Note: iptables.

a firewall could also be considered a policy enforcement system. Devices that inspect and then pass or filter network traffic could be called network policy enforcement systems.

Devices that inspect and then pass or filter host-centric activities could be called host policy enforcement systems

Properly configured traditional network firewall products basically deny all but allowed Internet protocols, IP addresses, TCP/UDP ports, and ICMP types and codes

Chapter 1: CARE AND FEEDING OF IPTABLES

iptables- iptables firewall được phát minh bởi Netfilter Project

- available to the masses as part of Linux since the release of the Linux 2.4 kernel in January 2001.

- iptables cung cấp các chức năng toàn diện bao gồm protocol state tracking, packet application layer inspection, rate limiting, powerful mechanism to specify a filtering policy.

- Bên cạnh đó, iptables sử dụng Netfilter framework to hook functions designed to perform operations on packets (such as filtering) into the networking stack

- Có thể nói Netfilter cung cấp các framework và iptables được xây dựng các chức năng đó.

- Netfilter does not filter traffic itself—it just allows functions that can filter traffic to be hooked into the right spot within the kernel

- Project chính cho vấn đề lọc, phân mảnh, được cung cấp bởi linux là Netfilter, nhưng thuật ngữ trên cũng được tham chiếu đến framework với nhân kernel, mà nó được sử dụng cho việc móc nối các chức năng trong networking status với các giai đoạn khác nhau.

- iptables sử dụng cho Netfilter framework để móc nối các chức năng, thực hiện các hoạt động trên packet (như lọc) trong network stack

- thuật ngữ iptables cũng nói đến đến ứng dụng cho người dùng như cú pháp cmd và nó kết nối với firewall policy trong kernel.

- các thuật ngữ như tables, chains, matches, targer quan trọng trong nội dung chính iptables

- netfilter không tự filter traffic, nó chỉ cung cấp các chức năng có thể filter traffic móc nối trong kernel. Netfilter Project cũng cung cấp các mảnh trong kernel như connection tracking, logging; bất kỳ chính sách nào của iptables đề có thể thực hiện việc xử lý 1 số packet nhất định

Packet Filtering with iptables- công cụ cao cấp, cho phép người dùng kiếm soát các IP packet tương tác với hệ thống, thi hành trên kernel