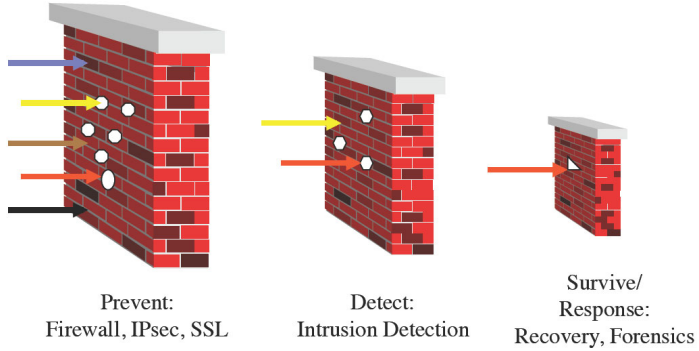
防火墙
以IPTABLES为例

1

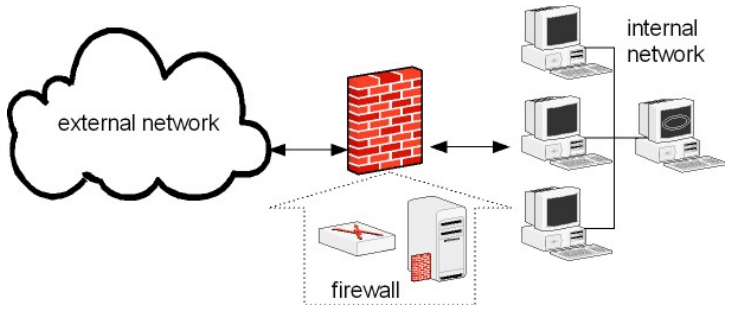
Multi-Layer Protection



2

3

Firewall Basics



4

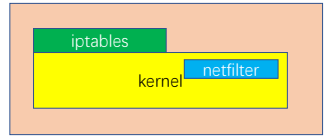
Firewall placement

TCP/IP layers

application	← application gateway 应用网关
transport	← circuit gateway 电路网关
network	← packet filtering 包过滤
data link	
physical	

5

Iptables



- Is an interface to the Netfilter firewall that is built-in to the Linux kernel
- It provides an administrator with an interface to add, remove, or modify packet rules
- http://www.netfilter.org/

6

四表五链

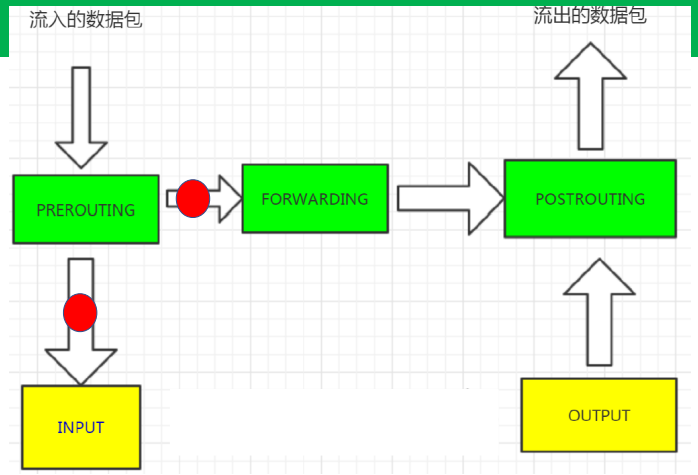
- iptables提供了一系列的表（tables）
- 每个表由若干链组成（chains）
- 每个链中有一条或数条规则组成（rules）

- Four tables：raw mangle nat filter
  - 按照上述顺序进行处理
- Five chains：Prerouting Input Forward Output Postrouting
  - iptables –t filter -L

7

- Prerouting:数据包进入路由表之前
- Input:通过路由表后目的地为本机
- Forward：通过路由表后目的地不为本机
- Output：由本机产生，向外转发
- Postrouting：发送到网卡接口之前

8



9

查看iptables现有规则

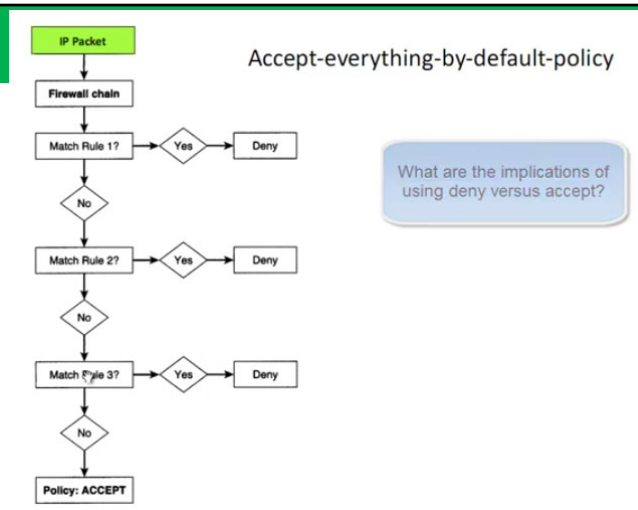
- iptables --help： 查看帮助文件
- iptables -L -n –v：查看iptables现有规则
- Iptables -N： 用户定义一个新链
- Iptables -F: 删除所有规则
- Iptables -X： 删除用户定义的链

10

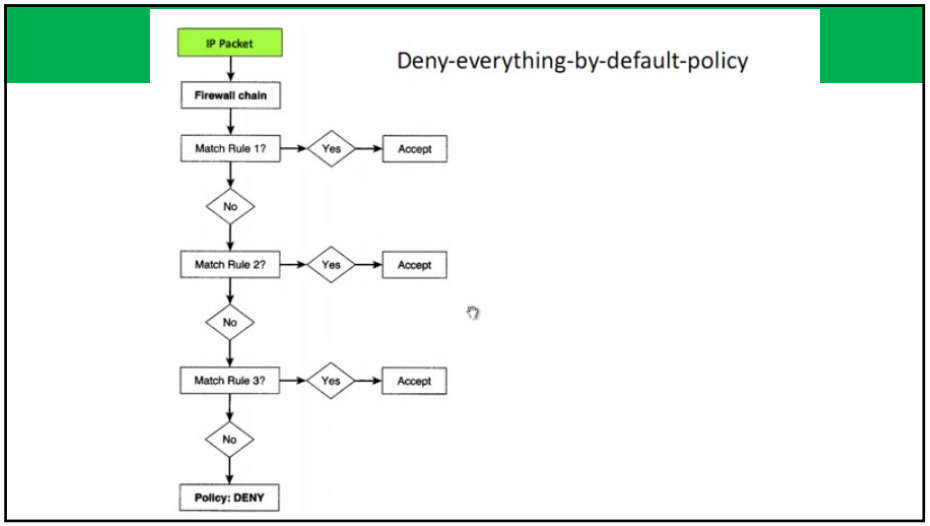
修改链的默认规则

- iptables -P INPUT DROP

11



12



13

删除链中的指定规则

- Iptables –nvL --line-number
- iptables –D INPUT 1

14

如何保存iptables规则

- 保存规则至指定的文件:
- iptables-save > /opt/iptables.1
- 从指定文件重载规则:
- iptables-restore < /opt/iptables.1

15

- -s 检查报文中的源地址
- -d 检查报文中的目标ip地址
- -p 传输层协议 tcp udp icmp
- -i --in-interface 数据报文的流入接口
- -o 数据报文的流出接口
- 下面的-j 是在做完了匹配规则之后，要怎么处理这些数据包:
- -j --jump target
- jump至指定的target
- 以下是target:
- ACCEPT：接受
- DROP：丢弃
- REJECT：拒绝

16

实验一：凡是由本机发出的TCP协议报文，都允许出去，其他协议不行

- iptables -A OUTPUT -s 本机IP -d 0.0.0.0/0 -p tcp -j ACCEPT
- iptables -P OUTPUT DROP #output的默认策略设置为DROP

- [root@test01 ~]# ping 127.0.0.1
- PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
- ping: sendmsg: 不允许的操作
- [root@test01 ~]# telnet 192.168.85.138 22
- Trying 192.168.85.138...
- Connected to 192.168.85.138.
- Escape character is '^]'.
- SSH-2.0-OpenSSH_7.4
- # telnet 可以成功，但是ping不允许

17

实验二：禁止ping本机

- iptables -A INPUT -s 0.0.0.0/0 -d 本机IP -p icmp -j DROP

- 查看本条规则是否生效

18

实验三：本机只开放tcp 22 端口，其余不允许

- iptables -I INPUT -d 本机IP -p tcp --dport 22 -j ACCEPT
- iptables -I OUTPUT -s 本机IP -p tcp --sport 22 -j ACCEPT
- iptables -P INPUT DROP
- iptables -P OUTPUT DROP
- iptables -P FORWARD DROP

19

实验四：开放多个端口

- iptables -I INPUT -s 0.0.0.0/0 -d 本机IP -p tcp --dport 22:80 -j ACCEPT

- 或者增加 -m multiport:

- iptables -I INPUT -s 0.0.0.0/0 -d 本机IP -m multiport -p tcp --dport 21,22:80,8443 -j ACCEPT

20

实验五：开放一段IP

- 特定的连续ip

- iptables -I INPUT -m iprange --src-range 192.168.85.126-192.168.85.138 -j ACCEPT
- iptables -I OUTPUT -m iprange --dst-range 192.168.85.125-192.168.85.139 -j ACCEPT

21

实验六：只允许ssh本机，不允许本机ssh其他主机

- [root@test01 ~]# iptables -I INPUT -d 本机IP -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
- [root@test01 ~]# iptables -I OUTPUT -s 本机IP -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
- [root@test01 ~]# iptables -P INPUT DROP
- [root@test01 ~]# iptables -P FORWARD DROP
- [root@test01 ~]# iptables -P OUTPUT DROP

22