Nftables.

File cấu hình cho nftables thực hiện cho phép ip của giám đốc và loopback

A screen shot of a computer program

Description automatically generated with low confidence

1. Dòng đầu tiên

A picture containing font, screenshot, text, graphics

Description automatically generated

Là một shebang (#!) chỉ định đường dẫn tới trình thông dịch nftables (/usr/sbin/nft) và tùy chọn -f để chỉ rõ rằng nội dung sau đây là một tập tin cấu hình.

1. Tiếp theo, ta có cấu trúc cơ bản của tập tin cấu hình nftables:

A picture containing screenshot, text, font, line

Description automatically generated

Tạo một bảng tên là **filter** dùng cho cả IPv4 và IPv6 (kiểu **inet**). Bảng này sẽ chứa các chain (chuỗi) để xử lý các quy tắc tường lửa.

1. Trong bảng filter, chúng ta có chain input:

A picture containing text, screenshot, font

Description automatically generated

Chain input có kiểu là filter và được đặt vào hook input với độ ưu tiên 0. Điều này có nghĩa là chain này sẽ xử lý các gói tin đến (incoming packets) trước khi chúng đến ứng dụng của người dùng.

1. Sau đó, là các quy tắc tường lửa trong chain input:

A screen shot of a computer code

Description automatically generated with low confidence

* Quy tắc đầu tiên cho phép tất cả các gói tin loopback (gói tin từ và đến cùng máy chủ) thông qua giao diện lo (loopback interface).
* Quy tắc thứ hai cho phép các gói tin đến từ địa chỉ IP của giám đốc (10.0.2.10).
* Quy tắc cuối cùng loại bỏ (drop) tất cả các gói tin đến khác không thỏa mãn các quy tắc trên.

Tóm lại, tập tin cấu hình này thiết lập một tường lửa chỉ cho phép gói tin đến từ địa chỉ IP của giám đốc và các gói tin loopback, còn lại sẽ bị chặn.