**Bắt đầu với Iptables**

TARGET PROT OPT IN OUT SOURCE DESTINATION

ACCEPT all -- lo any anywhere anywhere

ACCEPT all -- any any anywhere anywhere ctstate RELATED,ESTABLISHED

ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh

ACCEPT tcp -- any any anywhere anywhere tcp dpt:http

ACCEPT tcp -- any any anywhere anywhere tcp dpt:https

DROP all -- any any anywhere anywhere

- Ngay đoạn thứ nhất, chúng ta có các cột như TARGET, PROT, OPT, IN, OUT, SOURCE, DESTINATION, ý nghĩa của mỗi cột là như sau:

**+ TARGET**: Hành động sẽ thực thi cho mỗi chuỗi quy tắc.

**+ PROT**: Là viết tắt của chữ Protocol, nghĩa là giao thức. Tức là các giao thức sẽ được áp dụng để thực thi quy tắc này. Ở đây chúng ta có 3 lựa chọn là *all*, *tcp* hoặc *udp*. Các ứng dụng như SSH, FTP, sFTP,..đều sử dụng giao thức kiểu *TCP*.

**+ IN**: Thiết bị mạng nhận kết nối vào được áp dụng cho quy tắc, chẳng hạn như lo, eth0, eth1.

**+ OUT**: Thiết bị mạng phục vụ nhu cầu gửi kết nối ra ngoài được áp dụng quy tắc.

**+ DESTINATION**: Địa chỉ của lượt truy cập được phép áp dụng quy tắc.

VD:

ACCEPT all -- lo any anywhere anywhere

- Chấp nhận toàn bộ kết nối thông qua thiết bị lo, lo ở đây nghĩa là “**Loopback Interface**”, là một thiết bị mạng ảo nội bộ, chẳng hạn như IP 127.0.0.1 là kết nối qua thiết bị này.

ACCEPT all -- any any anywhere anywhere ctstate RELATED,ESTABLISHED

- Cho phép giữ lại các kết nối hiện tại. Nghĩa là khi bạn đang ở trong SSH và sửa đổi lại Firewall, nó sẽ không đá bạn ra khỏi SSH nếu bạn không thỏa mãn quy tắc.

ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh

- Cho phép kết nối vào SSH Server ở bất cứ thiết bị nào, bất cứ ai và bất cứ đâu. Mặc định nó sẽ hiển thị dpt:ssh để biểu diễn cổng 22 của SSH, nếu bạn đổi SSH thành cổng khác thì nó sẽ hiển số cổng.

ACCEPT tcp -- any any anywhere anywhere tcp dpt:http

- Cho phép kết nối vào cổng 80, mặc định nó sẽ biểu diễn bằng chữ http.

ACCEPT tcp -- any any anywhere anywhere tcp dpt:https

- Cho phép kết nối vào cổng 443, mặc định nó sẽ biểu diễn bằng chữ https.

DROP all -- any any anywhere anywhere

- Ngắt các kết nối ở mọi kết nối khác nếu không thuộc những loại kết nối ở trên.

**Cách tạo một quy tắc mới**

Nếu iptables của bạn chưa được thiết lập thì bạn gõ lệnh iptables -L -v nó sẽ trả kết quả về giống thế này:

Chain INPUT (policy ACCEPT 2245 packets, 200K bytes)

pkts bytes target prot opt in out source destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 1795 packets, 147K bytes)

pkts bytes target prot opt in out source destination

Tại đoạn trên, bạn sẽ thấy nó được chia ra làm 3 nhóm với 3 kiểu quy tắc đó là:

**- INPUT**: áp dụng cho các kết nối đi vào.

**- FORWARD**: áp dụng cho các kết nối đã được trỏ đến một vị trí khác.

**- OUTPUT**: áp dụng cho các kết nối ra ngoài từ máy chủ.

Ok, bây giờ chúng ta sẽ thêm một quy tắc đơn giản vào iptables với lệnh sau:

iptables -A INPUT -i lo -j ACCEPT

**- A INPUT**: khai báo kiểu kết nối sẽ được áp dụng (A nghĩa là Append).

**- i lo**: Khai báo thiết bị mạng được áp dụng (i nghĩa là Interface).

**- j ACCEPT**: khai báo hành động sẽ được áp dụng cho quy tắc này (j nghĩa là Jump).

- Và bây giờ hãy thử gõ lại lệnh iptables -L -v nhé, bạn sẽ thấy quy tắc chúng ta vừa thêm đã xuất hiện trong đó.

- Sau khi thêm một quy tắc hay làm bất cứ việc gì xong, nhớ gõ lệnh lưu quy tắc và khởi động lại iptables để nó áp dụng thay đổi.

service iptables save

service iptables restart

- Tiếp tục bây giờ chúng ta thêm một quy tắc để cho phép lưu lại các kết nối hiện tại để tránh hiện tượng tự block bạn ra khỏi máy chủ.

iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

Đoạn trên cấu trúc cũng như quy tắc chúng ta vừa thêm, nhưng nó sẽ có thêm hai tham số mới là:

- **-m conntrack**: Áp dụng cho các kết nối thuộc module tên là “Connection Tracking“. Module này sẽ có 4 kiểu kết nối là NEW, ESTABLISHED, RELATED và INVALID. Cụ thể là ở quy tắc này chúng ta sẽ sử dụng kiểu RELATED và ESTABLISHED để lọc các kết nối đang truy cập.

- **--ctstate** RELATED,ESTABLISHED: Khai báo loại kết nối được áp dụng của cái module Connection Tracking mà mình đã nói ở trên.

Và đây là đoạn tạo quy tắc cho phép truy cập cổng 22 của SSH.

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

- **-p tcp**: Giao thức được áp dụng.

- **--dport 22**: Cổng cho phép áp dụng.

Và cho phép truy cập cổng 80

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Nhưng sẽ khóa toàn bộ các kết nối còn lại:

iptables -A INPUT -j DROP

**Bổ sung một quy tắc**

- Ở phần tạo quy tắc, bạn có để ý là chúng ta luôn sử dụng tham số -A (tức là Append) để nối một quy tắc mới vào danh sách các quy tắc của iptables, mỗi khi tạo mới một quy tắc nó sẽ tự động đưa vào cuối cùng.

- Nhưng nếu bạn muốn thêm một quy tắc và đặt nó vào vị trí như mong muốn thì sẽ sử dụng tham số -I thay cho -A, chẳng hạn như:

iptables -I INPUT 2 -p tcp --dport 443 -j ACCEPT

- Trong đó, -I INPUT 2 nghĩa là mình đặt quy tắc này vào dòng thứ 2 trong danh sách các quy tắc thuộc loại kết nối INPUT. Cũng xin nói thêm là cổng 443 chính là cổng HTTPS/SSL.

**Cách xóa một quy tắc**

- Ở trên mình đã có nói qua cách thêm một quy tắc để cho phép kết nối vào cổng 22 của SSH. Nhưng nếu bạn đã đổi cổng SSH rồi thì dĩ nhiên chúng ta sẽ không cần quy tắc này nữa, nên sẽ cần xóa nó đi để thêm một quy tắc mới.

- Trước khi xóa một quy tắc, bạn cần phải xác định được quy tắc này nằm ở hàng thứ mấy trong loại kết nối (INPUT, OUTPUT,..). Bạn cứ gõ lệnh iptables -L ra và xem rồi đếm.

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere tcp dpt:https

ACCEPT all -- anywhere anywhere ctstate RELATED,ESTABLISHED

ACCEPT tcp -- anywhere anywhere tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere tcp dpt:http

DROP all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Vậy ở đây là mình cần xóa quy tắc số 4 của INPUT.

iptables -D INPUT 4

Ngoài ra, nếu bạn muốn xóa toàn bộ các quy tắc chứa hành động DROP thì có thể sử dụng lệnh sau:

iptables -D INPUT -j DROP