Firewall

Firewall

Firewall là gì?

- Firewall là một công cụ quan trọng có thể được cấu hình để bảo vệ máy chủ và cơ sở hạ tầng

Firewall

IPTables là gì?

- IPTables là một công cụ quản lý tường lửa trong Linux, được sử dụng để tạo và quản lý các rules để kiểm soát luồng gói dữ liệu trên mạng.

Firewall

Netfilter là gì?

- Netfilter là một phần trong kernel của hệ điều hành Linux.

- Netfilter theo dõi và xử lý các gói dữ liệu đi qua hệ thống, cho phép thực hiện các tác vụ như chặn gói dữ liệu không mong muốn hoặc chuyển hướng gói dữ liệu đến các máy chủ khác.

Netfilter Hooks

- Hooks là những điểm trong quá trình xử lý gói dữ liệu mạng, nơi có thể gắn các hàm xử lý riêng của người dùng.
- Các hook mà gói tin sẽ kích hoạt tùy thuộc vào việc gói đến hay đi, đích đến của gói và liệu gói bị loại bỏ hay bị từ chối tại điểm trước đó hay không

Netfilter Hooks

Có 5 loại Hook:

- NF_IP_PRE_ROUTING
- NF_IP_LOCAL_IN
- NF_IP_FORWARD
- NF_IP_LOCAL_OUT
- NF_IP_POST_ROUTING

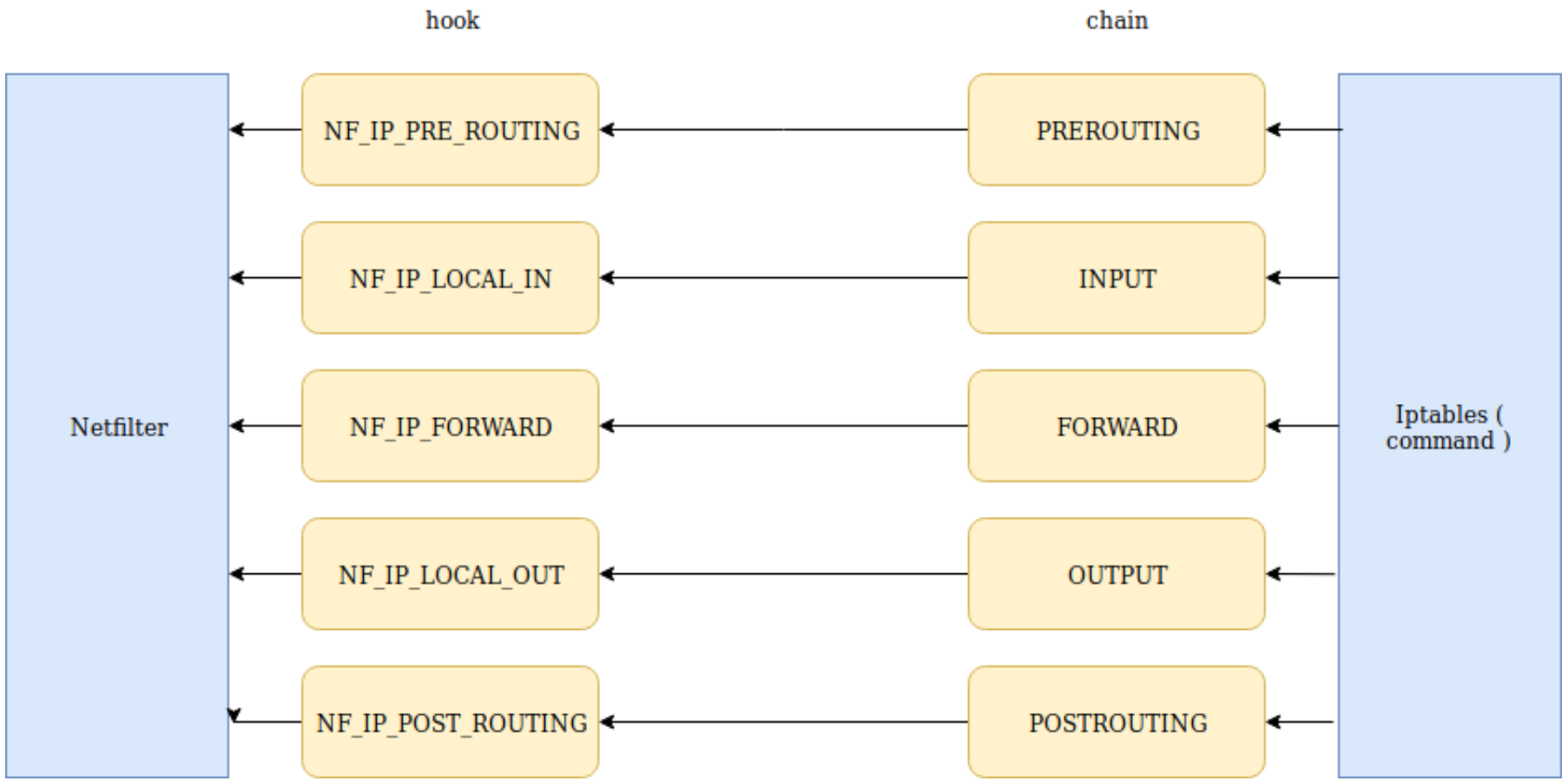
IPTables Tables

- Filter Table
- NAT Table
- Mangle Table
- Raw Table
- Security Table

IPTables Chains

PREROUTING : Được kích hoạt bởi hook NF_IP_PRE_ROUTING .
INPUT : Được kích hoạt bởi hook NF_IP_LOCAL_IN .
FORWARD : Được kích hoạt bởi hook NF_IP_FORWARD .
OUTPUT : Được kích hoạt bởi hook NF_IP_LOCAL_OUT .
POSTROUTING : Được kích hoạt bởi hook NF_IP_POST_ROUTING .

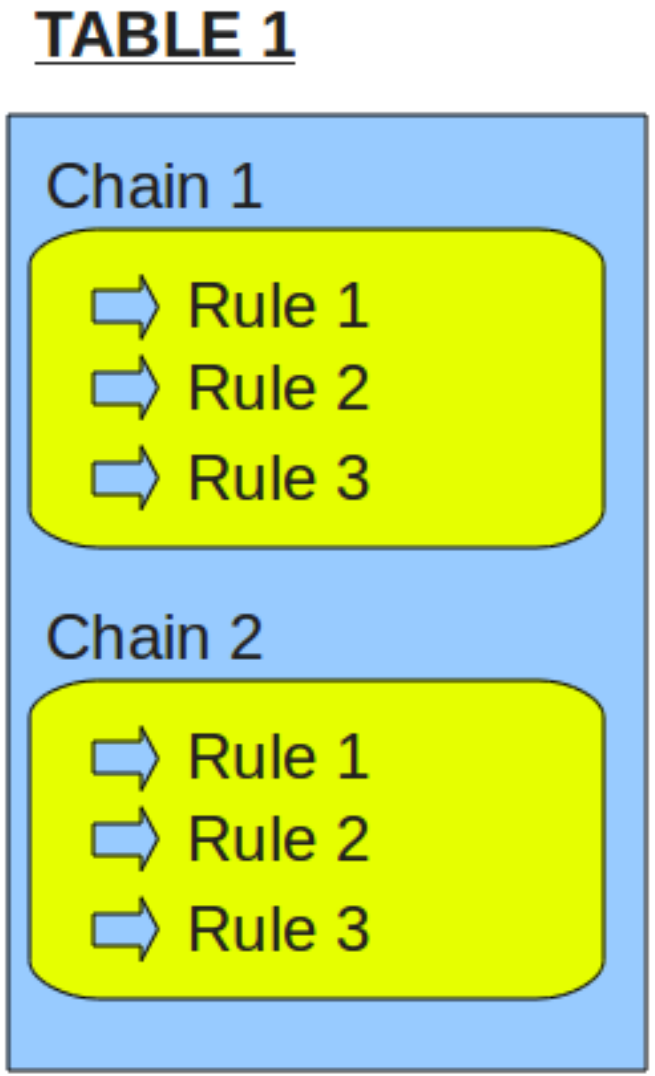
IPTables Tables and Chains



IPTables Rules

Các rule sẽ được đặt trong một chain cụ thể của một bảng cụ thể. Khi chain được gọi, gói được đề cập sẽ kiểm tra theo từng rule trong chain theo thứ tự.

ACCEPT: Hành động chấp nhận và cho phép gói tin đi vào hệ thống
DROP: Hành động loại gói tin, không có gói tin trả lời.
REJECT: Hành động loại gói tin nhưng vẫn cho phép gói tin trả lời Table gói tin khác.
LOG: Hành động chấp thuận gói tin nhưng có ghi lại log



IPTables Rules

Matching

Matching chỉ định các tiêu chí mà gói phải đáp ứng để hành động liên quan được thực thi

IPTables Rules

Target

Target là hành động được kích hoạt khi một gói đáp ứng các tiêu chí phù hợp của rule

- ACCEPT: Hành động chấp nhận và cho phép gói tin đi vào hệ thống

- DROP: Hành động loại gói tin, không có gói tin trả lời.

- REJECT: Hành động loại gói tin nhưng vẫn cho phép gói tin trả lời Table gói tin khác.

- LOG: Hành động chấp thuận gói tin nhưng có ghi lại log

IPTables Rules

Target

Target là hành động được kích hoạt khi một gói đáp ứng các tiêu chí phù hợp của rule

- **Terminating Target**

VD: Chặn tất cả các gói dữ liệu từ địa chỉ IP 192.168.1.100

```
iptables -A INPUT -s 192.168.1.100 -j DROP
```

IPTables Rules

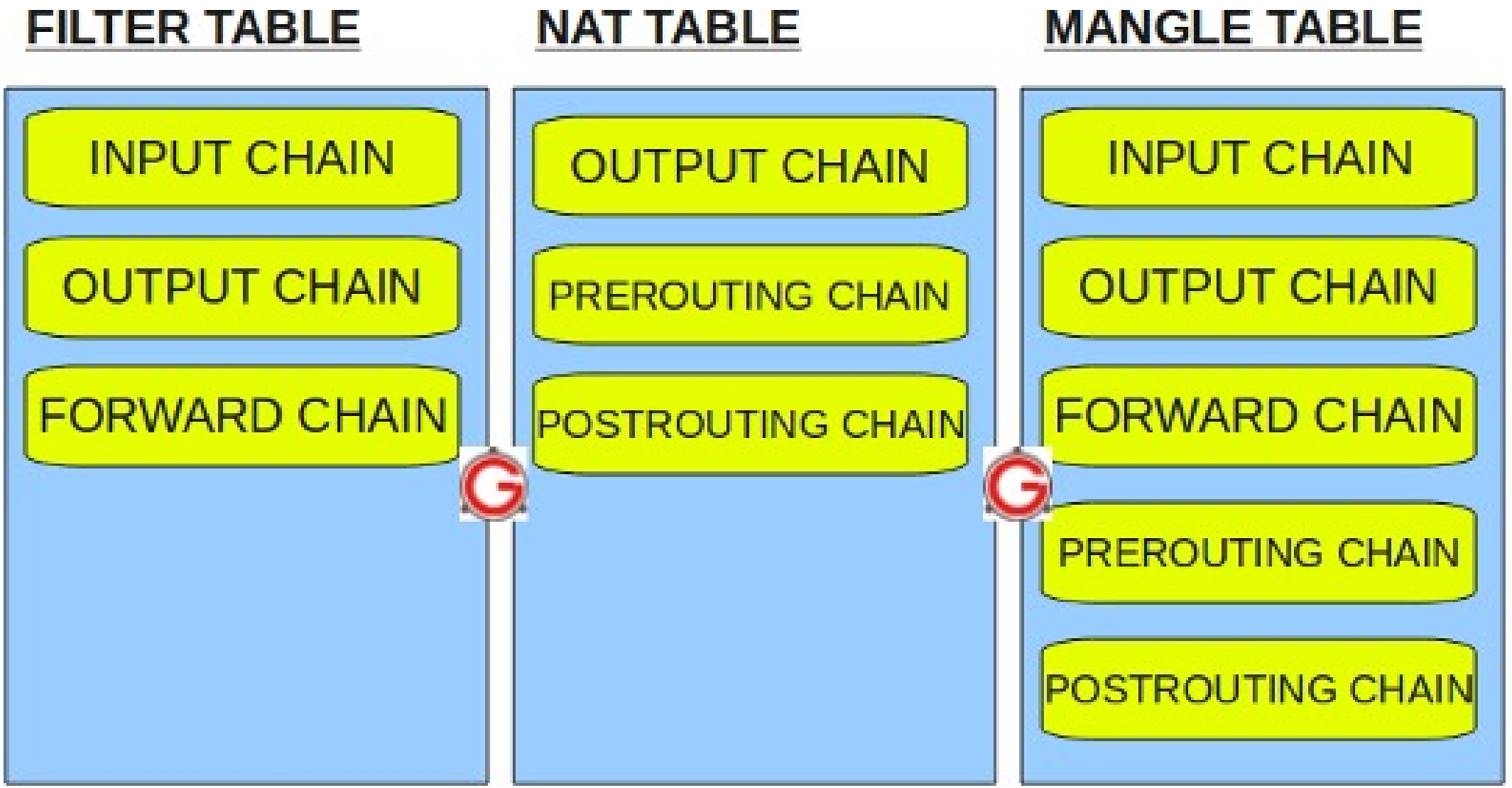
Target

Target là hành động được kích hoạt khi một gói đáp ứng các tiêu chí phù hợp của rule

- **Non-Terminating Target**

VD: Cho phép kết nối SSH từ địa chỉ IP 192.168.1.200

```
iptables -A INPUT -s 192.168.1.200 -p tcp --dport 22 -j ACCEPT
```


FILTER TABLE
NAT TABLE
MANGLE TABLE
INPUT CHAIN
OUTPUT CHAIN
FORWARD CHAIN
OUTPUT CHAIN
PREROUTING CHAIN
POSTROUTING CHAIN
INPUT CHAIN
OUTPUT CHAIN
FORWARD CHAIN
PREROUTING CHAIN
POSTROUTING CHAIN

IPTables Connection Tracking

- NEW
- ESTABLISHED
- RELATED
- INVALID
- SNAT
- DNAT