
 Hãy nói theo cách của bạn	TRUNG TÂM GIẢI PHÁP CÔNG NGHỆ THÔNG TIN VÀ VIỄN THÔNG VIETTEL	Mã hiệu:
	HƯỚNG DẪN CÀI ĐẶT CẤU HÌNH IPTABLES	Ngày có hiệu lực:
		Ngày hết hiệu lực:
		Lần ban hành: 01
		Trang: 1/5

BẢNG THEO DÕI SỬA ĐỔI

STT	Trang	Nội dung sửa đổi	Ngày có hiệu lực

	Biên soạn	Kiểm tra	Phê duyệt
Chữ ký	CuongND10		

	TRUNG TÂM GIẢI PHÁP CÔNG NGHỆ THÔNG TIN VÀ VIỄN THÔNG VIETTEL	Mã hiệu:
	HƯỚNG DẪN CÀI ĐẶT CẤU HÌNH IPTABLES	Ngày có hiệu lực:
		Ngày hết hiệu lực:
		Lần ban hành: 01
		Trang: 2/5

1. Mục đích

- Ban hành hướng dẫn để thực hiện chuẩn hóa an toàn thông tin Firewall các hệ thống CNTT của Trung tâm Giải pháp Công nghệ thông tin và Viễn thông Viettel (VTICT).

2. Phạm vi áp dụng

- Áp dụng cho tất cả các máy tính ảo hóa và hệ thống chạy thật cho khách hàng tại Trung tâm Giải pháp Công nghệ thông tin và Viễn thông.

3. Nội dung

1. Giới thiệu về iptables

Iptables do Netfilter Organization viết ra để tăng tính năng bảo mật trên hệ thống Linux.

- Iptables cung cấp các tính năng sau:
- Tích hợp tốt với kernel của Linux.
- Có khả năng phân tích package hiệu quả.
- Lọc package dựa vào MAC và một số cờ hiệu trong TCPHeader
- Cung cấp chi tiết các tùy chọn để ghi nhận sự kiện hệ thống
- Cung cấp kỹ thuật NAT
- Có khả năng ngăn chặn một số cơ chế tấn công theo kiểu DoS

2. Cài đặt iptables

Iptables được cài đặt mặc định trong hệ thống Linux, package của iptables là iptables-version.rpm hoặc iptables-version.tgz ..., ta có thể dùng lệnh để cài đặt package này:

\$ rpm -ivh iptables-version.rpm đối Red Hat


\$ apt-get install iptables đối với Debian

- Khởi động iptables: service iptables start
- Tắt iptables: service iptables stop
- Khởi động lại iptables: service iptables restart
- Xác định trạng thái iptables: service iptables status

3. Cơ chế xử lý package trong iptables

Iptables sẽ kiểm tra tất cả các package khi nó đi qua iptables host, quá trình kiểm tra này được thực hiện một cách tuần tự entry đầu tiên đến entry cuối cùng.

Có ba loại bảng trong iptables:

	TRUNG TÂM GIẢI PHÁP CÔNG NGHỆ THÔNG TIN VÀ VIỄN THÔNG VIETTEL	Mã hiệu:
	HƯỚNG DẪN CÀI ĐẶT CẤU HÌNH IPTABLES	Ngày có hiệu lực:
		Ngày hết hiệu lực:
		Lần ban hành: 01
		Trang: 3/5

Mangletable: chịu trách nhiệm biến đổi quality of service bits trong TCPheader. Thông thường loại table này được ứng dụng trong SOHO (Small Office/Home Office).

Filter queue: chịu trách nhiệm thiết lập bộ lọc packet (packet filtering), có ba loại builtin chains được mô tả để thực hiện các chính sách về firewall (firewall policy rules).

- Forward chain : Cho phép packet nguồn chuyển qua firewall.
- Input chain : Cho phép những gói tin đi vào từ firewall.
- Output chain : Cho phép những gói tin đi ra từ firewall.

NAT queue: thực thi chức năng NAT (Network Address Translation), cung cấp hai loại built-in chains sau đây:

- Pre-routing chain: NAT từ ngoài vào trong nội bộ. Quá trình NAT sẽ thực hiện trước khi thực thi cơ chế routing. Điều này thuận lợi cho việc đổi địa chỉ đích để địa chỉ trong thích với bảng định tuyến của firewall, khi cấu hình ta có thể dùng khóa DNAT để mô tả kỹ thuật này.


Post-routing chain: NAT từ trong ra ngoài. Quá trình NAT sẽ thực hiện sau khi thực hiện cơ chế định tuyến. Quá trình này nhằm thay đổi địa chỉ nguồn của gói tin. Kỹ thuật này được gọi là NAT one-to-one hoặc many-to-one, được gọi là Source NAT hay SNAT.

- OUTPUT: Trong loại này firewall thực hiện quá trình NAT.

4. Target và Jumps

- Jump là cơ chế chuyển một packet đến một target nào đó để xử lý thêm một số thao tác khác.
- Target là cơ chế hoạt động trong iptables, dùng để nhận diện và kiểm tra packet. Các target được xây dựng sẵn trong iptables như:

- ACCEPT : iptables chấp nhận chuyển data đến đích.
- DROP: iptables khóa những packet.
- LOG: thông tin của packet sẽ gửi vào syslog daemon iptables tiếp tục xử lý luật tiếp theo trong bảng mô tả luật. Nếu luật cuối cùng không match thì sẽ drop packet. Với tùy chọn thông dụng là --log-prefix="string", tức iptables sẽ ghi nhận lại những message bắt đầu bằng chuỗi "string".

	TRUNG TÂM GIẢI PHÁP CÔNG NGHỆ THÔNG TIN VÀ VIỄN THÔNG VIETTEL	Mã hiệu:
	HƯỚNG DẪN CÀI ĐẶT CẤU HÌNH IPTABLES	Ngày có hiệu lực:
		Ngày hết hiệu lực:
		Lần ban hành: 01
		Trang: 4/5

- REJECT : ngăn chặn packet và gửi thông báo cho sender . Với tùy chọn thông dụng là -r eject-with qualifier, tức qualifier chỉ định loại reject message sẽ được gửi lại cho người gửi. Các loại qualifer sau: icmp-port-unr eachable (default), icmp-net-unr eachable, icmp-host-unr eachable, icmp-protocol-unreachable, ...

- DNAT : thay đổi địa chỉ đích của packet. Tùy chọn là --to-destination ipaddress.

- SNAT : thay đổi địa chỉ nguồn của packet. Tùy chọn là --to-source <address>[-address][:<port>-<port>]

- MASQUERADING: được sử dụng để thực hiện kỹ thuật NAT (giả mạo địa chỉ nguồn

với địa chỉ của interface của firewall). Tùy chọn là [--to-ports <port>[-<port>]], chỉ

định dải port nguồn sẽ ánh xạ với dải port ban đầu.

5. Thực hiện lệnh trong iptables


Iptables command Switch	Mô tả
-t <table>	Chỉ định bảng cho iptables bao gồm: filter, nat, mangle tables.
-j <target>	Nhảy đến một target chain khi packet thỏa luật hiện tại.
-A	Thêm luật vào cuối iptables chain.
-F	Xóa tất cả các luật trong bảng lựa chọn.
-p <protocol-type>	Mô tả các giao thức bao gồm: icmp, tcp, udp và all
-s <ip-address>	Chỉ định địa chỉ nguồn
-d <ip-address>	Chỉ định địa chỉ đích
-i <interface-name>	Chỉ định “input” interface nhận packet
-o <interface-name>	Chỉ định “output” interface chuyển packet ra ngoài

Ví dụ 1: Firewall chấp nhận cho 1 địa chỉ nguồn được chỉ định kết nối đến server port 22

```
# -A INPUT -s 10.61.68.93 -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

#####Cấu hình mặc định chặn gói tin đi vào:

```
-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

	TRUNG TÂM GIẢI PHÁP CÔNG NGHỆ THÔNG TIN VÀ VIỄN THÔNG VIETTEL	Mã hiệu:
	HƯỚNG DẪN CÀI ĐẶT CẤU HÌNH IPTABLES	Ngày có hiệu lực:
		Ngày hết hiệu lực:
		Lần ban hành: 01
		Trang: 5/5

-A FORWARD -j REJECT --reject-with icmp-host-prohibited

####Cấu hình ghi log truy cập trái phép

-A OUTPUT -j LOG --log-level debug --log-prefix "Dropped output by firewall: "

Cấu hình mặc định chặn gói tin đi ra

-A OUTPUT -j DROP