 显然，防护网络的第一步是防护网络中的所有计算机，包括个人工作站和服务器。然而，这只是网络安全的一部分，防火墙必不可少，大多数专家还建议用IDS，有许多IDS可供选择，有些甚至还是免费的。IDS可以检测攻击行为，像端口扫描，这可能预示着有人尝试侵入网络边界安全。 假如网络很大，就要考虑用带防火墙的路由器把网络分成若干部分，这样的话，一个部分发生问题，不会影响成个网络。这里，可以考虑把所有重要的服务器都放在一个安全区域内，这通常叫DMZ区。 如Web服务器是对外提供服务的，并且最常受到攻击，把他们单独放在一个区域内是比较合理的。许多网络管理员会考虑在Web服务器与其它网络之间再放一个防火墙。这样的话，骇客就算利用服务器漏洞侵入了Web服务器，也不能进入整个网络。同时，一定要有策略指导用户如何使用系统，再健壮的安全系统都会因为用户的稍不注意而功亏一篑。一定要记住必须要有安全策略指导用户哪些能做，哪些不能做。 在加固服务器（打补丁，关闭不必要的服务等）的同时，也需要加固路由器。如何加固路由器需要咨询相应的安全厂商，但是这里有一些基本原则： 1、使用强壮的密码：所有的路由器都可配置。因此，必须要遵循统一的安全策略，最少字符、复杂度、生存期、密码历史等要求。如果路由器支持加密（如Cisco及一些大厂商），那么最好加密。 2、使用日志：大多数路由器有日志功能。应该把此功能打开，就像监视

服务日志那样。 3、安全原则：一些基本的路由安全准则要遵守。 4、不要响应非本地网络内主机的ARP（Address Resolution Protocol，地址解析协议）。 5、网络内不需要端口应该在路由器关闭。 6、不是从本地网络内发起的数据不予转发（此条为企业网原则，不适用于透传情况）。 以上是总体原则。好了，还是理一下防护网络的常规动作吧。分为两个级别：一般级和增强级。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com