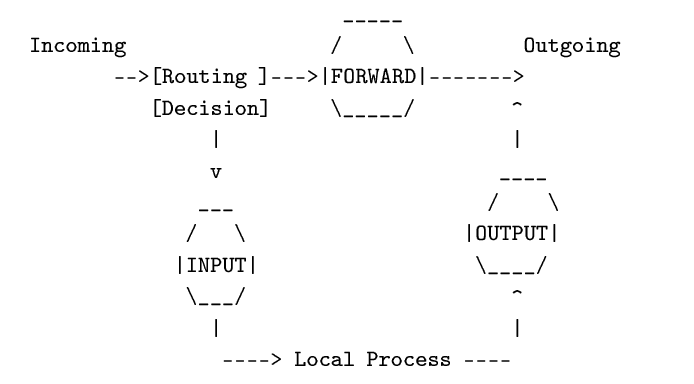
IP tables

Nói đến IP tables trong linux cần phải kể thêm đến netfilter , theo ý tui hiểu thì netfilter sẽ đóng vai trò đảm nhiệm nhiệm vụ xử lí bên trong kernel <chỉ những kernel hỗ trợ netfilter> , còn phần IP tables chỉ là vai trò trung gian giữa người dùng và netfilter

Vấn đề đặc ra đối với việc sử dụng iptables và netfilter là việc những cấu hình sẽ bị mất khi hệ thống reboot <nễn sẽ xuất hiện khái niêm iptables save and restore script> tuy nhiên theo tui nghĩ vẫn mất thời gian trễ sau khi khởi động hệ thống , thứ nữa , trong toàn bộ hoạt động của IP tables và netfilter không nhắc đến vấn đề hệ thống bị ngưng hoạt việc cập nhật luật có online hay không ….

Về cơ bản IPtables hoạt động dựa trên ba chain chính



Input , output và forward

Liên quan đến việc chuyển hay chấp nhận xử lý và xuất những gói tin đã được xử lý ra môi trường ngoài , mối gói tin tới filter nếu dành cho địa chỉ khác thì nếu hệ thống có hỗ trợ forward gói tin sẽ được forward theo chain forward , ngược lại nếu hệ thống không hỗ trợ gói tin sẽ bị drop , trường hợp gói tin là dành cho mình , thì chain Input được kích hoạt , gói tin sẽ được duyệt qua chain này nếu không bị drop sẽ được chuyển tiếp qua các quá trình xử lý , cuối cùng duyệt qua chain output tương tự như chain input để có thể ra môi trường ngoài

Nói nãy h vẫn chưa định nghĩa chain ,nó gồm một dãy các rules , mỗi rule sẽ có dạng nếu gói tin như thế này thì sẽ xử lí như sau….Nếu gói không match điều kiện của rules này thì sẽ được kiểm tra ở rule kế tiếp , nếu không còn rules nào nữa thì kernel sẽ kiểm tra policy của chain đó <chỉ các chain Input ,output ,forward kể trên có policy> để biết phải làm zì với gói tin.

Chain có hai loại built-in chains và user-define chains , chỉ built-in chains có policy <gồm các chain kể trên> .Theo tui nghĩ gói tin khi vào filter thì được kiểm định với built-in chains đầu tiên ,sau đó có thể nhảy sang kiểm tra bởi các chain khác do người dùng định nghĩa,theo tui nghĩ các chain này là để hỗ trợ việc sử dụng lại ...thui.

Iptable hỗ trợ việc định nghĩa các chains các rule trong các chain đó với nhiều mức độ cũng như thành phần khác nhau , ngoài ra còn hỗ trợ việc pass các gói tin bị drop vào các queue chuyển sang các ứng dụng khác về chi tiết mình xem trong file ps ,tui không trình bày ở đây .

PktFilter

Tổng quan:

Là một phần mã nguồn mở ,chức năng chính là chỉnh sửa cấu hình IPv4 filtering driver trong các phiên bản Windows 2000/XP/Server 2003

Gồm 2 phần pktfltsrv tương tác trực tiếp với IP filtering driver và pktfilter đứng giữa người sử dụng và pktfltsrv <dạng command-line> có thể thêm bớt rule theo cú pháp định sẵn được đặc tả chi tiết trong file pdf .

Phần mềm này nhỏ gọn .có khả năng drop packet và log lại những thong tin về packet bị drop .

Phần mềm này hoạt động dựa chủ yếu trên hệ thống các rule được đặc tả trong một file txt

Phần mềm này chỉ đơn giản là configure lại driver có sẵn trong windows nên chỉ thực hiện được một số tính năng đơn giản liên quan đến việc drop gói tin , vấn đề mở rộng sau này không tương thích , mặc khác khi khởi động hệ thống ,PktFilter phải mất một khoảng thời gian trước khi chính thức chạy , bởi thế trong khoảng thời gian này coi như hệ thống không có filter <khoảng 2 phút đầu>

Không biết phần mềm này có giúp ích zì an hem xem xét thử !