Linux网关及安全应用 配置IPTABLES防火墙

1、在 RHEL5 系统中配置 iptables 防火墙规则，若需要禁止数据包通行且不反馈任何信息，应该采取的策略动作为（ ）。(选择一项)

A、ACCEPT B、DROP C、REJECT D、DENY

2、在 RHEL5 系统中，iptables 防火墙默认使用的规则表中不包括（ ）。 (选择两项)

A、raw B、input C、mangle D、forward

3、在 RHEL5 系统中，iptables 命令的（ ）选项可用于设置指定规则链的缺省策略。 (选择一项)

A、-A B、-D C、-P D、-X

4、在 RHEL5 系统中，依次执行了下列 iptables 规则设置语句，则根据该策略配置，从 IP 地址为 192.168.4.4 的客户机中 ping 防火墙主机的数据包将会被（ ）。 (选择一项)

iptables -F INPUT
iptables -A INPUT -p icmp -j REJECT
iptables -I INPUT -p icmp -s 192.168.4.0/24 -j LOG
iptables -I INPUT -p icmp -s 192.168.4.0/24 -j DROP
iptables -P INPUT ACCEPT

A、ACCEPT B、DROP C、REJECT D、LOG 之后 DROP

5、在 RHEL5 系统中可以使用 iptables 命令对系统中的网络防火墙策略进行查看和维护，当执行“iptables -L”命令时，将显示（ ）规则表的配置清单。 (选择一项)

A、nat B、filter C、mangle D、input

6、管理员在 linux 上使用 iptables 命令配置了防火墙，现要把配置保存，以便当计算机重启时恢复设置，他可以使用（ ）来实现。 (选择二项)

A、iptables-save > iptables B、iptables-restore < iptables
C、service iptables save D、service iptalbes restore

7、在 linux 中，防火墙的默认策略为 ACCEPT。管理员小李配置防火墙时，决定设置 INPUT 链的默认策略设置为 DROP，下面（ ）命令能够完成这一功能。 (选择一项)

A、iptables -X INPUT DROP B、iptables -L INPUT DROP
C、iptables -P INPUT DROP D、iptables -D INPUT DROP

8、管理员小李配置防火墙时，想把原有防火墙设置全部清空，以便全部重新设置。下面（ ）命令能够完成这一功能。 (选择一项)

A、iptables –F B、iptables –P C、iptables –D D、iptables -X

9、Linux 中防火墙的运行状态可以使用 iptables 命令进行查询，下面（ ）可以查询 filter 表中的所有链上的规则。 (选择一项)

A、iptables –A B、iptables –L C、iptables –F D、iptables –D

10、下面关于 Iptables 防火墙软件说法正确的是 （ ）。 (选择二项)

A、iptables 工作在应用层，属于应用层代理
B、iptables 工作在网络层，属于包过滤型防火墙
C、iptables 主要有 INPUT，OUTPUT，FORWARD，PREROUTING，POSTROUTING 五个规则链
D、iptables 工作在传输层，属于包过滤型防火墙

11、在 RHEL5 系统中，默认配置了 iptables 防火墙工具。一般的，iptables 维护着四种规则表和五条规则链，其中 Filter 规则表中包括规则链 （ ）。 (选择三项)

A、PREROUTING B、INPUT C、FORWARD D、OUTPUT E、POSTROUTING

12、在 RHEL5 系统中，若要禁止 IP 地址位于 61.23.45.0/24 网络的客户机访问本机的 WEB 服务，可以使用一下（ ）防火墙规则。 (选择两项)

A、iptables –I INPUT -s 61.23.45.0/24 -p tcp --dport 80 -j DROP
B、iptables –I INPUT -s 61.23.45.1-61.23.45.254 -p tcp --dport 80 -j DROP
C、iptables –I INPUT --src-range 61.23.45.1-61.23.45.254 -p tcp --dport 80 -j DROP
D、iptables –I INPUT -m iprange --src-range 61.23.45.1-61.23.45.254 -p tcp --dport 80 -j DROP

13、在 RHEL5 中系统中配置 iptables 策略时，若对符合条件的数据包进行（ ）处理，则目标主机将无法接收到此数据包。 (选择二项)

A、LOG B、ACCEPT C、DROP D、REJECT

14、在 RHEL5 服务器中开放了 FTP 服务 (21 端口)，若设置如下 IPTABLES 规则，则客户机 192.168.1.111

访问该 FTP 服务的数据包将会（　　）。（选择一项）
iptables –F
iptables –A INPUT –p tcp --dport 21 –j ACCEPT
iptables –A INPUT –p tcp –s 192.168.1.111 --dport 21 –j REJECT
iptables –P INPUT DROP
A、被允许　　B、被拒绝　　C、被丢弃　　D、一部分被允许，一部分被拒绝
15、在配置 RHEL5 系统的 iptables 防火墙时，执行（　）命令可以将当前的防火墙配置保存到
/etc/sysconfig/iptables 文件中。（选择一项）
A、service iptables reload　　B、iptables-save >/etc/sysconfig/iptables
C、iptables-restore</etc/sysconfig/iptables　　D、iptables--save-config
16、在 RHEL5 系统中,若需要禁止客户机 192.168.1.20 访问防火墙主机的 telnet 服务,可以添加如下(　　)。（选择二项）
A 、 iptables -A INPUT –p tcp –s 192.168.1.20 --dport 23 –j REJECT
B 、 iptables -A INPUT –p tcp –d 192.168.1.20 --sport 23 –j REJECT
C 、 iptables -A OUTPUT –p tcp –s 192.168.1.20 --dport 23 –j REJECT
D 、 iptables -A OUTPUT –p tcp –d 192.168.1.20 --sport 23 –j REJECT
17、公司有一台对外提供 Web 服务的运行 RHEL5 系统主机，为了防止外部对它的攻击，现在想要设置防火墙规则，使它只接受外部的Web 访问，其它的外部连接一律拒绝，可能的设置步骤包括:
1、iptables -A INPUT-p tcp-j DROP
2、iptable -A INPUT-P TCP--dport80-jACCEPT
3、iptable -F
4、iptable -P INPUT DROP
则对于上述 4 个步骤，以下（　　）组合能够实现该需求。（选择一项）
A、1-2-3　　B、2-4-3　　C、3-1-2　　D、3-4-2
18、在 RHEL5 系统中，若执行“iptables –A INPUT –i eth0 –s 192.168.1.0 /24 -j DROP”命令设置防火墙规则，则以下说法正确的是（　　）。（选择一项）
A、允许 192.168.1.0/24 网段的主机通过 eth0 接口访问本主机
B、拒绝 192.168.1.0/24 网段的主机通 eth0 接口访问本主机
C、系统重启后，该规则不再有效
D、允许本机通过 eth0 接口访问 192.168.1.0/24 网段的主机
19、在 RHEL5 系统中设置 iptables 规则时，以下（　）可用于匹配 192.168.0.20/24～192.168.0.50/24 范围内的源 IP 地址。（选择一项）
A、-s 192.168.0.20:50　　B、-s 192.168.0.20-50/24
C、-m iprange --src-range 192.168.0.20-50/24　　D、-m iprange --src-range 192.168.0.20-192.168.0.50
20、在安装 RHEL5 系统的网关主机中，通过正确设置 iptables 防火墙的（　）策略，可用于使局域网主机能够共享同一个公网 IP 地址访问 Internet。　（选择二项）
A、SNAT　　B、DNAT　　C、MASQUERADE　　D、REDIRECT
21、在 RHEL5 系统中，对于源地址、目标地址均不是防火墙本机但需要经过防火墙进行转发的数据包，将会经过 nat 表（　）链的规则处理。（选择二项）
A、OUTOPUT　　B、FORWARD　　C、PREROUTING　　D、POSTROUTING
22、在使用 RHEL5 系统的Linux 网关主机中，eth1 网卡IP 地址为 201.12.13.14.，用于连接 Internet。为了使
Internet 中的用户能够通过“http://201.12.13.14”的地址访问到局域网中的 Web 服务器 192.168.4.14，可以设置（　　）防火墙规则。（选择一项）
A 、 iptables –t nat –A PREROUTING -d 201.12.13.14 –p tcp --dport 80 –j MASQUERADE
B、iptables –t nat –A POSTROUTING -d 201.12.13.14 –p tcp --dport 80 –j MASQUERADE
C、 iptables – t nat – A PREROUTING -d 201.12.13.14 – p tcp --dport 80 – j DNAT --to-destination 192.168.4.14
D 、 iptables –t nat –A POSTROUTING -d 201.12.13.14 –p tcp --dport 80 –j DNAT --to-destination 192.168.4.14

23、使用 RHEL5 系统构建网关服务器,在 iptables 防火墙的 nat 表中正确设置(　　)策略,可用于在 Internet 网络中发布位于局域网内的应用服务器。（选择一项）

A、SNAT　　B、DNAT　　C、MASQUERADE　　D、REDIRECT

24、在 RHEL5 系统中设置 iptables 防火墙规则时，DNAT 策略只能在 nat 表的（ ）规则链中使用 (选择两项)

A、PREROUTING　　B、POSTROUTING　　C、OUTPUT　　D、FORWARO

25、管理员小张在网络中利用 NAT 服务器进行地址转换，使公司局域网中的计算机可以利用 NAT 服务器访问 Intenet。这时当局域网中的计算机向 Internet 中的某个主机发送请求时，NAT 服务器将数据包的（　　）转换为 NAT 服务器的公网地址。（选择一项）

A、源地址　　B、目标地址　　C、源端口号　　D、目标端口号

27、在 RHEL5 系统中重新编译 Linux 内核，执行“make menuconfig”步骤后保存的内核配置文件名默认为（　　）。（选择一项）

A、.config　　B、.config-2.6.28.8　　C、makefile　　D、kernel.cfg

28、在 RHEL5 系统环境中，若需要设置从 Internet 远程管理位于公司局域网的内部服务器，可使用 iptables 的（　　）策略实现。（选择一项）A、SNAT　　B、DNAT C、MASQUERADE　　D、REDIRECT

29、在 RHEL5 系统中，若需要配置 iptables 防火墙使用内网用户能够共享网关主机的公网 IP 地址上网，可以在（　　）中设置 MASQUERADE 地址伪装策略。（选择一项）

A、filter 表内的 OUTPUT 链　　B、filter 表内的 FORWARD 链

C、nat 表中的 PREROUTING 链　　D、nat 表中的 POSTROUTING 链

B、