Phần 10: Linux Firewall

Tường lửa Linux (tường lửa) là gì

Một bức tường ảo trong thế giới bảo mật hệ thống được thiết kế để bảo vệ hệ thống của chúng tôi khỏi việc lưu lượng truy cập không mong muốn và truy cập trái phép vào hệ thống của chúng tôi. Hệ thống bảo mật trong HĐH Linux được gọi là Tường lửa Linux, hệ thống này giám sát và quản lý lưu lượng mạng (kết nối ra/vào). Nó có thể được sử dụng để chặn quyền truy cập vào các IP địa chỉ khác nhau , cụ thểmang , port (điểm ảo nơi mạng kết nối bắt đầu và kết thúc) và dịch vụ

Tường lửa này hoạt động theo khái niệm về phân vùng (phân đoạn).

Kiểm tra trạng thái tưởng lửa

sudo systemctl status firewalld

Một số quy tắc của Tường lửa

Để bảo vệ hệ thống của chúng tôi khỏi bị truy cập trái phép và kiểm soát lưu lượng mạng (đến và đi). Chúng tôi có thể thực hiện tùy chỉnh về cổng, địa chỉ, giao thức, vv một số ví dụ phổ biến được liệt kê bên dưới:

Quy tắc 1: Cho phép lưu trữ SSH (Secure Shell hoặc Secure Socket Shell)

Bằng cách này, chúng tôi có thể cho phép mọi lượng truy cập được lưu trữ trên cổng SHH để có thể kết nối với hệ thống từ xa.

```
sudo tường lửa-cmd --zone=public --add-services=ssh --permanent

sudo tường lửa-cmd --reload
```

```
[root@localhost ~]# sudo firewall-cmd --zone=public --add-service=ssh --permanen
t
success
```

Như chúng tôi có thể thấy nó đã được thực hiện thành công

Quy tắc 2: Cho phép lưu trữ lượng truy cập trên một cổng cụ thể

Chúng tôi cho phép lưu trữ lượng truy cập trên cổng TCP cụ 8080, bạn có thể thay thế bằng các yêu cầu.

```
sudo tường lửa-cmd --zone=public --add-port=8080/tcp --permanent

sudo tường lửa-cmd --reload
```

```
[root@localhost ~]# sudo firewall-cmd --zone=public --add-port=8080/tcp --perman
ent
success
[root@localhost ~]# sudo firewall-cmd --reload
success
```

Cả hai lệnh đều được tìm thấy thành công

Quy tắc 3: Chặn quyền truy cập lưu lượng đến một công cụ IP địa chỉ

Chúng tôi đang chặn lượng truy cập IP 192.168.52.1, bạn có thể thay thế yêu cầu của mình.

```
sudo tường lửa-cmd --zone=public --add-rich='rule family="ipv4" source
address="192.168.52.1" từ chối'

sudo tường lửa-cmd --reload
```

```
[root@localhost ~]# sudo firewall-cmd --zone=public --add-rich-rule='rule family
="ipv4" source address="192.168.52.1" reject'
success
[root@localhost ~]# sudo firewall-cmd --reload
success
```

chúng tôi cũng đã đề cập đến IP của họ (ipv4)

Các loại Tường lửa Linux

Có nhiều hơn một tùy chọn Tường lửa Linux. Khi chúng tôi thả xuống và nghiên cứu, chúng tôi có một số cái tên phổ biến nhất là IPCop, iptables, Shorewall và UFW Nhưng một trong những cái tên phổ biến nhất là Tường lửa **“ iptables ”** .
Iptables đang hoạt động:
Phần mềm dựa trên Linux thực hiện các chức năng hoạt động, lọc gói tin và NAT (dịch địa chỉ mạng) được gọi là Iptables. Với sự trợ giúp của Iptables, cho phép quản trị viên hệ thống kiểm soát lưu lượng truy cập đến và đi bằng cách thiết lập các quy tắc.
Khi một gói được nhận trong cơ sở hệ thống Linux, nó phải đi qua các chuỗi và bảng trong iptables tường lửa. Các bảng được sử dụng phổ biến nhất là filter và nat nhưng chúng tôi có năm bảng được xác định trước trong iptables (raw, nat, filter, security và mangle).

Bảng loại

Chúng ta sẽ thảo luận về bảng được xác định trước đó:

1. **Bảo mật bảng:** Thường được sử dụng kết hợp với các công cụ bảo mật khác như SELinux, cũng được sử dụng cho các quy tắc MAC (Kiểm soát truy cập bắt buộc), có thể được sử dụng để thiết lập các quy tắc liên kết quan đến bảo mật và kiểm soát quyền truy cập. Bảng này có hợp nhất bốn chuỗi: OUTPUT, FORWARD, INPUT và SECMARK.
2. **Mangle Table:** Được sử dụng để sửa đổi các gói bằng cách thiết lập ToS/DSCP của trường ToS/DSCP, thay đổi trường tiêu đề của gói và thay đổi các dấu dấu. Nó có tích hợp năm chuỗi: POSTROUTING, FORWARD, OUTPUT, PREROUTING và INPUT.
3. **Nat Table:** Tắt bản dịch địa chỉ mạng, giúp chia sẻ một địa chỉ IP công cộng duy nhất giữa nhiều thiết bị. Nó có hai tích hợp: PREROUTING và POSTROUTING.
4. **Raw Table:** Được sử dụng để cấu hình xử lý gói cấp thấp. Nó có chế độ hợp lý các chuỗi, nhưng người dùng có thể tạo thêm các chuỗi nếu cần.
5. **Tấm lọc:** Được sử dụng để lọc gói tin. Bảng này có ba tích hợp: INPUT, OUTPUT và FORWARD.

Ở đây, **bộ lọc** chịu trách nhiệm lọc các gói theo quy tắc được xác định dựa trên nguồn và đích của IP địa chỉ, số cổng và loại giao thức. Và **Chains** có ba loại chuỗi tích hợp khác nhau.

Các loại chuỗi

Quy tắc chuỗi: Quy tắc được mô tả cho một công cụ cụ thể. Được chia thành ba loại:

1. **Bước VÀO:** Lọc lưu lượng truy cập vào hệ thống cục bộ.
2. **OUTPUT** : Lọc lưu lượng truy cập cho bộ hệ thống cục bộ.
3. **CHUYỂN TIẾP:** Các gói tin được chuyển tiếp từ hệ thống này sang hệ thống khác sẽ được chuyển tiếp.

Cấu hình tường lửa trên Hệ điều hành Linux
Chúng ta sẽ cấu hình iptables trong hệ điều hành của mình.

Để cài đặt iptables

```
sudo dnf cài đặt iptables
```

```
[root@localhost ~]# sudo dnf install iptables
```

Lệnh này được sử dụng để cài đặt iptables

Cú pháp cơ bản để sử dụng iptables

```
sudo iptables [option] Quy tắc CHAIN [-j item]
```

Ghi chú:

1. **Đầu ra chuỗi:** Lưu lượng truy cập qua các bộ máy cục bộ phải đi qua các đầu chuỗi này.
2. **Đầu vào chuỗi:** Lưu lượng phải đi từ mọi quy tắc được chỉ định trong đầu vào chuỗi.
3. **Chuyển tiếp chuỗi:** Lưu lượng truy cập từ mạng phát hiện vị trí khác đến mạng vị trí khác phải đi qua chuyển tiếp chuỗi.

Chúng tôi có một số biến thể iptables tùy chọn

Option	Description
-C	**[KIỂM TRA]:** Kiểm tra tra cứu và tìm quy tắc phù hợp với yêu cầu của chuỗi.
-D	**[XÓA]:** Dùng để xóa một quy tắc cụ thể.
-A	**[PHỤ LỤC]:** Dùng để bổ sung hoặc kết nối các quy tắc.
-I	**[INSERT]:** Thao tác này có thể thêm quy tắc vào một vị trí cụ thể trong chuỗi.
-L	**[LIST]:** Để hiển thị tất cả các quy tắc, chúng tôi có thể sử dụng điều này.
-v	**[VERBOSE]:** Được sử dụng để bổ sung thông tin trong danh sách tùy chọn.
-X	**[XÓA CHUỖI]:** Thao tác này xóa toàn bộ chuỗi được cung cấp.
-P	**[Protocol_name]:** Được sử dụng để xác định tên của giao thức.
-N	**[CHUỖI NEW]:** Để tạo một chuỗi mới.
-j	**[công việc]:** Nó cho biết bất kỳ hoạt động nào phải được thực hiện với gói tin.
-F	**[Flush]:** Xóa tất cả các quy tắc.
-S	**[chỉ định]:** Đây là cờ được sử dụng để chỉ định nguồn của gói.

Các vấn đề thường gặp về tường lửa và mẹo giải quyết sự cố
Chúng tôi có ba cơ sở chính sách. Hãy thảo luận về Một số cơ sở hoạt động và cú pháp của chúng

1. **DROP:** Có thể chặn tín hiệu đến, về cơ bản có nghĩa là chặn chặn đối với công cụ IP đó.
2. **CHẤP NHẬN:** Cho phép chúng tôi cung cấp IP để người dùng có thể truy cập vào hệ thống.

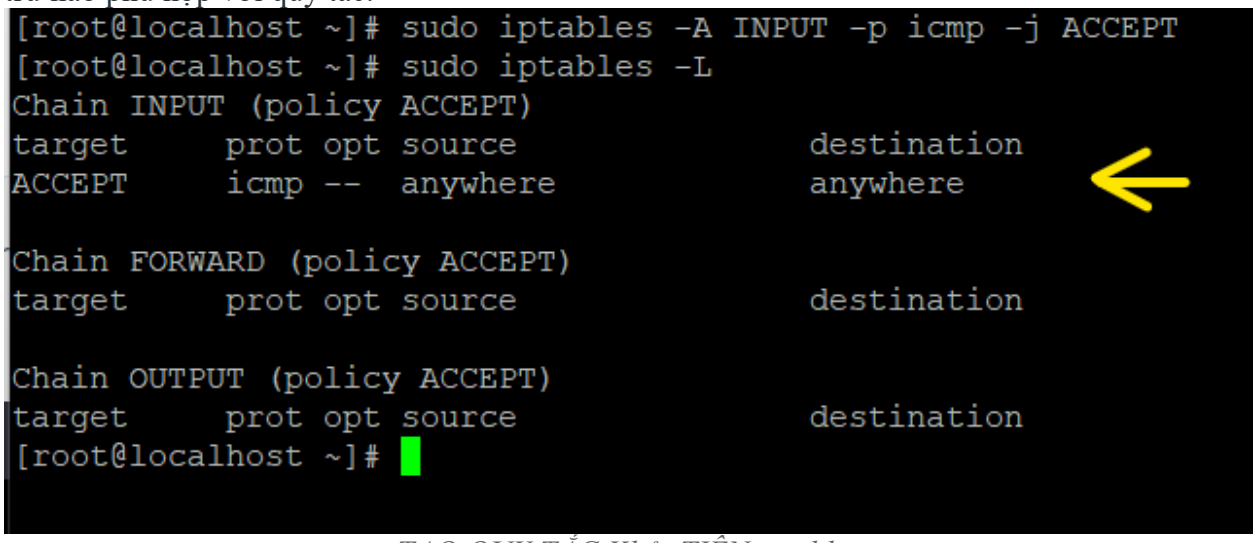
3. **REJECT:** Hoạt động tương tự như Drop, but in ' **drop** ', người gửi sẽ bị chặn mà không có bất kỳ thông báo nào trong khi ở ' **từ chối** ', một thông báo sẽ nêu lý do không thể kết nối.

Một số cơ sở hoạt động và cú pháp của chúng

Tạo quy tắc đầu tiên của chúng tôi
Quy tắc đầu tiên cho phép lưu trữ ICMP (ping) lượng trên INPUT chuỗi:

```
sudo iptables -A INPUT -p icmp -j CHẤP NHẬN
```

Sử dụng ' **-A** ' để thêm quy tắc vào INPUT chuỗi cuối. ' **-p icmp** ' cho biết quy tắc đang áp dụng cho lưu lượng ICMP. ' **-j ACCEPT** ' cho biết bạn chấp nhận (cho phép) bất kỳ lượng lưu trữ nào phù hợp với quy tắc.



TẠO QUY TẮC Khởi TIÊN iptables

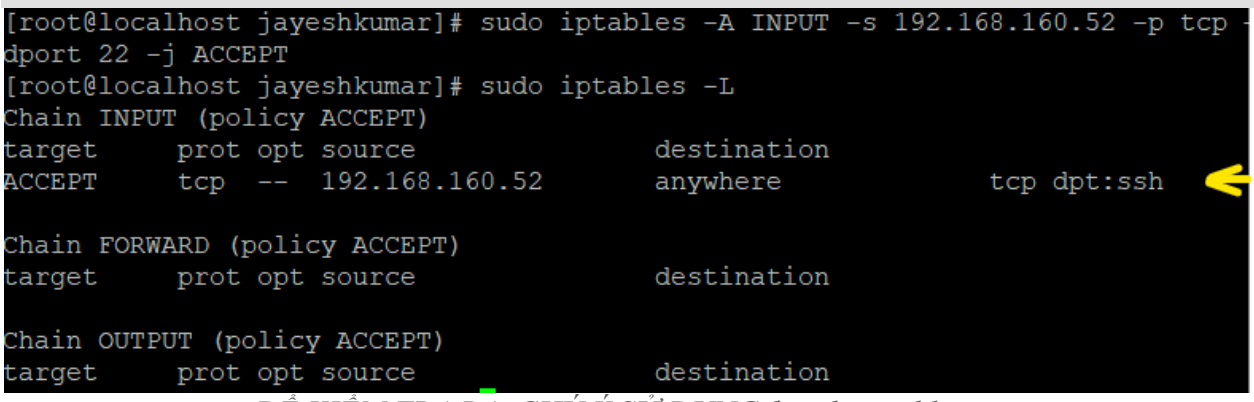
Cú pháp sử dụng chính sách

```
# Tham khảo ngữ cảnh được đề cập ở trên để xem trường hợp sử dụng của [ -I , -A , -p , -s ,-j ]

sudo iptables -I/-A name_chain -s source_ip -p Protocol_name --dport số cổng -j hành động_to_do
```

Ví dụ:
Quy tắc chấp nhận: Nếu chúng tôi phải chấp nhận IP (nguồn) 192.168.160.51 trên cổng số 22 bằng giao thức TCP.

```
sudo iptables -A INPUT -s 192.168.160.51 -p tcp --dport 22 -j CHẤP NHẬN
```



ĐỂ KIỂM TRA RA, CHÚ Ý SỬ DỤNG $ sudo iptables -L

Quy tắc xóa: If we must delete a IP (source) 192.168.160.51.

```
sudo iptables -A/-I chain_name -s source_ip -j action_to_do
```

```
[root@localhost jayeshkumar]# sudo iptables -A INPUT -s 192.168.160.51 -j DROP
[root@localhost jayeshkumar]# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.160.52       anywhere             tcp dpt:ssh
DROP       all  --  localhost.localdomain  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Như chúng ta có thể tìm thấy 192.168.160.51 đã bị xóa

Thiết lập lại quy tắc: Để thiết lập lại tất cả các iptables quy tắc, chúng ta sử dụng -F.

```
sudo iptables -F
```

```
[root@localhost jayeshkumar]# sudo iptables -F
[root@localhost jayeshkumar]# sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost jayeshkumar]#
```

Như chúng ta có thể thấy tất cả các quy tắc đã được thiết lập lại