

System Admin

Training Assignments

|  |  |
| --- | --- |
| Program Code |  |
| Issue/Revision | x/y |
| Effective date | 04/Aug /2023 |

Assignment Day 10. Security

Mục Lục:

[Hướng dẫn cài đặt và cấu hình Iptable trên Linux 2](#_Toc1735541039)

[2. Tạo Rule IPtables 4](#_Toc396815140)

[3. Lọc các kết nối: 5](#_Toc754939034)

[4. Lưu lại các kết nối hiện tại: 5](#_Toc792461114)

[5. Cho phép truy cập port cụ thể 6](#_Toc606097840)

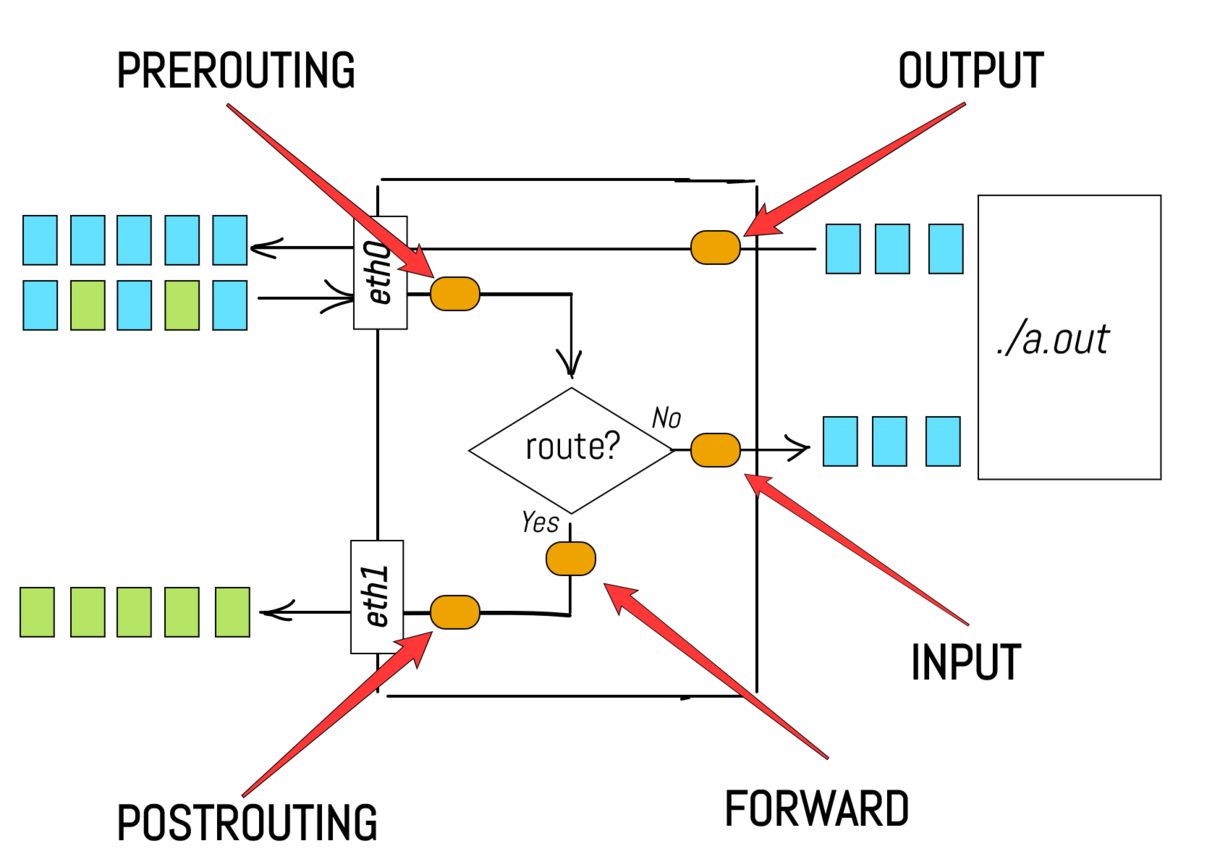
[6. Bổ sung Rule IPtables 6](#_Toc741507604)

[7. Xóa Rule IPtables 6](#_Toc1334649065)

[8. Lưu cấu hình IPtables 7](#_Toc341099290)

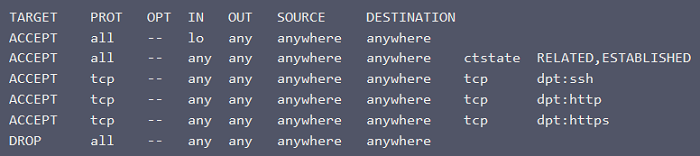
# Hướng dẫn cài đặt và cấu hình Iptable trên Linux

Lý thuyết:





danh sách các rule – quy tắc – tường lửa cần thiết trong mỗi server. Mặc định thì iptables sẽ không có bất cứ rule nào cả.



Theo như hình, 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**: viết tắt của chữ **Protocol** – giao thức. Tức là các giao thức sẽ được áp dụng để thực thi quy tắc này.
* Chúng ta có 3 lựa chọn bao gồm: **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.

Chúng ta cùng nhau giải thích ý nghĩa các hàng ngang trong danh sách như sau:

Ví dụ : Hàng đầu tiên

1

*Ý nghĩa :* Chấp nhận toàn bộ kết nối thông qua thiết bị *lo* – *“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.

Ví dụ : Hàng thứ 2

2

*Ý nghĩa :* Cho phép giữ lại các kết nối hiện tại : là khi bạn đang ở trong SSH và sửa đổi lại Firewall, hệ thống sẽ không ngắt kết nối của bạn ra khỏi SSH nếu bạn không thỏa mãn quy tắc.

Ví dụ : Hàng thứ 3

3

*Ý nghĩa :* Cho phép kết nối vào SSH Server ở bất cứ thiết bị nào, bất cứ ai và bất cứ đâu. Mặc định hệ thống sẽ hiển thị **dpt:ssh** để diễn đạt port 22 của *SSH*, nếu bạn có thay đổi port *SSH* thì hệ thống sẽ hiển thị thông tin port tương ứng.

Ví dụ : Hàng thứ 4

4

*Ý nghĩa :* Cho phép kết nối vào cổng 80, mặc định sẽ diễn đạt bằng chữ **http**.

Ví dụ : Hàng thứ 5

5

*Ý nghĩa :* Cho phép kết nối vào cổng 443, mặc định sẽ diễn đạt bằng chữ **https**.

Ví dụ : Hàng thứ 6

6

## **2. Tạo Rule IPtables**

Nếu IPtables chưa được thiết lập thì chúng ta thực thi command kiểm tra Filter rule:

|  |  |
| --- | --- |
| 1 | iptables -L -v |

Tại đoạn trên, bạn sẽ thấy hệ thống gồm có 3 quy tắc nhỏ (chain) để giúp bạn thiết lập các nguyên tắc lọc gói:

* **Forward chain** : lọc gói khi đi đến các server khác.
* **Input chain** : lọc gói khi đi vào trong server.
* **Output chain** : lọc gói khi ra khỏi server.

## **3. Lọc các kết nối:**

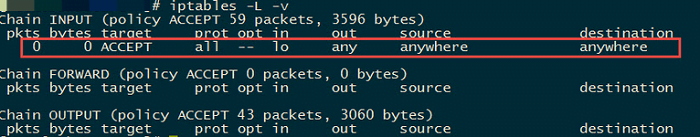
Giả dụ tôi thiết lập một rule đơn giản vào IPtables bằng command:

|  |  |
| --- | --- |
| 1 | iptables -A INPUT -i lo -j ACCEPT |

Với ý nghĩa :

* **-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 < interface-name >** nghĩa là *Interface*).
* **-j ACCEPT**: khai báo hành động sẽ được áp dụng cho quy tắc này (**-j < target >** nghĩa là *Jump*).

Kiểm tra Filter rule lần nữa, chắc chắn bạn sẽ thấy rule chúng ta vừa thiết lập đã xuất hiện:



Hoặc ta cùng xem một ví dụ sau :

|  |  |
| --- | --- |
| 1 | iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP -j ACCEPT |

Với ý nghĩa : IPtables được cấu hình cho phép “firewall” chấp nhận các gói dữ liệu *TCP*, đến từ card mạng *eth0*, có bất kỳ địa chỉ IP nguồn đi đến địa chỉ *192.168.1.1* – là địa chỉ IP của firewall. *0/0* nghĩa là bất kỳ địa chỉ IP nào.

## **4. Lưu lại các kết nối hiện tại:**

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

|  |  |
| --- | --- |
| 1 | iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT |

Đoạn trên cấu trúc cũng như rule chúng ta vừa thiết lập ở ví dụ trên nhưng lần này sẽ có thêm hai tham số mới là:

* **-m conntrack**: Áp dụng cho các kết nối thuộc module “*Connection Tracking*“ với 4 kiểu kết nối là **NEW**, **ESTABLISHED**, **RELATED** và **INVALID**. Cụ thể ở rule 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 module “*Connection Tracking*“.

## **5. Cho phép truy cập port cụ thể**

Chúng ta sử dụng command :

|  |  |
| --- | --- |
| 1  2  3 | iptables -A INPUT -p tcp --dport 22 -j ACCEPT  iptables -A INPUT -p tcp --dport 80 -j ACCEPT  iptables -A INPUT -j DROP |

Với ý nghĩa :

* **-p tcp**: Giao thức được áp dụng.
* **–dport 22** và **–dport 80**: Cổng cho phép áp dụng.
* **-j DROP** : Nhưng sẽ khóa toàn bộ các kết nối còn lại.

## **6. Bổ sung Rule IPtables**

Xuyên suốt phần 2, nếu bạn tinh ý sẽ nhận thấy chúng ta luôn sử dụng tham số **-A** (nghĩa là *Append*) để nối một rule mới vào danh sách các rule của IPtables, với mỗi 1 rule mới hệ thống sẽ chèn vào dòng cuối cùng.

Nhưng nếu bạn muốn thêm một quy tắc và sắp xếp vị trí như mong muốn thì phải điều chỉnh tham số thành **-I** thay cho **-A**, chẳng hạn như:

[?](https://wiki.matbao.net/Bao-mat-may-chu-Linux-Huong-dan-cau-hinh-IPtables-can-ban.ashx#)

|  |  |
| --- | --- |
| 1 | iptables -I INPUT 2 -p tcp --dport 443 -j ACCEPT |

Trong đó, **-I INPUT 2** là việc chúng tôi đặt rule này vào dòng thứ 2 trong danh sách các rule thuộc loại kết nối *INPUT*. Cũng xin nêu rõ thêm là port 443 chính là cổng HTTPS/SSL.

## **7. Xóa Rule IPtables**

Trong phần 2C chúng ta đã thiết lập rule 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 rule này nữa, vì thé chúng ta cần xóa đi để thêm một rule mới.

Trước khi xóa, quan trọng nhất là bạn cần phải xác định được quy tắc này nằm ở hàng thứ mấy trong loại kết nối (INPUT, OUTPUT,..) bằng việc thực thi command : iptables -L

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | 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 chúng ta cần xóa quy tắc số 4 của *INPUT*:

|  |  |
| --- | --- |
| 1 | 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:

|  |  |
| --- | --- |
| 1 | iptables -D INPUT -j DROP |

## **8. Lưu cấu hình IPtables**

Sau khi cấu hình xong, bạn phải luôn nhớ gõ lệnh lưu quy tắc và khởi động lại IPtables để hệ thống áp dụng thay đổi.

|  |  |
| --- | --- |
| 1  2 | service iptables save  service iptables restart |