iptables and apache

魏凡琮 (Jerry Wei)

Agenda

- iptables
- apache

iptables

What is Firewall

- 用來防範未經允許的程式或使用者來存取內部資源的軟體或硬體。
- 依據封包資訊以及 ip header 的內容來進行過濾的一種機制。
- UTM (Unified Threat Management) 。

iptables

Firewall options

- Commercial firewall devices. (UTM)
  (Cisco PIX/ASA 、 Junpier SSG 、 Fortinet fortiGate...etc.)
- Router (ACL list.)
- Linux (tcp wrapper 、 iptables)
- Software Packages.
  (BlackIce 、 Norton personal firewall...etc.)

iptables

Linux Firewall

- ipfwadm (kernel 2.0.X)
- ipchains (kernel 2.2.X)
- iptables (kernel 2.4.X)

iptables

What is iptables

- Integration with Linux kernel (netfilter).
- Stateful packet inspection.
- Filter packets according to TCP header and MAC address.
- Network address translation (NAT).
- A rate limit feature.

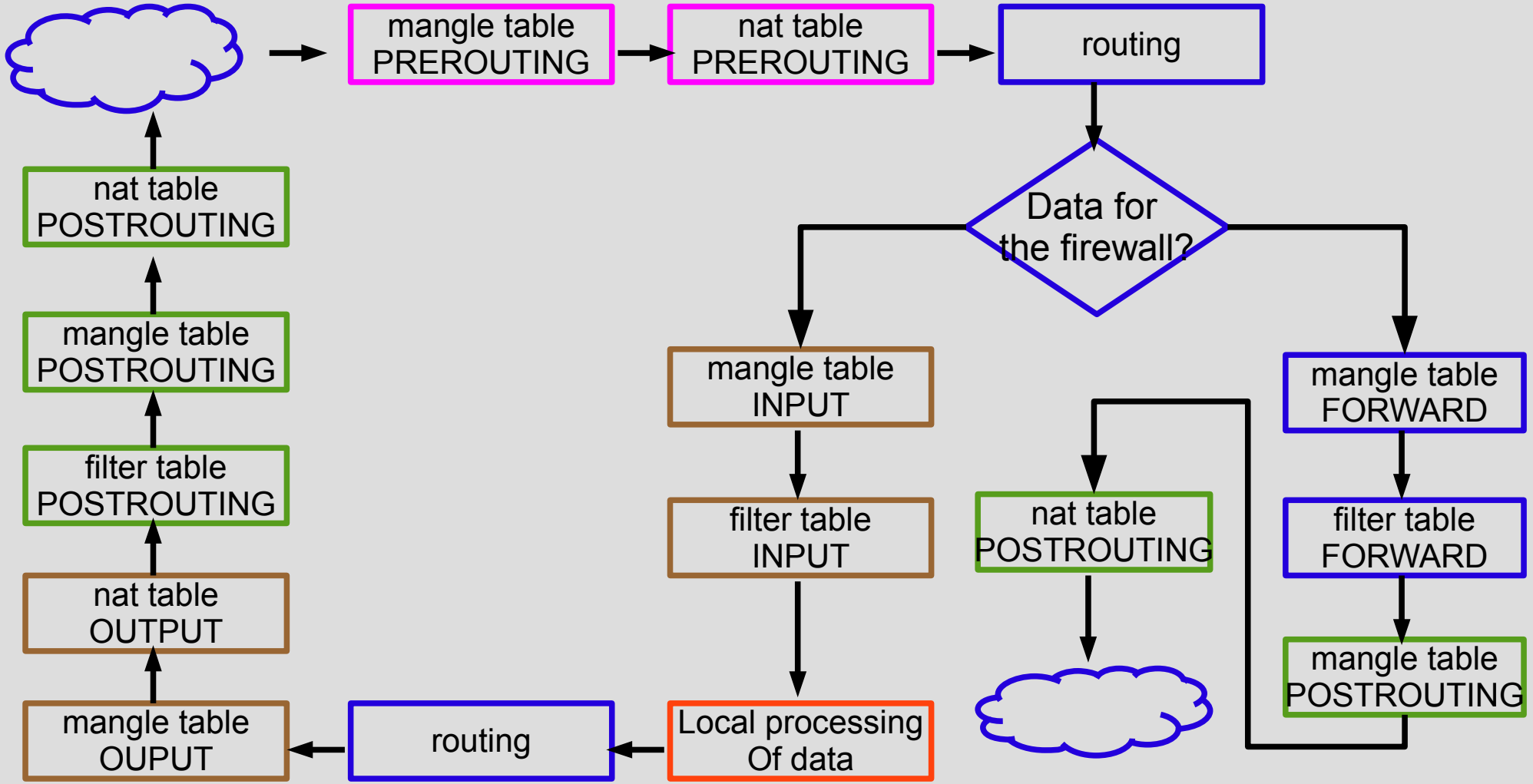
iptables

iptables rule table

- Filter ： packet filter.
(FORWARD 、 INPUT 、 OUTPUT)
- NAT ： network address translation.
(PREROUTING 、 POSROUTING 、 OUPUT)
- Managle ： TCP header modification.
(PREROUTING 、 POSTROUTING 、 OUTPUT 、 INPUT 、 FORWARD)

iptables

iptables flow



iptables

Tagets and Jumps

- ACCPET
- DROP
- REJECT
- LOG

iptables

Tagets and Jumps

- DNAT
- SNAT
- MASQUERADE

iptables

Command options 1

- -t [table]
- -j [target]
- -A ： Append rule to end of chain.
- -F ： Flush. Deletes all the rules in the selected table.
- -D ： Delete rule from the selected table.

iptables

Command options 1

- -p [protocol type] ： match protocol. tcp 、 udp 、 icmp 、 all.
- -s [ip address] ： match source ip address.
- -d [ip address] ： match destination ip address.
- -i [interface] ： match “INPUT “ interface on which the packet enters.
- -o [interface] ： match “OUTPUT “ interface on which the packet exits.

iptables

Example1-1

- iptables -A INPUT -i eth0 -p icmp -s 0/0 -d 0/0 -j DROP
- iptables -L --line-numbers
- iptables -A OUTPUT -o eth0 -p icmp -s 0/0 -d 0/0 -j DROP
- iptables -F
- iptables -P INPUT DROP 、 iptables -P OUTPUT DROP

iptables

Example1-2

- iptables -A INPUT -i eth0 -p icmp -s 0/0 -d 0/0 -j REJECT
- iptables -I INPUT -i eth0 -p icmp -s 0/0 -d 0/0 -j LOG
- iptables -I INPUT -i eth0 -p icmp -s 0/0 -d 0/0 -j ACCEPT

iptables

Command options 2

- -p tcp --sport {[port] | [start-port:end-port] }
- -p tcp --dport {[port] | [start-port:end-port] }
- -p tcp { --syn | !--sync }
- -p udp --sport {[port] | [start-port:end-port] }
- -p udp --dport {[port] | [start-port:end-port] }
- -p icmp --icmp-type [type]

iptables

Example2-1

- iptables -A OUTPUT -o eth0 -p tcp --sport 1024:65535 --dport 80 -j DROP
- iptables -A OUTPUT -o eth0 -p udp --dport 53 -j ACCEPT
- iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j DROP
- iptables -A OUTPUT -o eth0 -p icmp --icmp-type echo-reply -j DROP

iptables

Command options 3

- -m multiport --sports [port1,port2,port3]
- -m multiport --dports [port1,port2,port3]
- -m multiport --ports [port1,port2,port3]
- -m state --state [NEW | ESTABLISHED | RELATED | INVALID]
- -m limit --limit [rate]
- -m limit --limit-burst

iptables

Example3-1

- iptables -A OUTPUT -o eth0 -p tcp -m multiport --dports 53,80 -j DROP
- iptables -A OUTPUT -o eth0 -s 0/0 -d 0/0 -p tcp -m state --state ESTABLISHED -j ACCEPT
- iptables -A INPUT -i eth0 -p icmp -m limit --limit 1/s -j ACCEPT
- iptables -A INPUT -i eth0 -p icmp -m limit --limit-burst 2 -j ACCEPT

iptables

NAT

- DNAT / IP mapping / Port forwarding
- SNAT / MASQUERADE

iptables

DNAT

- Port forwarding.
- IP mapping

iptables

SNAT

- SNAT.
- MASQUERADE
- ip_forward

iptables

Example4-1

- iptables -t nat -A PREROUTING -p tcp -d 192.168.254.17 --dport 2222 -j DNAT --to 192.168.254.17:22
- iptables -t nat -A PREROUTING -i eth0 -d 192.168.254.17 -j DNAT --to-destination 10.20.1.2
- iptables -t nat -A POSTROUTING -o eth0 -s 10.20.1.2 -j SNAT --to-source 192.168.254.17
- iptables -t nat -A POSTROUTING -o eth0 -s 10.20.1.0/24 -j SNAT --to-source 192.168.254.17

iptables

Example4-2

- iptables -t nat -A POSTROUTING -o eth0 -s 10.20.1.0/24 -j SNAT --to-source 192.168.254.17
- iptables -t nat -A POSTROUTING -o eth0 -s 10.20.1.0/24 -j MASQUERADE

iptables

Mangle

- MARK
- TOS
  (IPV4 ： Type Of Service)
  (IPV6 ： set Traffic Control Value)
- TTL

iptables

Example5-1

- iptables -t mangle -A POSTROUTING -o eth0 -j TTL --ttl-set 1

iptables

Save and Restore

- iptables-save
- iptables-restore
- rc.local

Q & A

休息一下！

apache

Install

- wget “source tarball file”
- ./configure – prefix=/usr/local/apache-version --enable-rewrite
- make
- make install
- ./bin/apachectl { start | stop | restart }

apache

Configuration

- httpd.conf
- Virtual host
- .htaccess
- mod_rewrite

apache

VirtualHost

- Include vhosts.conf

apache

.htaccess

- Access control.
- ./htpasswd -c /usr/local/apache/conf/users csie
- User & group
- ./conf/groups

apache

.htaccess

- AuthName “Admin Login”
  AuthUserFile “/usr/local/apache/conf/users”
  AuthType Basic
  require valid-user
- AuthGroupFile “/usr/local/apache/conf/groups”
  require group

apache

mod_rewrite

- Provides a rule-based rewriting engineto rewrite request URLs.
- --enable-rewrite
- [NC] (no case) 、 [L] (last rule) 、 [R] (redirect)
- RewriteRule
- RewriteCond [OR] (or next)

Q & A

謝謝！