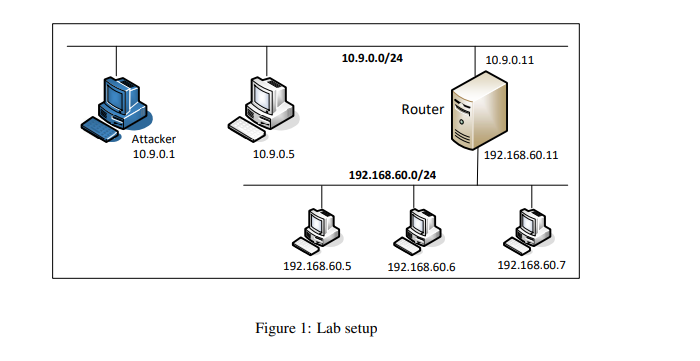
Task 3: Connection Tracking and Stateful Firewall

Task 3.A: Experiment with the Connection Tracking



* Mô hình mạng sử dụng trong bài lab
* ICMP Experiment

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Đầu tiên ta chạy lệnh ping 192.168.60.5

Ảnh có chứa văn bản

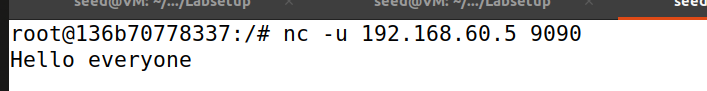
Mô tả được tạo tự động

* Không như TCP ICMP không có kết nối
* Sau đó qua router và chạy lệnh conntrack -L 1 vài lần
* Ta thấy ICMP connection state được giữa từ 26 giảm dần là thời gian
* UDP Experiment

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bên máy Host1 ta chạy lệnh nc -lu 9090



* Bên HostA ta dùng lệnh nc -u 192.168.60.5 9090
* Sau đó gõ bất kỳ và nhấn gửi

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thấy timer không thay đổi chỉ có sequence number thì giảm
* Và khi ta hủy kết nối giữa 2 máy thì thì nc giữa 2 máy cũng bị hủy
* TCP Experiment

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bên máy Host1 ta dùng lệnh nc -l 9090 để mở kết nối tcp

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau đó bên HostA ta kết nối vào IP của máy Host1 qua cổng 9090
* Sau đó gõ bất kỳ và ấn gửi

Ảnh có chứa bàn

Mô tả được tạo tự động

* Bên router ta dùng lệnh conntrack -L để xem thông tin
* Ta thấy lần này cont time của conntrack và sequence number thì giảm xuống thì thay đổi

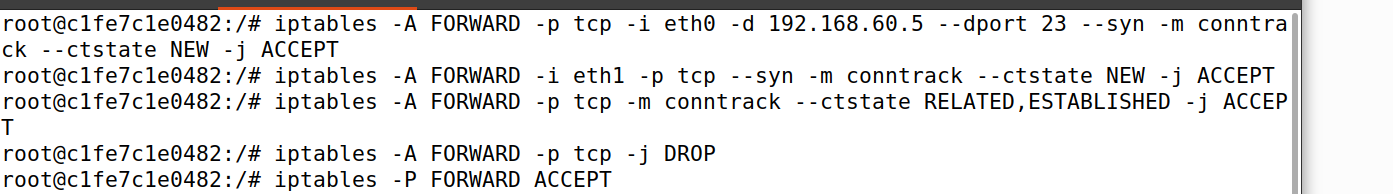
Ảnh có chứa văn bản

Mô tả được tạo tự động

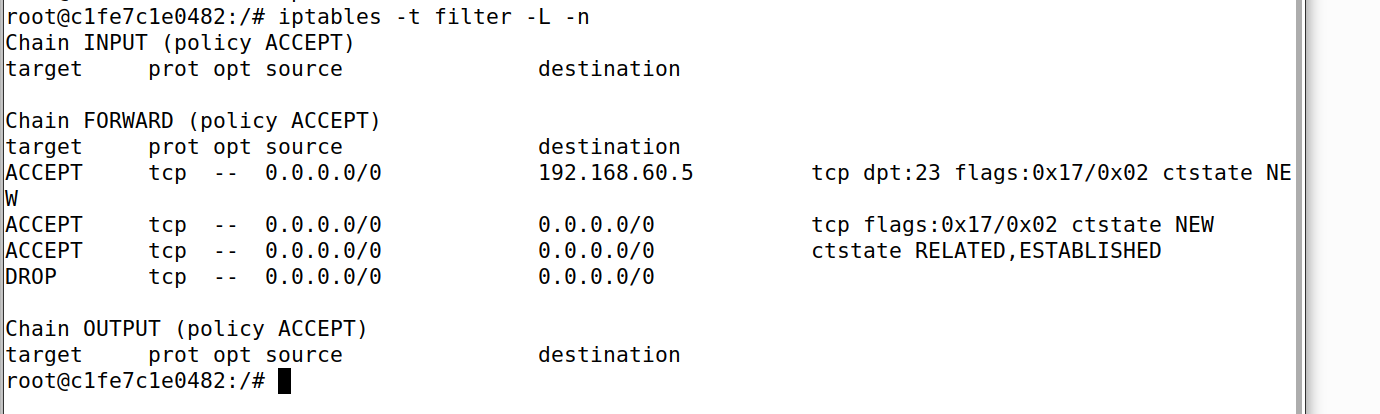
* Sau khi đóng kết nối bên Host1 thì bên router trạng thái đã trở thành CLOSE\_WAIT và timer giảm dần
* Khi giảm về 0 thì nó sẽ ngắt kết nối

Task 3.B: Setting Up a Stateful Firewall

* Tại task này ta sẽ setup cho tuồng lửa



* Chạy những lệnh như trên



* Sau đó ta dùng lệnh iptables -t filter -L -n để xem rule của tường lửa ta đã thiết lập

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bên HostA ta dùng lệnh telnet 192.168.60.5 để kết nối tới server và nó được

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sau đó ta thử kết nối với 192.168.60.6 nhưng không được
* Vì ta đã thiết lập tường lửa các máy bên ngoài internet chỉ có thể kết nối tới 192.168.60.5

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bên Host2 ta kết nối telnet 192.168.60.5 và kết nối được
* Nghĩa là các internet host có thể kết nối nội bộ tới internet server

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta đã define firewall rule để cho phép máy chủ nội bộ kết nối máy chủ bên ngoài
* Stateless firewall còn được gọi là access control list và không lưu thông tin về trạng thái kết nối
* Trong khi statefull firewall luôn theo dõi trạng thái của các kết nối mạng
* Khi 1 trả lời 1 loại lưu lương truy cập được phê duyệt bởi tường lửa trạng thái nó sẽ được lưu vào bảng trạng thái