

老男孩教育运维班必会 iptables 面试题

老男孩教育因为优秀所以优秀，作为老男孩学生的一员，你要不要一样优秀？

要求：大家务必会笔答，会熟练口头表达，面试完败其他竞争的面试者

（一）基础口试题

- 1、详述 iptables 工作流程以及规则过滤顺序？
- 2、iptables 有几个表以及每个表有几个链？
- 3、iptables 的几个表以及每个表对应链的作用，对应企业应用场景？
- 4、画图讲解 iptables 包过滤经过不同表和链简易流程图并阐述。
- 5、请写出查看 iptables 当前所有规则的命令。
- 6、禁止来自 10.0.0.188 ip 地址访问 80 端口的请求
- 7、如何在命令行执行的 iptables 规则永久生效？
- 8、实现把访问 10.0.0.3:80 的请求转到 172.16.1.17:80
- 9、实现 172.16.1.0/24 段所有主机通过 124.32.54.26 外网 IP 共享上网。
- 10、描述 tcp 3 次握手及四次断开过程？
(课外参考：<http://user.qzone.qq.com/49000448/blog/1426987479>)
- 11.详细描述 HTTP 工作原理？
- 12.请描述 iptables 的常见生产应用场景。
- 13、请描述下面 iptables 命令的作用
iptables -N syn-flood
iptables -A INPUT -i eth0 -syn -j syn-flood
iptables -A syn-flood -m limit -limit 5000/s -limit-burst 200 -j RETURN
iptables -A syn-flood -j DROP
- 14、企业 WEB 应用较大并发场景如何优化 iptables？

（二）企业运维面试题：

- 15、写一个防火墙配置脚本，只允许远程主机访问本机的 80 端口（奇虎 360 面试题）
(<http://user.qzone.qq.com/49000448/blog/1429755081>)

16、请描述如何配置一个 linux 上网网关？

17、请描述如何配置一个专业的安全的 WEB 服务器主机防火墙？

18、企业实战题 6：请用至少两种方法实现！

写一个脚本解决 DOS 攻击生产案例

提示：根据 web 日志或者网络连接数，监控当某个 IP 并发连接数或者短时内 PV 达到 100，即调用防火墙命令封掉对应的 IP，监控频率每隔 3 分钟。防火墙命令为：iptables -A INPUT -s 10.0.1.10 -j DROP。

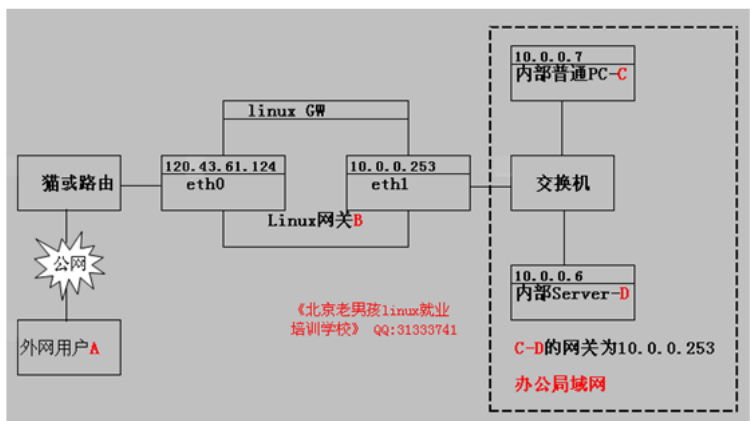
（此题来自老男孩教育 SHELL 编程必会考试题之一）

19、/var/log/messages 日志出现 kernel: nf_conntrack: table full, dropping packet.请问是什么原因导致的？如何解决？

20、压轴上机实战 iptables 考试题

■ 老男孩教育课堂案例企业面实战试题

已知企业内部架构如图：



要求：

1.实现普通 PC-C 可经过 Linux 网关 B，上因特网浏览网页等。

2.实现外部用户 A 通过访问 linux 网关 B 120.43.61.124:80，即

可访问到内部 Server D 10.0.0.6:80 提供的 web 服务(假设已配好)。

请分别给出命令完整实现细节(操作目标机 Linux 网关 B)？

3.假如 1,2 都配好了，但是问题出在内网普通 PC-C 和内部 Server D

没有配置正确的网关，如何通过 tcpdump 来排查出来。

4.如何保证内部普通 PC-C 能够通过访问 120.43.61.124:80 也访问到内部 Server D

注：本试题全部摘自老男孩教育运维班课堂讲过的内容，课程不断，精彩不断，老男孩教育国内最优秀的教育机构，教学效果全国 NO1。