LAB7 – FIREWALL

***Chuẩn bị:***

1. *Truy cập link bằng trình duyệt web:* [*https://drive.google.com/drive/folders/1LjCOeC3ad6GoKQHoipIVDj3je5RBxk6j?usp=sharing*](https://drive.google.com/drive/folders/1LjCOeC3ad6GoKQHoipIVDj3je5RBxk6j?usp=sharing)

*Tải các tập tin sau:*

+ VirtualBox Machine\Windows Client\Windows 10-LTSB 32-Bit Mod.20201111.ova

+ VirtualBox Machine\Router\RouterOS 5.25.ova

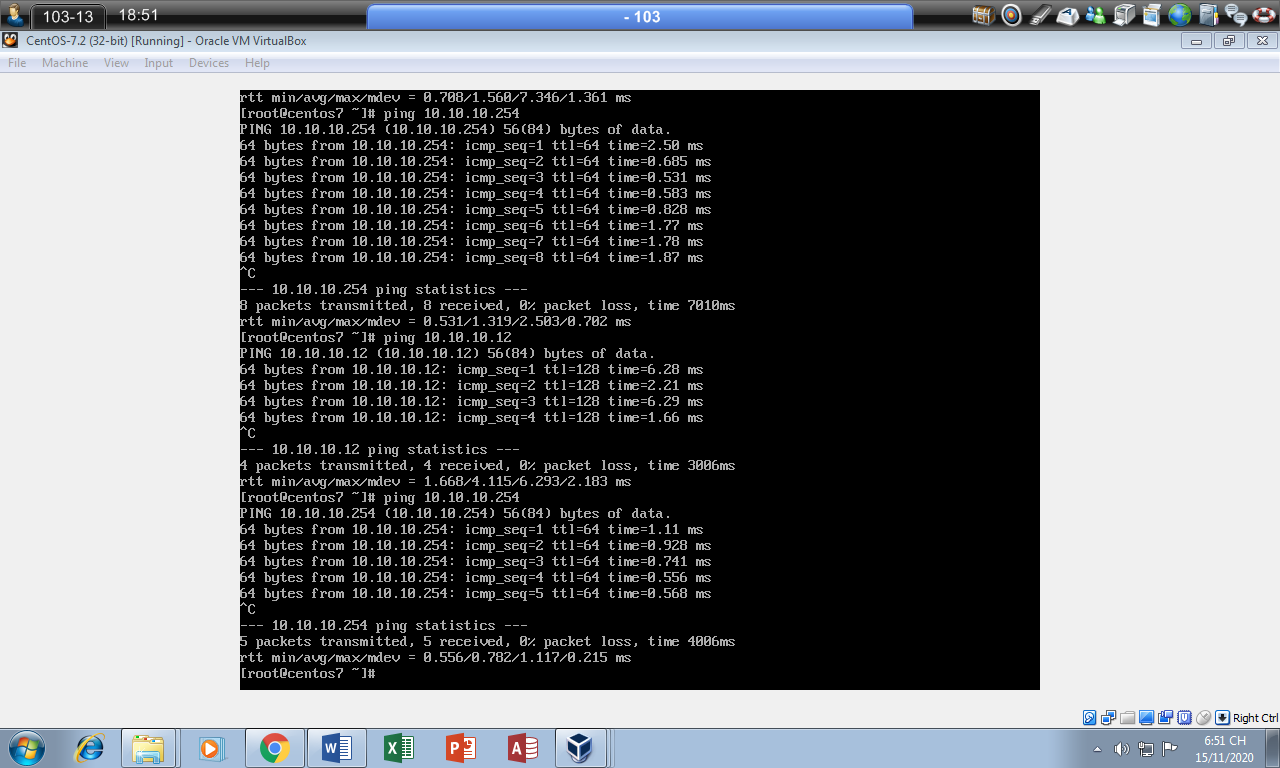
+ VirtualBox Machine\Linux\CentOS-7.2 32-Bit.20201021.ova

1. *Thực hiện:*

* Cài đặt VirtualBox-5.2.44-139111-Win.exe (Vbox)
* Import các tập tin .ova thành các máy ảo, bỏ qua audio và usb khi import
* Set tên máy ảo, RAM và Network Adapter:
  + Windows 10: 1GB – Host Only
  + RouterOS 5.25: 256MB – Host Only + Host Only
  + CentOS 7.2: 512MB – Host Only

Lưu ý: đối với máy RAM 2GB tất cả RAM khai báo giảm ½

* Khởi động lại 3 Máy ảo lần lượt đảm bảo 2 máy ảo Windows 10 và CentOS ping thấy nhau



# Firewall on Router

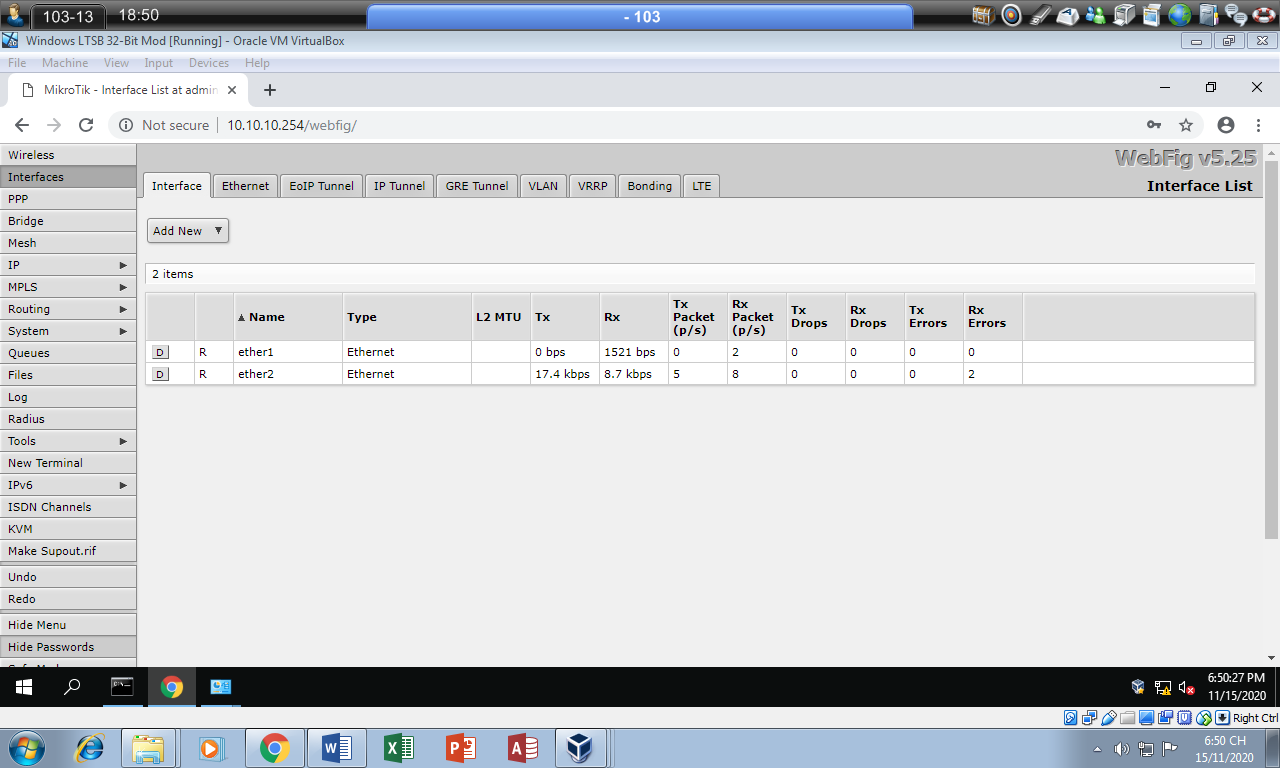
**Mô tả**

Mikrotik RouterOS là hệ điều hành được xây dựng cho kiến trúc phần cứng RouterBoard của Mikrotik. Hệ điều hành RouterOS được xây dựng với đầy đủ các chức năng như định tuyến (router), tường lữa (firewall), quản lý băng thông, AP, liên kết mạng trục, quản lý Truy cập Mạng Công cộng (có dây hoặc không dây) , thiết lập VPN, ..

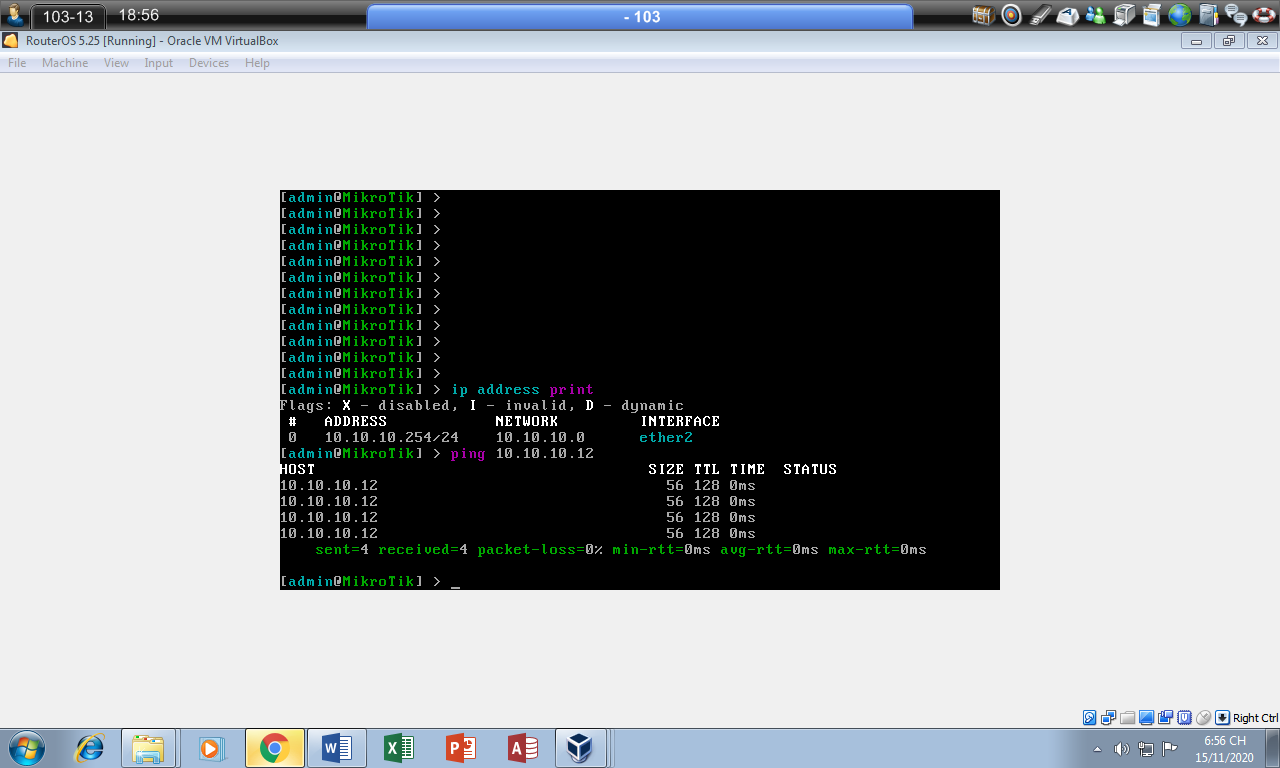
RouterOS là một hệ điều hành chuẩn dựa trên nền Linux v2.6, cung cấp tất cả những tính năng của bộ định tuyến cộng với khả năng cài đặt nhanh chóng, đơn giản và giao diện sử dụng dễ dàng.

**Thực hiện**

1.1 Truy cập web quản trị RouterOS



1.2 Kiểm tra IP eth2 cùng lớp máy ảo windows 10 và ping thông



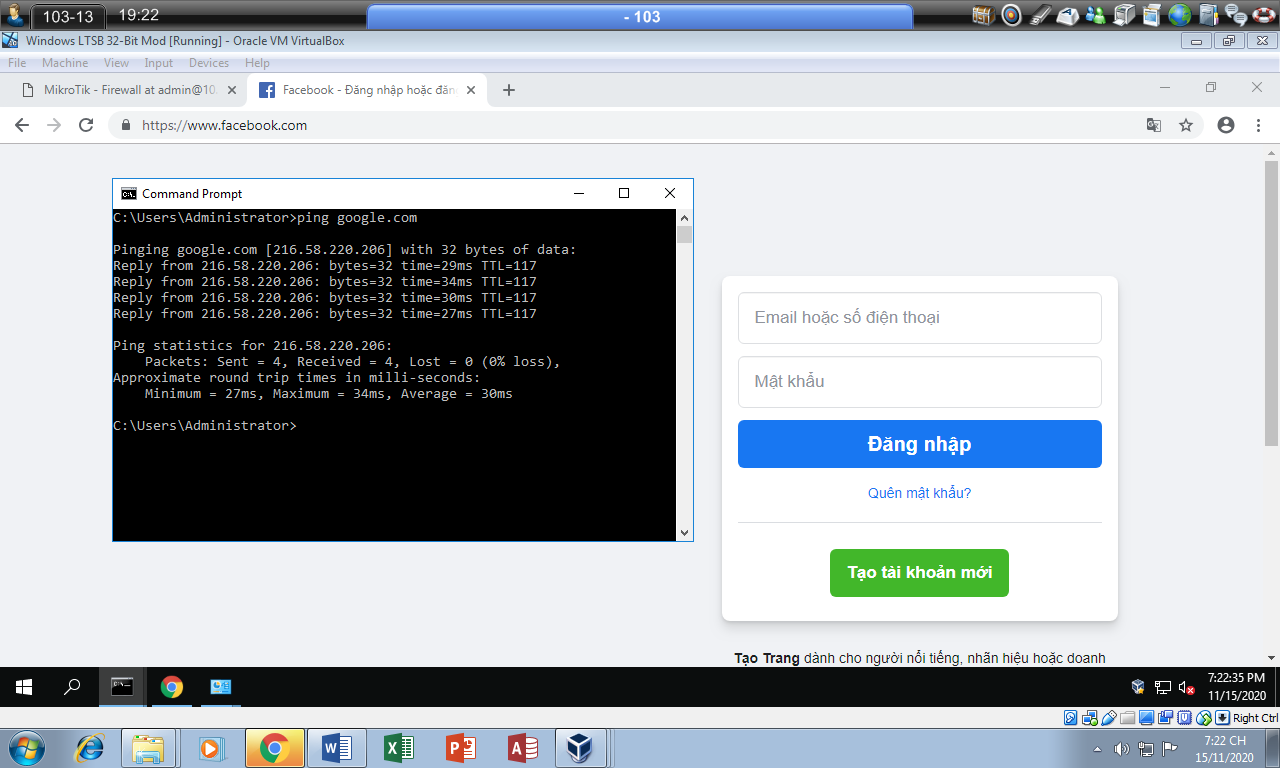
* ip address print

1.3 Chuyển đổi Network Adapter 1 (tương ứng eth1 của RouterOS) sang NAT , NAT port trên Router OS để máy ảo windows 10 truy cập được Internet

-> ip -> dhcp client -> add new -> Enable [Check] -> Interface: eth1

-> ip -> firewall -> nat -> add new -> Enable [Check] -> chain: srcnat -> out interface: eth1 -> Action: masquerade

-> ip -> dns -> server: 8.8.8.8

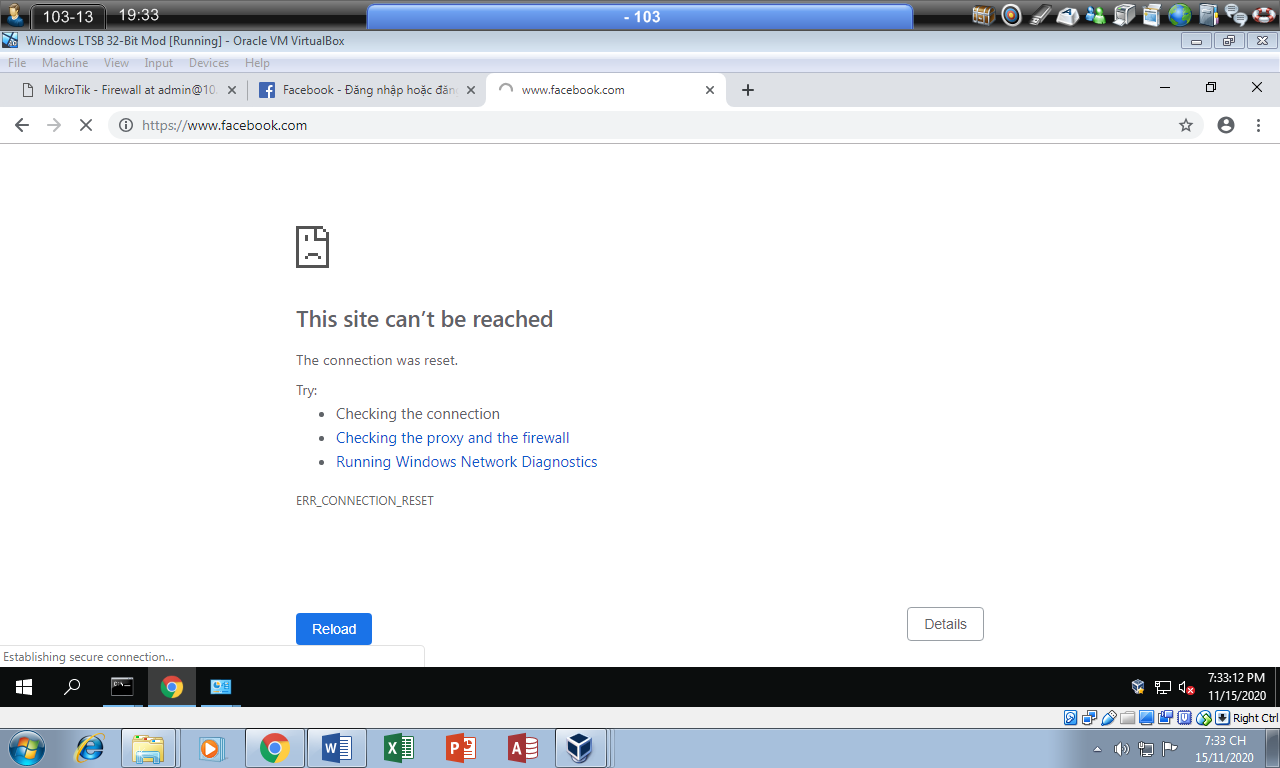


* ip dhcp-client add disabled=no interface=eth1
* ip firewall nat add action=masquerade chain=srcnat out-interface=eth1
* ip dns set servers=8.8.8.8

1.4 Chặn truy cập facebook.com đối với máy ảo windows 10

-> ip -> firewall -> l7 protocol -> add new -> Name: BlockFB -> Regexp: ^.+(facebook.com).\*$

-> ip -> firewall -> filter rules -> add new -> Enable [check] -> Chain: forward -> protocol: tcp -> dst port:80,443 -> layer7 protocol: blockfb > action: drop



# Firewall on Windows

# Firewall on Linux

Iptables là một ứng dụng tường lửa dựa trên lọc gói rất mạnh, miễn phí và có sẵn trên Linux. Cơ chế lọc gói tin của Iptable được xây dựng dựa trên 3 thành phần cơ bản đó là table, chain và target. Nói đơn giản, table là một xử lý các gói tin theo những cách cụ thể. Nếu không chỉ định cụ thể thì mặc định là chúng ta sẽ làm việc với filter table, ngoài ra còn có các bảng khác.

Mỗi bảng sẽ được gắn thêm các chain. Việc gắn thêm chain vào table cho phép xử lý gói tin ở những giai đoạn khác nhau, ví dụ chúng ta có thể xử lý gói tin ngay khi gói tin vừa đến interface hay xử lý các gói tin trước khi các gói này được đẩy ra interface. Bạn có thể tạo ra rule rất cụ thể, ví dụ gói tin đó đến từ port nào, đến từ IP nào sau đó chỉ định hành động (TARGET) sẽ áp dụng với gói tin này.

Khi có một gói tin đến hoặc gói tin đi Iptable sẽ so sánh với từng rule trong một chain. Khi một gói tin giống với rule đặt ra Iptable sẽ thực hiện hành động ứng với rule đó. Nhưng nếu gói tin không khớp với bất cứ rule nào thuộc chain, Iptable sẽ áp dụng "default policy" cho gói tin đó. Mặc định "default policy" của các chain là cho phép gói tin.

Một số lệnh cơ bản

* Tạo một rule mới

iptables -A INPUT -i lo -j ACCEPT

Lệnh này có nghĩa là:

-A INPUT: khai báo kiểu kết nối sẽ được áp dụng (A nghĩa là Append).

-i lo: Khai báo thiết bị mạng được áp dụng (i nghĩa là Interface).

-j ACCEPT: khai báo hành động sẽ được áp dụng cho quy tắc này (j nghĩa là Jump).

Gõ lại lệnh iptables -L -v bạn sẽ thấy 1 rule mới xuất hiện

after-created-iptables-rule

Sau khi thêm mới hoặc thay đổi bất cứ gì, hãy gõ lệnh lưu và khởi động lại iptables để áp đặt các thay đổi.

service iptables save

service iptables restart

Tiếp tục bây giờ chúng ta thêm một rule mới để cho phép lưu lại các kết nối hiện tại để tránh hiện tượng tự block bạn ra khỏi máy chủ.

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Cho phép các cổng được truy cập từ bên ngoài vào qua giao thức tcp: SSH(22), HTTP(80), HTTPS(443)

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

-p tcp: Giao thức được áp dụng (tcp, udp, all)

--dport 22: Cổng cho phép áp dụng. 22 là cho SSH

Và cuối cùng, chặn toàn bộ các kết nối truy cập từ bên ngoài vào không thỏa mãn những rule trên. Tương ứng với rule 5 ở trên.

iptables -A INPUT -j DROP

Đến đây cơ bản bạn đã có đủ các qui tắt cần thiết để thiết lập các chính sách của bạn cho hệ thống,

Bổ sung một rule mới

Nếu bạn muốn chèn 1 rule mới vào 1 vị trí (hàng) nào đó, ví dụ là vị trí thứ 2. Thì bạn hãy thay tham số -A table tham số INSERT -I.

iptables -I INPUT 2 -p tcp --dport 8080 -j ACCEPT

Xóa 1 rule

Để xóa 1 rule mà bạn đã tạo ra tại vị trí 4, ta sẽ sử dụng tham số -D

iptables -D INPUT 4

Xóa toàn bộ các rule chứa hành động DROP có trong iptables:

iptables -D INPUT -j DROP