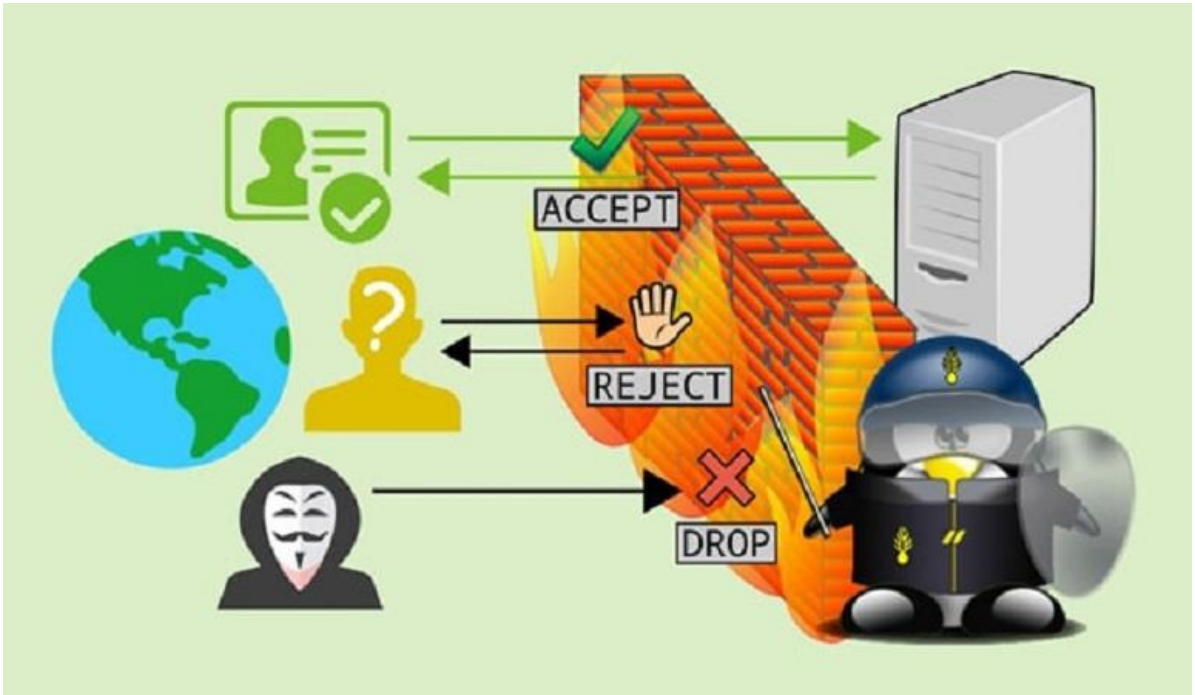
LÝ THUYẾT VỀ IPTABLES

I. Iptables là gì?

- IP talbes là một tiện ích dòng lệnh để cấu hình các quy tắc tường lửa trên hệ điều hành Linux. Nó cho phép thiết lập các quy tắc cho lưu lượng truy cập mạng vào ra, dựa trên các tiêu chí như IP nguồn/đích, giao thức, cổng kết nối.
- Khi sử dụng máy chủ, Iptables sẽ tiến hành thực thi tốt nhất nhiệm vụ ngăn chặn các truy cập không hợp lệ bằng cách sử dụng Netfilter. Phần Netfilter ở bên trong nhân Linux. Phần còn lại là Iptables nằm ở bên ngoài. Vì vậy sự hiện diện của Iptables chính là hệ thống giao tiếp với người dùng. Sau đó đẩy các luật của người dùng vào cho Netfilter xử lý.

Netfilter chịu trách nhiệm lọc các gói dữ liệu ở mức IP Netfilter làm việc trực tiếp trong nhân, nhanh và giảm tốc độ của hệ thống. Iptables chỉ là Interface cho Netfilter.

Trong đó tường lửa quyết định các packet nào được phép đi vào hay đi ra khỏi hệ thống. Các Packet ở bất kỳ Network nào cũng đều giao tiếp bằng cách sử dụng các cổng port. Để quyết định Port nào được phép kết nối từ bên ngoài là nhiệm vụ của Tường lửa



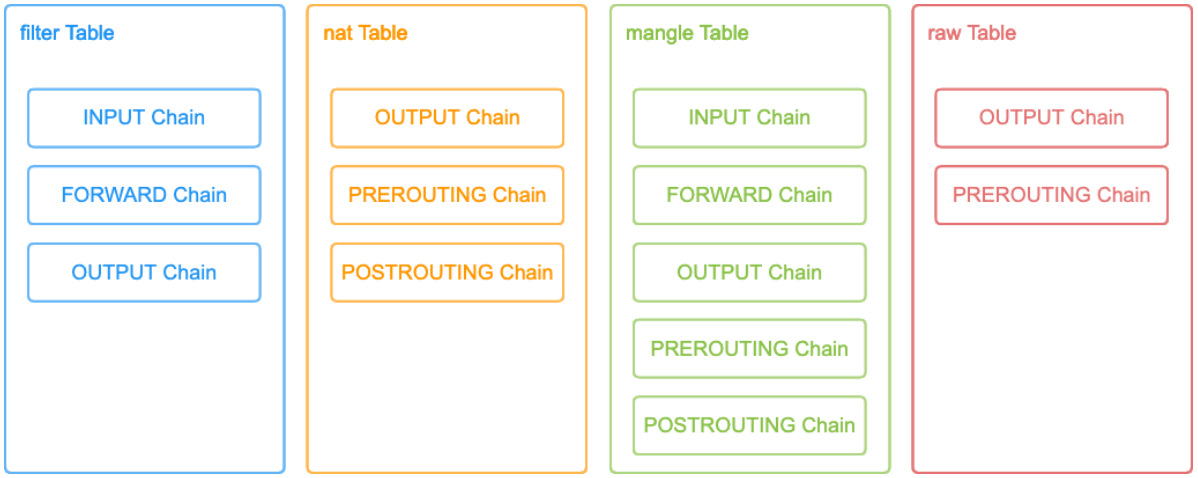
II. Ba thành phần cơ bản của Iptables:

- Iptables gồm 3 thành phần cơ bản là:

+ Tables - là các bảng trong iptables
+ Chains - là các chuỗi luật trong iptables
+ Targets - là các hành động đáp ứng của iptables

1. **Bảng trong iptables:**

- Tables là các bảng trong iptables, xử lý gói tin theo những cách cụ thể khác nhau. Nếu không được chỉ định thì sẽ mặc định làm việc với filter table.

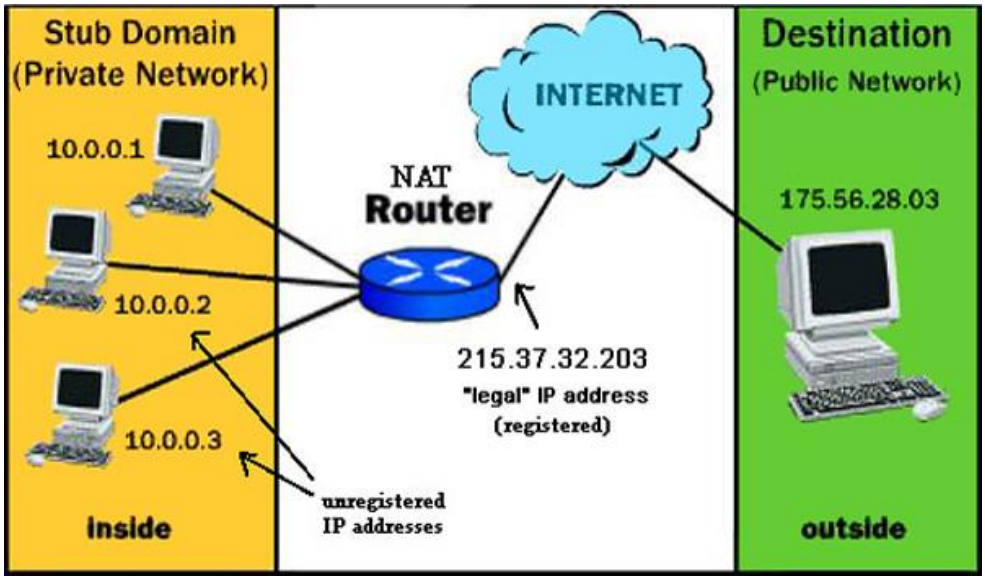


a. **Filter table:**

- Được sử dụng nhiều nhất trong iptables trong suốt quá trình hoạt động (nên nó là table mặc định)
- Nhiệm vụ: quyết định một gói tin có được đi đến đích dự kiến hay không hoặc quyết định từ chối yêu cầu của gói tin.
- Trong table này, bạn sẽ quyết định xem packet có được phép vào (input) hoặc ra (output) khỏi máy tính của bạn hay không. Nếu bạn muốn chặn một port để ngừng nhận bất cứ thứ gì, đây là điểm table bạn cần.

b. NAT table:

- NAT (Network Address Translation) là một kỹ thuật cho phép một hoặc nhiều địa chỉ IP nội miền chuyển đổi sang một hoặc nhiều địa chỉ IP ngoại miền.



- NAT tables sẽ dùng các rules về NAT.
- Nhiệm vụ chính: chỉnh sửa các Source hay còn gọi là IP nguồn. Hoặc chỉnh sửa các destination (IP đích) của các gói tin.
- Table này là table phổ biến thứ hai và chịu trách nhiệm tạo kết nối mới. Đó là cách viết tắt của Network Address Translation.

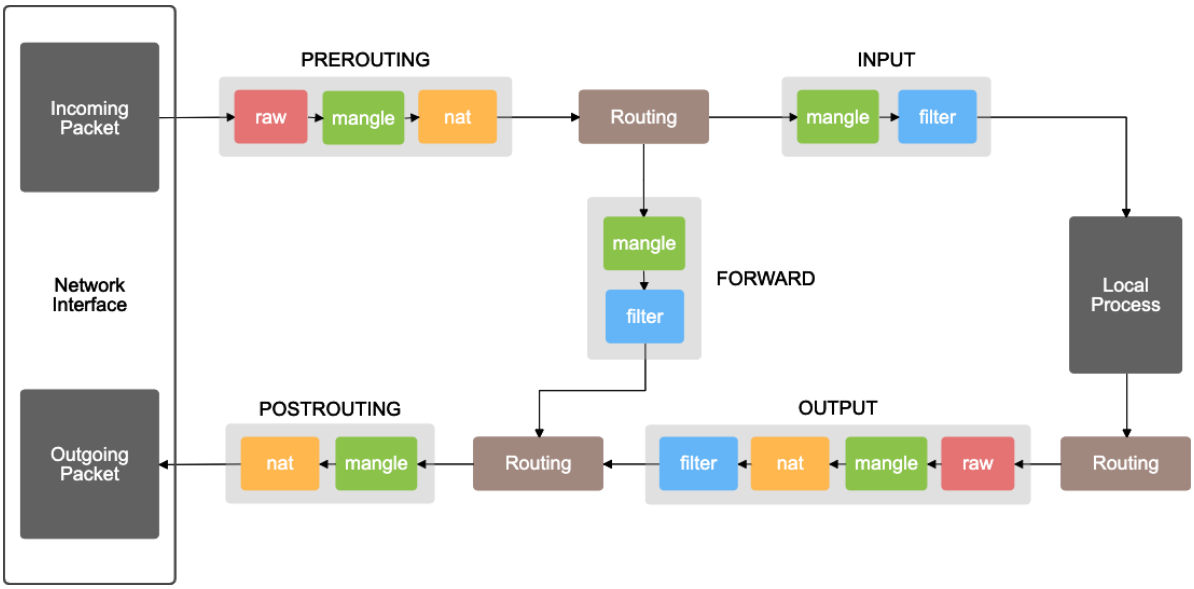
c. Mangle table

- Mangle Table là một trong những bảng quan trọng trong Iptables.
- Bảng này có nhiệm vụ chỉnh sửa header của gói tín. Ngoài ra, sự hiện diện của Mangle Table còn cho phép chỉnh sửa giá trị của các trường: TTL, MTL, Type of Service.
- table này dùng để thay đổi dữ liệu bên trong các packet trước khi chúng đến hoặc ra khỏi máy tính.

d. Raw tables

- table này xử lý packet raw chưa qua xử lý như tên gọi của nó. Chủ yếu là để theo dõi trạng thái kết nối. Chúng ta sẽ thấy các ví dụ về điều này bên dưới khi muốn cho các packet thành công từ kết nối SSH.

e. Sercurity tables



- có nhiệm vụ đánh dấu những gói tin có liên quan đến context của SELinux, nó giúp cho SELinux hoặc các thành phần khác hiểu được context SELinux và xử lý gói tin.

2. Chains

- Chains (chuỗi rule) được tạo ra với số lượng nhất định ứng với mỗi bảng trong iptables. Công dụng chính của thành phần này là giúp lọc gói tin tại các thời điểm khác nhau

a. Chain Prerouting:

- Chain tồn tại trong Nat Table, Mangle Table và Raw Table.
- Các rules trong Chain sẽ được thực thi ngay khi gói tin vào đến giao diện Network Interface.
- Quyết định điều gì sẽ xảy ra với một packet ngay khi nó tới Network Interface. Chúng ta có các tùy chọn khác nhau như thay đổi packet (có thể là NAT), bỏ packet hoặc không làm gì cả và để nó tiếp tục di chuyển và được xử lý ở nơi khác trên đường đi.

b. Chain input

- Chain chỉ có ở Mangle Table và Nat Table.
- Các rules trong Chain này được cung cấp nhiệm vụ thực thi trước khi gói tin vào tiến trình.

- Đây là một trong những chain phổ biến vì nó hầu như luôn chứa các rule nghiêm ngặt để kiểm soát truy cập từ internet gây hại cho máy tính của chúng ta. Nếu bạn muốn mở hay chặn một port thì đây là nơi bạn sẽ làm điều đó.
-

c. Chain output

- Chain này tồn tại ở các bảng quen thuộc như Raw Table, Mangle Table và Filter.
- Các rules tại đây được cung cấp nhiệm vụ thực thi sau khi gói tin được tiến trình tạo ra.
- chịu trách nhiệm cho tất cả quá trình truy cập ra bên ngoài. Bạn không thể gửi một packet mà không được sự cho phép. Đó là nơi tốt nhất để hạn chế lưu lượng outgoing của bạn nếu bạn không chắc chắn mỗi ứng dụng đang giao tiếp qua cổng nào.

d. Chain forward

- Chain này tồn tại ở các bảng Mangle Table và Filter Table.
- Các rules được cung cấp nhiệm vụ thực thi cho các gói tin được định tuyến qua host hiện đại.
- chain này chịu trách nhiệm forward packet. Chúng ta có thể coi máy tính như một bộ định tuyến (router) và đây là nơi mà một số quy tắc (rule) có thể áp dụng để thực hiện công việc.

e. Chain Postrouting

- Chain này chỉ tồn tại ở các bảng Mangle Table và Nat Table.
- Các rules trong Chain được thực thi khi gói tin rời giao diện Internet.
- chain này là nơi các packet để lại dấu vết cuối cùng, trước khi rời khỏi máy tính của chúng ta. Điều này được sử dụng để định tuyến (routing) trong số nhiều tác vụ khác để đảm bảo các packet được xử lý theo cách chúng ta muốn

3. Target

- Target – hành động sử dụng dành cho các gói tin khi các gói tin thỏa mãn các rules đặt ra.
- Các target chỉ định nơi packet sẽ đi. Điều này được quyết định bằng cách sử dụng các target của chính iptables:
    + ACCEPT (chấp nhận): Hành động chấp nhận và cho phép gói tin đi vào hệ thống
    + DROP (gỡ bỏ): Hành động loại gói tin, không có gói tin trả lời.

    + RETURN (quay trở lại): Bỏ qua chuỗi hiện tại. Quy trở lại quy tắc tiếp theo từ chuỗi được gọi. Hữu ích khi muốn dừng xử lý một gói tin trong một chain, nhưng cũng không muốn accept hoặc drop gói tin đó ⇒ chuyển gói tin trở lại rule tiếp theo trong chain được gọi. Vd chain A gọi chain B xử lý một gói, nếu trong chain B, gói phù hợp 1 quy tắc có target là return thì gói sẽ trở lại chain A để tiếp tục xử lý bởi rule tiếp theo trong chain A.
    + Hoặc target của các extension module, phổ biến nhất là DNAT, LOG, MASQUERADE, REJECT, SNAT, TRACE và TTL.
- Các target được chia thành có kết thúc và không kết thúc. Các target có kết thúc chấm dứt rule và các packet sẽ bị ngừng ở đó. Nhưng các target không kết thúc sẽ xử lý packet theo một cách nào đó và rule sẽ được thực hiện tiếp tục sau đó.

4. Giao thức (protocol)
- Xác định các giao thức mà rule thực hiện trên nó.
- Các giao thức thường gặp là TCP UDP ICMP
5. Source/Destination
- Xác định địa chỉ IP nguồn hoặc IP đích và số cổng của rule
- Có thể dùng một vùng IP hoặc một vùng Port trong rule
6. Options:
- Các thành phần khác như state, limit, limit burst,v.v...