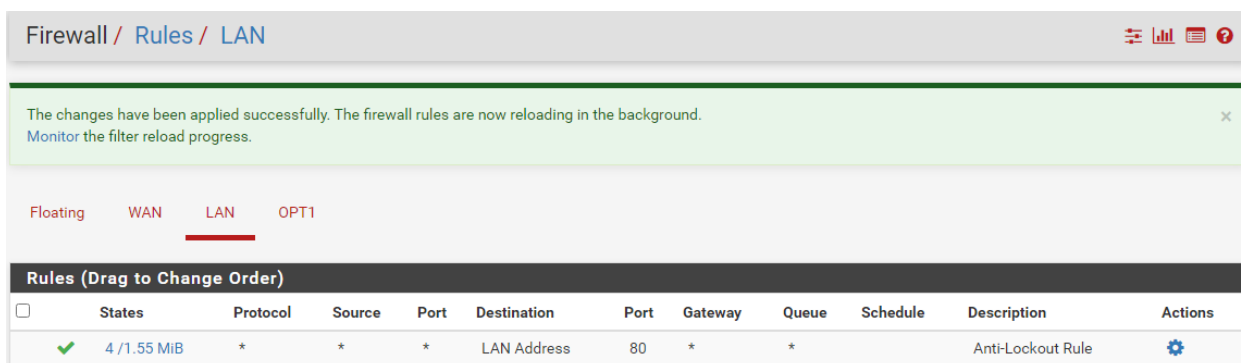
- Kịch bản 0: Xóa các luật mặc định.

Mặc định khi cài đặt xong tường lửa sẽ có các luật mặc định tạo sẵn, những luật này chưa đảm bảo an toàn vì thế cần thiết lập lại từ đầu.

Truy cập theo đường dẫn: Firewall → Rules → LAN



Xóa các luật mặc định, kích vào tùy chọn Apply changes, kết quả.



Lúc này chỉ còn 1 luật mặc định, luật này không thể xóa được vì đây là luật cho quản trị tường lửa.

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

Trước khi thiết lập luật, kiểm tra Ping:

```
C:\Users\admin>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Kết quả đang bị chặn bởi tường lửa.

Chọn Add, giao diện cấu hình luật xuất hiện lựa chọn các thông tin sau:

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP R
whereas with block the packet is dropped silently. In either case, the original pac

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

any

Alternate Host

Datagram conversion error

Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source		
<u>Source</u>	<input type="checkbox"/> Invert match	LAN net

Destination		
<u>Destination</u>	<input type="checkbox"/> Invert match	any

Chọn Save để lưu cấu hình. Kết quả

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 1.77 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	LAN net	*	*	*	*	none			

Ping kiểm tra lại, kết quả:

```
C:\Users\admin>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=268ms TTL=127
Reply from 8.8.8.8: bytes=32 time=28ms TTL=127
Reply from 8.8.8.8: bytes=32 time=27ms TTL=127
Reply from 8.8.8.8: bytes=32 time=28ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 27ms, Maximum = 268ms, Average = 87ms
```

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, cấu hình luật với thông tin như sau;

Edit Firewall Rule	
<u>Action</u>	Pass <small>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP) whereas with block the packet is dropped silently. In either case, the original packet is discarded.</small>
<u>Disabled</u>	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
<u>Interface</u>	LAN <small>Choose the interface from which packets must come to match this rule.</small>
<u>Address Family</u>	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>
<u>Protocol</u>	UDP <small>Choose which IP protocol this rule should match.</small>

Source

Source ☐ Invert match LAN net

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the its default value, **any**.

Destination

Destination ☐ Invert match any

Destination Port Range DNS (53) From Custom To

Specify the destination port or port range for this rule. The "To" field may be left empty if only

Nhấn Save để lưu, và Apply Changes để chạy luật.

Floating

WAN

LAN

OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 1.83 MiB	*	*	*	LAN Address	80	*	*		Anti-Logout Rule	
<input type="checkbox"/>	6 / 71 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	0 / 480 B	IPv4 ICMP	LAN net	*	*	*	*	none			

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

```
C:\Users\admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> facebook.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: facebook.com
Addresses: 2a03:2880:f109:81:face:b00c:0:25de
31.13.75.35
```

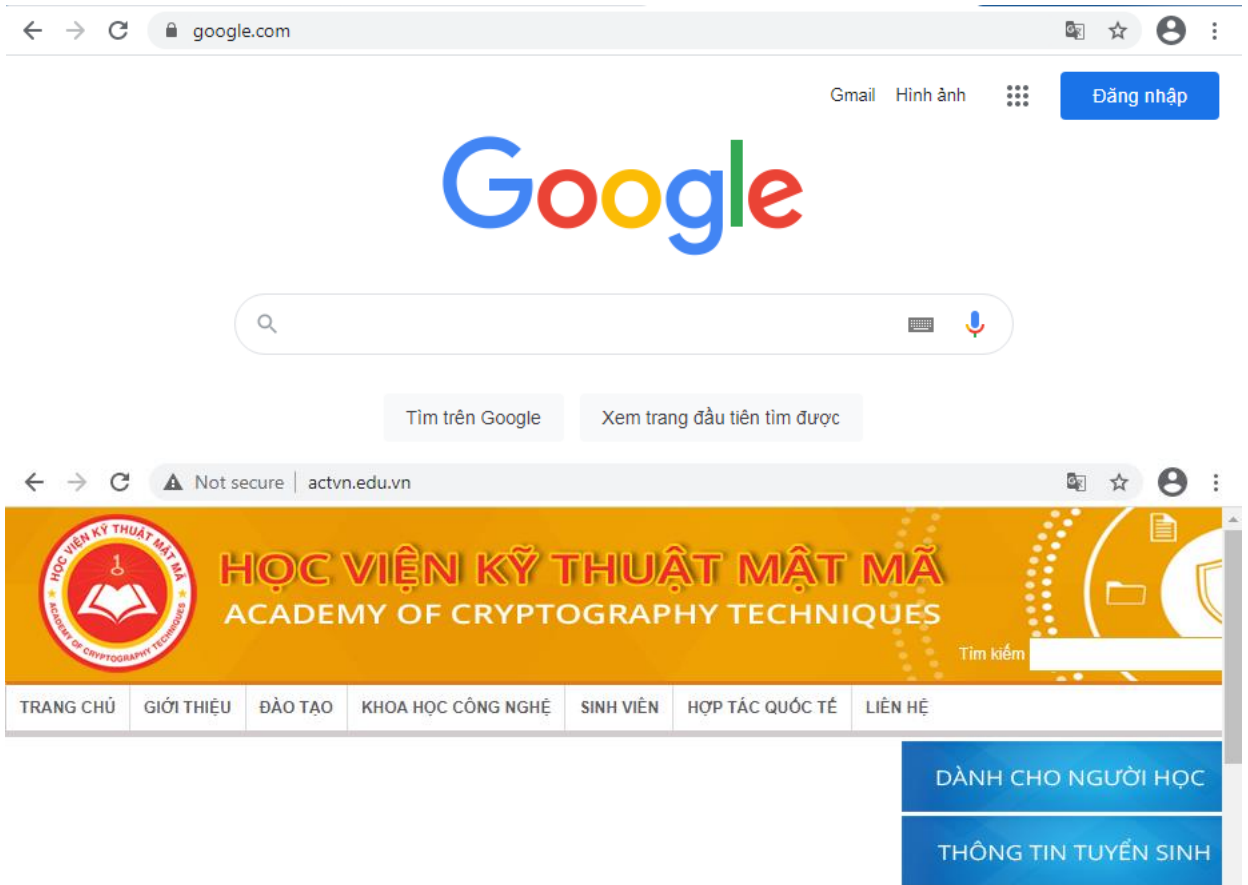
Có kết quả trả về địa chỉ IP tương ứng với tên miền.

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:

Floating WAN LAN OPT1											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 1.91 MIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	68 / 2.92 MiB	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	0 / 82 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	0 / 480 B	IPv4 ICMP any	LAN net	*	*	*	*	none			

Kiểm tra kết quả truy cập website trên Windows 7:



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:

Reserved Networks	
Block private networks and loopback addresses <input type="checkbox"/>	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks <input type="checkbox"/>	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Lưu và thoát.

Vào phần Add để tạo luật với các thông tin như sau:

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP) whereas with block the packet is dropped silently. In either case, the original packet is not sent to the destination.

Disabled

☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port range. Its default value, **any**.

Destination

Destination

☐ Invert match

WAN address

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Specify the destination port or port range for this rule. The "To" field may be left empty if only one port is specified.

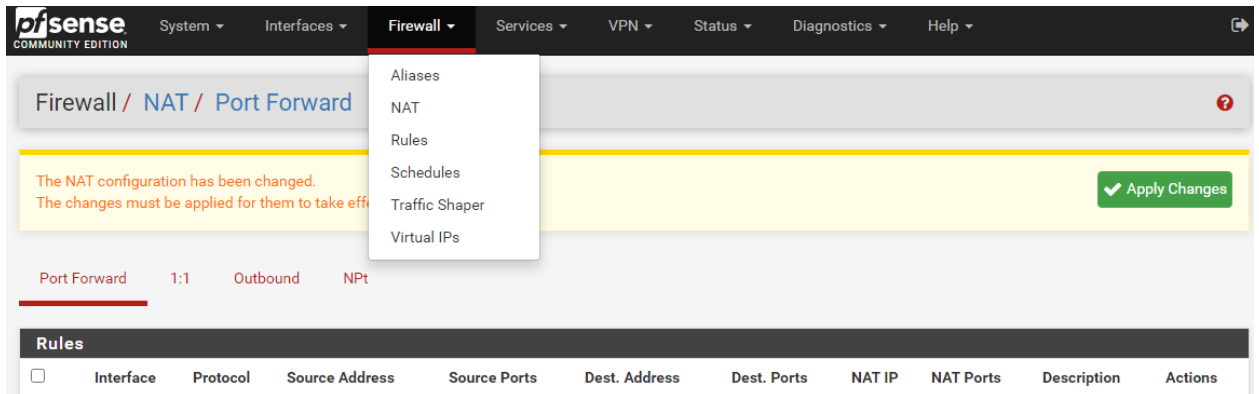
Lưu và thoát.

Kết quả:

Floating	WAN	LAN	OPT1								
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none		Anchor Edit Copy Delete

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:

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match.
Type

Destination port range
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port

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: 192.168.190.129. 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:





Port Forward

1:1

Outbound

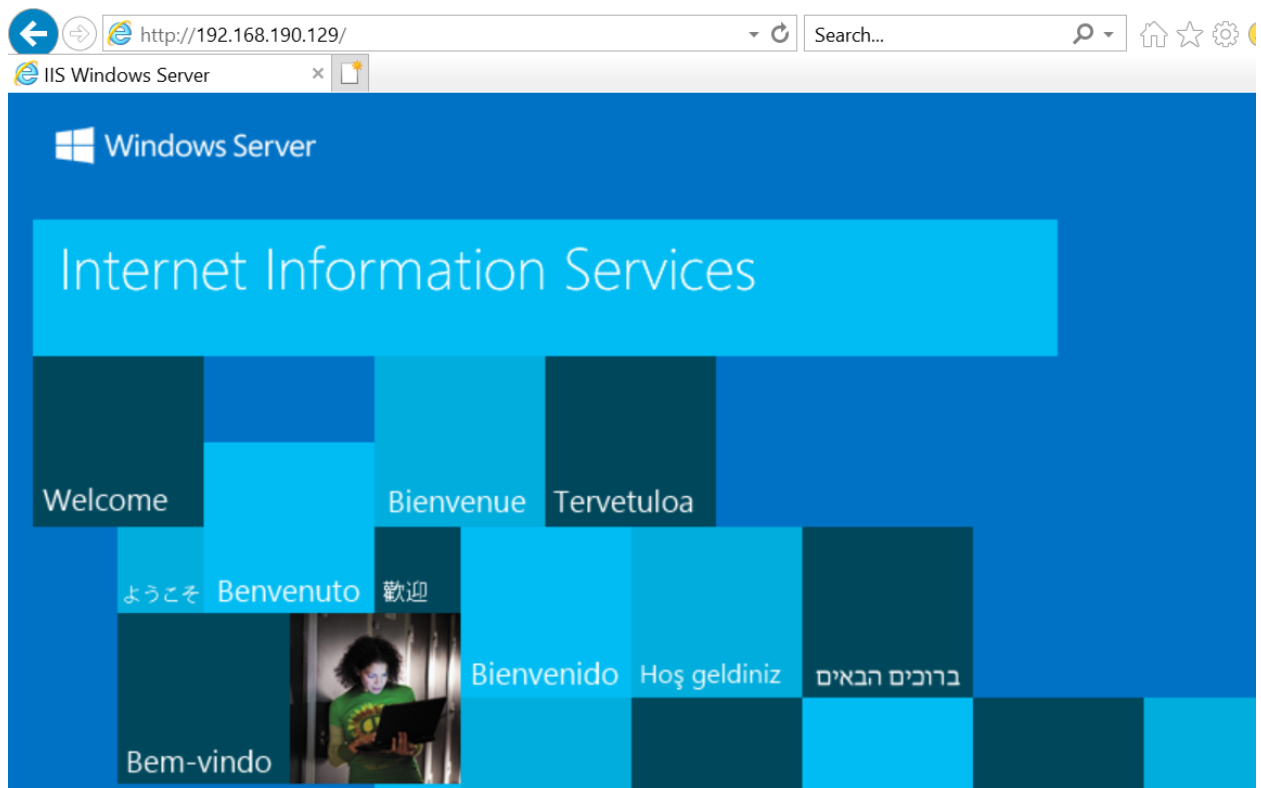
NPt

Rules

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	 WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.20	80 (HTTP)		  

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).

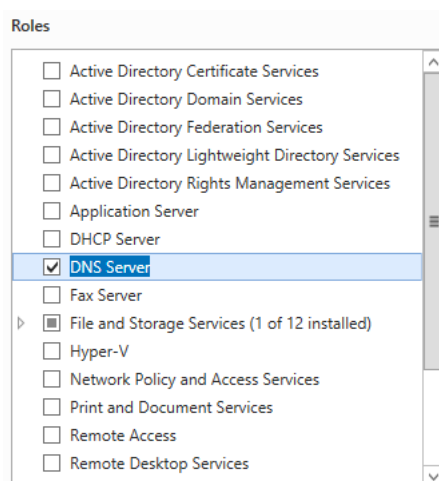


Kết quả thành công.

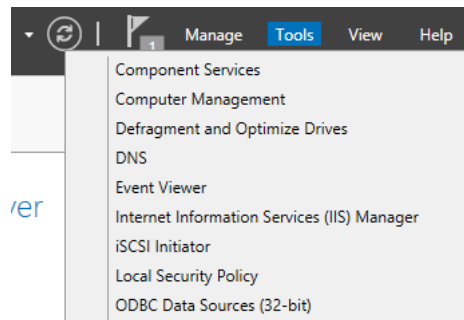
1.9.5. Kịch bản 5: cho phép người dùng trong mạng LAN gửi và nhận mail với người dùng ngoài Internet sử dụng mail server trong DMZ.

- Cài đặt dịch vụ DNS trên máy chủ Windows Server 2012

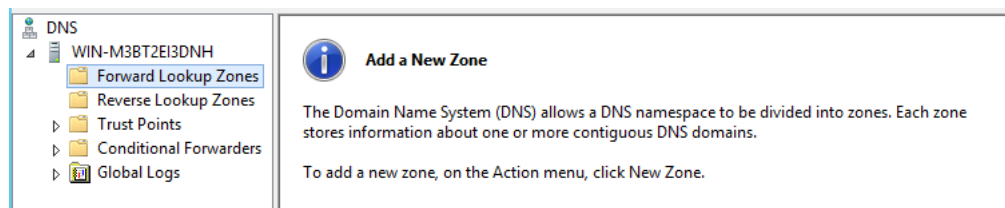
Truy cập vào Server Manager chọn Manage → Add role and feature



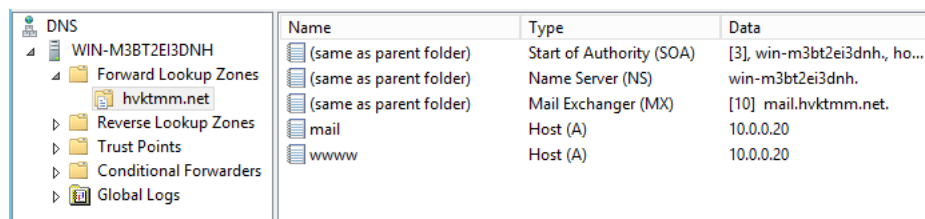
Tích vào dịch vụ DNS để cài đặt. Các tùy chọn tiếp theo để mặc định. Sau khi cài đặt thành công vào Tool để cấu hình cho DNS.



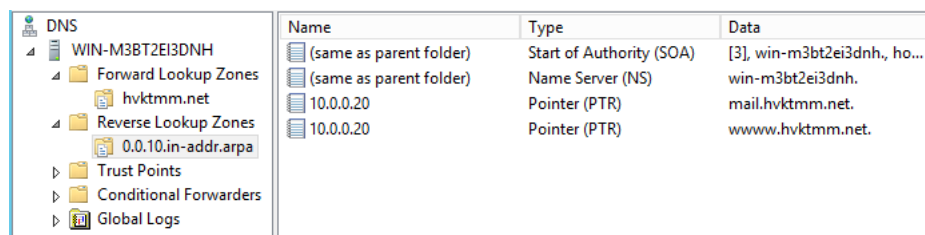
Giao diện quản trị DNS xuất hiện:



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.

☐ Obtain an IP address automatically
☒ Use the following IP address:

IP address:	10 . 0 . 0 . 20
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 0 . 0 . 1

☐ Obtain DNS server address automatically
☒ Use the following DNS server addresses:

Preferred DNS server:	10 . 0 . 0 . 20
Alternate DNS server:	.

Kiểm tra:

```

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server: www.hvktmm.net
Address: 10.0.0.20

> mail.hvktmm.net
Server: www.hvktmm.net
Address: 10.0.0.20

Name: mail.hvktmm.net
Address: 10.0.0.20
>
  
```

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: hvktmm.net

Primary IP DNS: 10.0.0.20

Sau khi cài đặt xong mail server, tạo các tài khoản người dùng mail.

Vào mục Account → new account, với các thông tin

Tương tự tạo tài khoản cho user2.

- Tại máy Windows 7 thiết lập tài khoản cho user1.

Sử dụng phần mềm Thunderbird Setup 31.5.0 làm mail client cho tài khoản user1.

Cài đặt và cấu hình như sau:

Trước tiên phải chuyển IP DNS trên Windows 7 như sau:

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

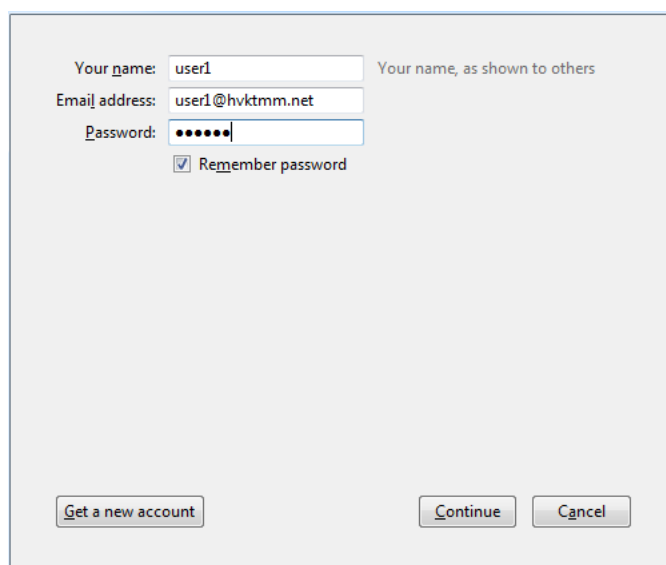
```
C:\Users\admin>nslookup
Default Server: mail.hvktmm.net
Address: 10.0.0.20

> mail.hvktmm.net
Server: mail.hvktmm.net
Address: 10.0.0.20

Name: mail.hvktmm.net
Address: 10.0.0.20
```

Kết quả thành công.

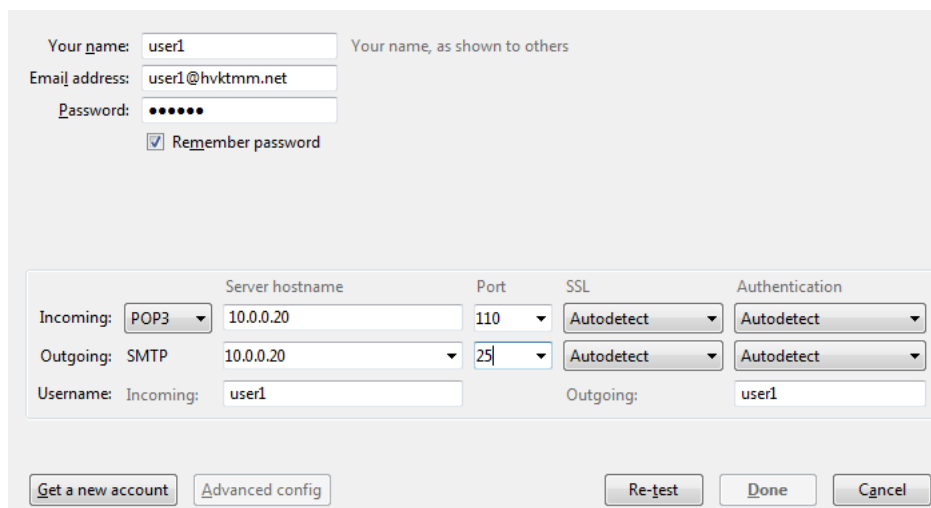
Cài đặt phần mềm Thunderbird, cấu hình như sau:



The image shows the 'Account Setup' dialog box in Thunderbird. It contains the following fields and options:

- Your name: user1 (with a note 'Your name, as shown to others')
- Email address: user1@hvktmm.net
- Password: [masked with dots]
- ☒ Remember password
- Buttons at the bottom: 'Get a new account', 'Continue', and 'Cancel'.

Chọn Continue để tiếp tục, cửa sổ xuất hiện chọn Manual config



The image shows the 'Manual Configuration' dialog box in Thunderbird. It contains the following fields and options:

- Your name: user1 (with a note 'Your name, as shown to others')
- Email address: user1@hvktmm.net
- Password: [masked with dots]
- ☒ Remember password
- Advanced configuration section with the following fields:
 - Incoming: POP3 (dropdown)
 - Outgoing: SMTP (dropdown)
 - Username: Incoming: user1 (text field)
 - Outgoing: user1 (text field)
 - Server hostname: 10.0.0.20 (text field)
 - Port: 110 (dropdown for incoming, 25 for outgoing)
 - SSL: Autodetect (dropdown)
 - Authentication: Autodetect (dropdown)
- Buttons at the bottom: 'Get a new account', 'Advanced config', 'Re-test', 'Done', and 'Cancel'.

Chọn Re-test để kiểm tra kết nối.

Lúc này chương trình sẽ báo lỗi vì tường lửa đang chặn kết nối từ LAN tới DMZ.

- Mở luật trong tường lửa để cho phép kết nối mail (POP3, SMTP) truyền tải thông tin.

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

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	7 / 2.15 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	LAN net	*	OPT1 net	25 (SMTP)	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	LAN net	*	OPT1 net	110 (POP3)	*	none			

Kết quả: mail client truy vấn thành công

Your name: Your name, as shown to others
 Email address:
 Password:
☒ Remember password

The following settings were found by probing the given server

	Server hostname	Port	SSL	Authentication
Incoming: POP3	10.0.0.20	110	None	Normal password
Outgoing: SMTP	10.0.0.20	25	None	Encrypted password

Username: Incoming: Outgoing:

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

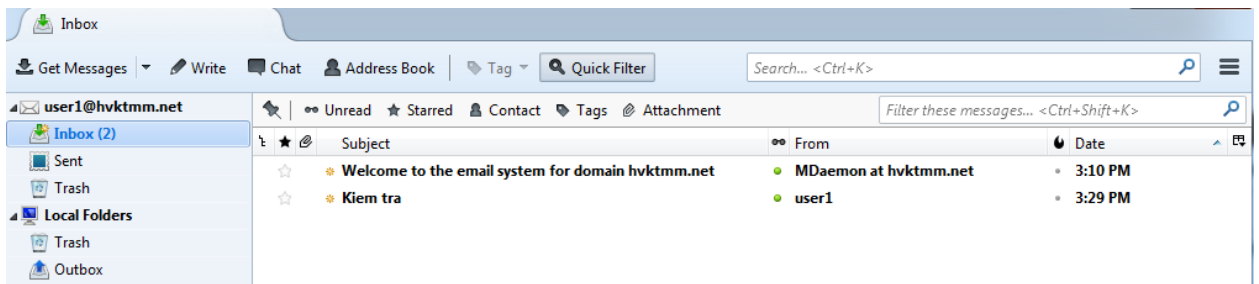
Tại phần mềm mail, với tài khoản user1 gửi và nhận thư cho chính nó để kiểm tra

From: user1 <user1@hvktmm.net> user1@hvktmm.net
 To: user1@hvktmm.net
 Subject: Kiểm tra

Body Text Variable Width

Kiểm tra thu

Kết quả:



Đã gửi và nhận thư thành công.

- Cấu hình luật để Public dịch vụ mail ra Internet:

Floating

WAN

LAN

OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div>✓</div><div>0 / 0 B</div></div>	IPv4 TCP	*	*	WAN address	25 (SMTP)	*	none			<div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0 / 0 B</div></div>	IPv4 TCP	*	*	WAN address	110 (POP3)	*	none			<div><div></div><div></div><div></div><div></div></div>

Cấu hình NAT:

Port Forward

1:1

Outbound

NPt

Rules

<input type="checkbox"/>		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	25 (SMTP)	10.0.0.20	25 (SMTP)	
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	110 (POP3)	10.0.0.20	110 (POP3)	
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	WAN address	80 (HTTP)	10.0.0.20	80 (HTTP)	

- Cấu hình trên máy tính vật lý

Cài đặt phần mềm Thunderbird và thiết lập giống như trong Win7

Your name: Your name, as shown to others

Email address:

Password:

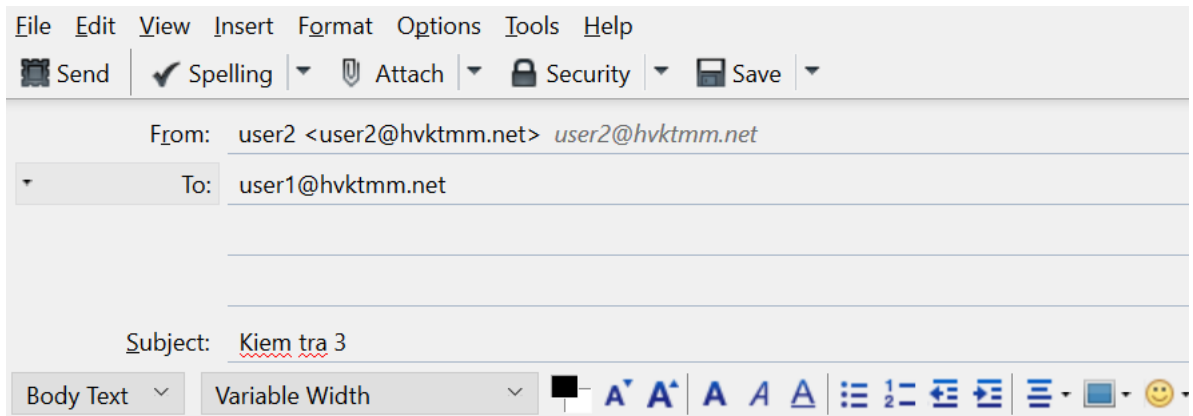
☒ Remember password

The following settings were found by probing the given server

	Server hostname	Port	SSL	Authentication
Incoming: POP3	<input type="text" value="192.168.190.129"/>	<input type="text" value="110"/>	<input type="text" value="None"/>	<input type="text" value="Normal password"/>
Outgoing: SMTP	<input type="text" value="192.168.190.129"/>	<input type="text" value="25"/>	<input type="text" value="None"/>	<input type="text" value="Encrypted password"/>
Username: Incoming:	<input type="text" value="user2"/>		Outgoing:	<input type="text" value="user2"/>

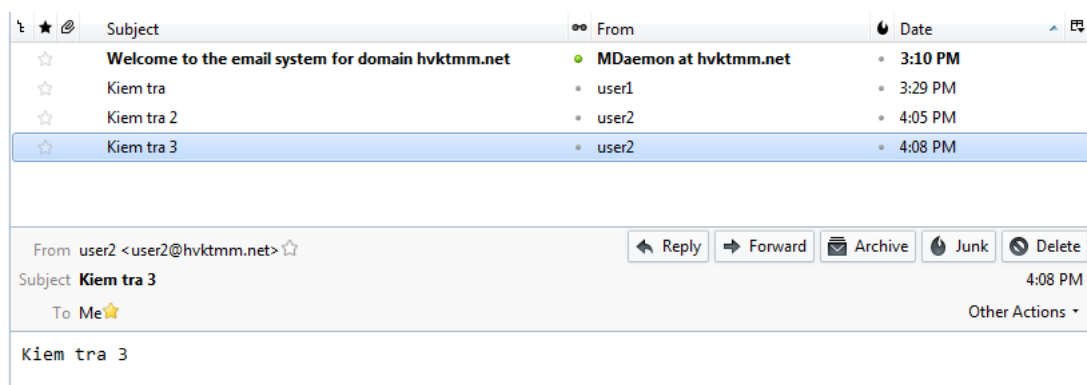
Kết quả thành công. Done để đóng cửa sổ cấu hình.

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



Kiem tra 3

Truy cập vào mail client trên Win 7 để kiểm tra:



Kết quả người dùng user1 trên Windows 7 đã nhận được mail từ người dùng user2 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.

Kết thúc bài thực hành./.