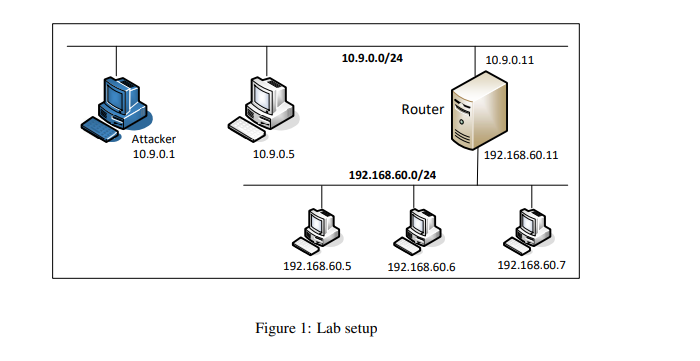
Task 3: Connection Tracking and Stateful Firewall

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

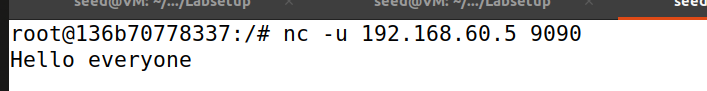
Mô tả được tạo tự động

* 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

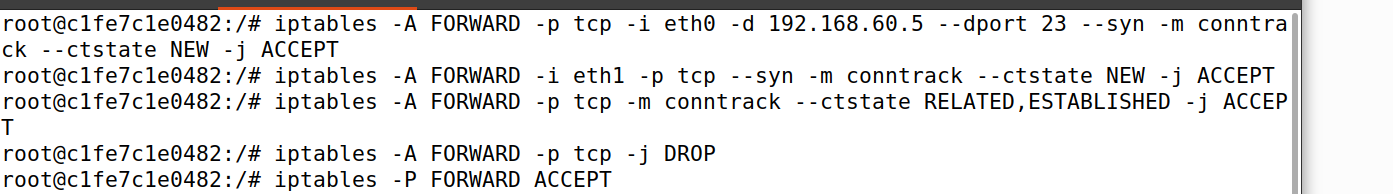
Ảnh có chứa văn bản

Mô tả được tạo tự động

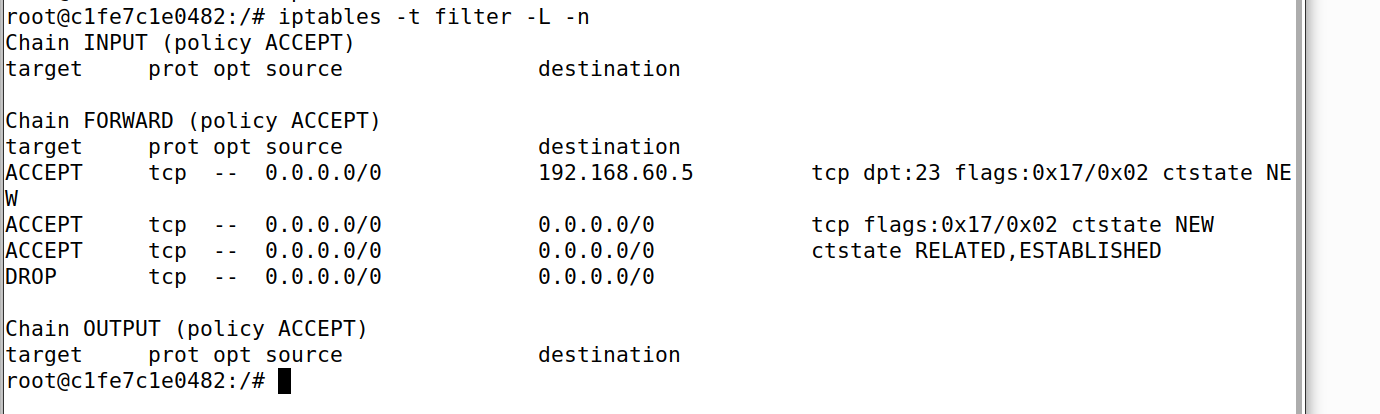
* Sau khi đóng kết nối bên Host1 thì bên router trạng thái đã trở thành CLOSE\_WAIT và timer giảm dần
* Khi giảm về 0 thì nó sẽ ngắt kết nối

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

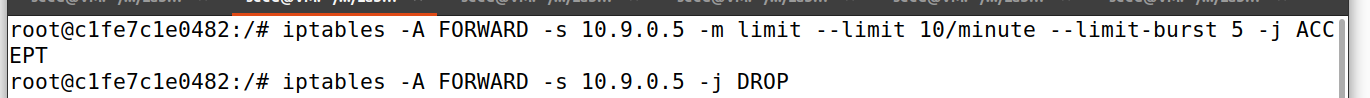
Ảnh có chứa văn bản

Mô tả được tạo tự động

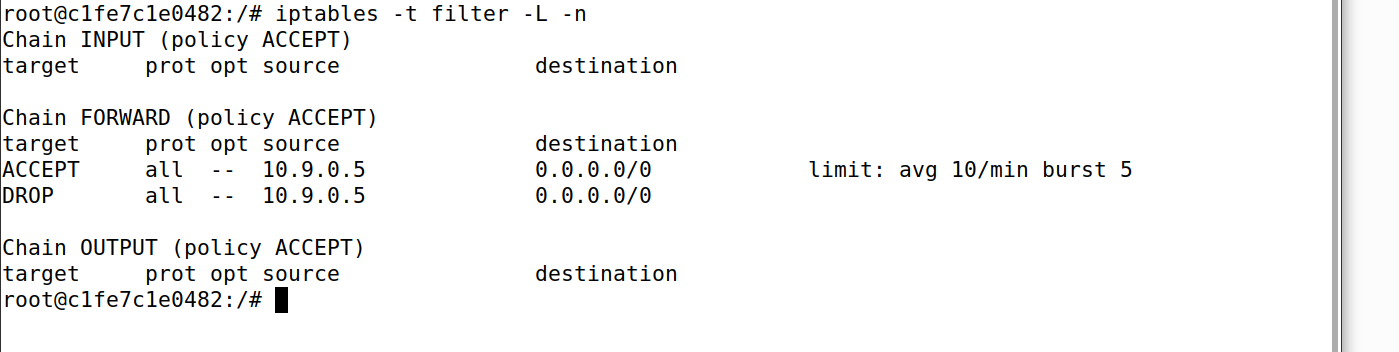
* Ta đã define firewall rule để cho phép máy chủ nội bộ kết nối máy chủ bên ngoài
* Stateless firewall còn được gọi là access control list và không lưu thông tin về trạng thái kết nối
* Trong khi statefull firewall luôn theo dõi trạng thái của các kết nối mạng
* Khi 1 trả lời 1 loại lưu lương truy cập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

Task 4: Limiting Network Traffic

* Trong task này ta sẽ giới hạn số lượng packet qua tường lửa sử dụng limit module trong iptables



* Thực thi các lệnh như trên



* Các rule ta thiết lập trong iptables

Ảnh có chứa bàn

Mô tả được tạo tự động

* Ở HostA ta ping tới máy 192.168.60.5 ta thấy có 13 packets được gửi đi nhưng chỉ có 7 được nhận vì ta đã giới hạn chỉ có 10 packet/phút

Ảnh có chứa bàn

Mô tả được tạo tự động

* Bên Host2 ta ping thử 192.168.60.5 và thấy các gói được gửi đi đều nhận được vì ta không giới hạn ở Host2
* Vì ta chỉ giới hạn từ các host bên ngoài và cho phép mọi thứ ở host bên trong

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi ta chỉ chạy lệnh đầu để thiết lập rule cho iptables

Ảnh có chứa văn bản, bàn

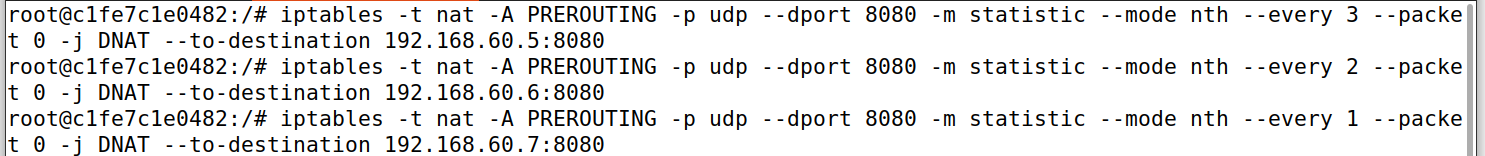
Mô tả được tạo tự động

* Bên HostA ta ping 192.168.60.5 tất cả các gói gửi đi đều nhận được và không có gói nào bị mất
* Ta đã không thiết lập rule để drop các gói bị giới hạn nên HostA vẫn gửi và nhận các gói bình thường

Task 5: Load Balancing

Using the nth mode (round-robin)

* Trong task này ta sẽ dùng iptables để cân bằng tải 3 UDP server chạy internal network



* Thực hiện các command trên để thiếp lập rule cho các Host1, Host2, và Host3
* Ta đã set rule áp dụng chó các gói UDP sẽ đến cổng 8080
* Chế độ nth mode được sử dụng. Nó thực hiện chính sách cân bằng tải round-robin. Cứ 3 gói(tức là gói đầu tiên), thay đổi địa chỉ IP đích và số cổng tương ứng là 192.168.60.5 và 8080. Các gói được sửa đổi sẹ tiếp tực được gửi

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Iptables entries

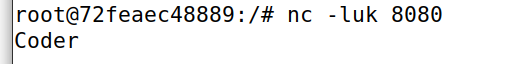


* Bên HostA ta mở kết nối UDP bằng nc -luk 8080 và làm tương tự bên Host2, Host3

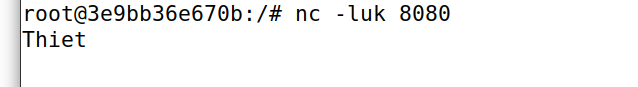
Ảnh có chứa văn bản

Mô tả được tạo tự động

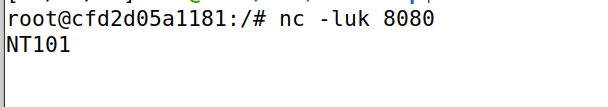
* Sau đó bên HostA ta dùng nc -u 10.9.0.11 8080 sau đó nhập “Coder” chờ 30 giây và nhập “Thiet” và chờ 30 giây nhập “NT101”



* Bên Host1 ta nhân dược “Coder”



* Bên Host2 ta nhận được “Thiet”



* Bên Host3 ta nhận được “NT101”

Ảnh có chứa văn bản

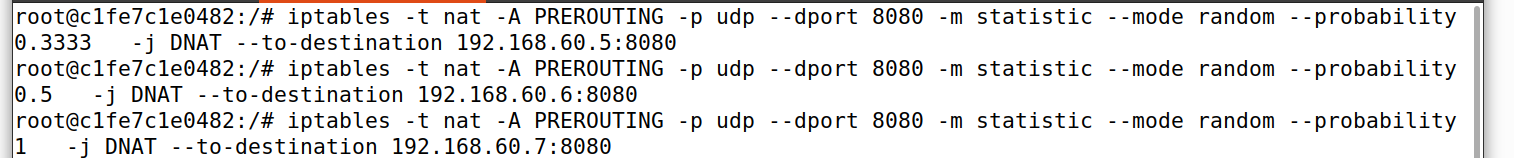
Mô tả được tạo tự động

* Nếu ta nhập liên tiếp và không đợi 30s thì nó sẽ được nhận ở cùng 1 Host

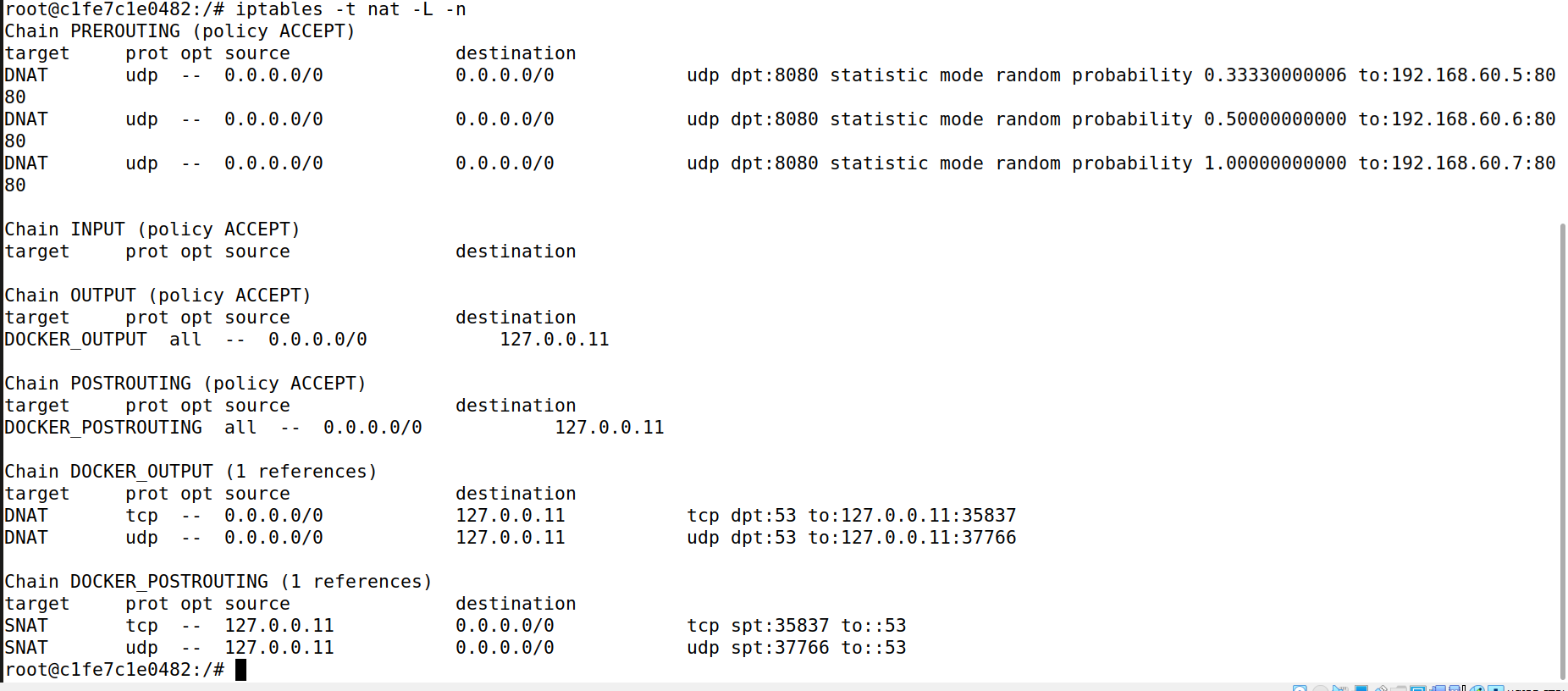
Ảnh có chứa văn bản

Mô tả được tạo tự động

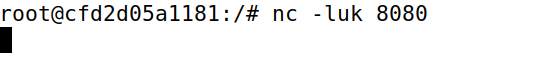
Using the random mode



* Thực hiện các command như trên



* Nó sẽ liệt kê các mục có giá trị sác xuất lần lượt là 0.33 ở ip 192.168.60.5, 0.5 ở ip 192.168.60.6, 1.0 ở ip 192.168.60.7



* Sau đó ta chạy lạy các kết nối UDP ở các Host

Ảnh có chứa văn bản

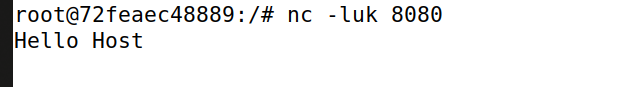
Mô tả được tạo tự động

* Ở HostA ta gửi thử các gói tin

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Thấy ở Host2 nhận được cả 3 gói vì xác xuất là 0.5 khá lớn



* Và Host1 có xác xuất 0.333 cũng nhận được gói tin

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta đã gửi khá nhiều gói tin nhưng chỉ có Host1 nhận được

Ảnh có chứa văn bản

Mô tả được tạo tự động

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Host3 vẫn chưa nhận được gói tin nào