教你怎样全方位打造安全高效的上网环境 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/264/2021_2022__E6_95_99_E4_BD_A0_E6_80_8E_E6_c67_264845.htm 对多数企业来说，互联网不仅带来了丰富的网上资源，也把信息化带进了企业，使得企业传统运作方式迎来了深刻的变革。互联网极大地陈低了组织的运营和沟通成本，利用互联网，大多数员工可以更高效率的完成工作。 但是，作为一把“ 双刃剑 ”，互联网也给组织和企业带来前所未有的威胁。全天候24小时在网络上流动的内容当中，存在着太多的风险：垃圾邮件、恶意网站、网上欺诈、网络病毒等无时无刻不在困扰着互联网用户，而另外一方面，网络滥用行为，包括恶意的P2P下载、网络游戏、IM等娱乐应用挤占了组织有限的业务带宽，同样导致网络应用效率低下。 那么，如何绕开这些互联网弊端，充分享受互联网给组织带来的方便与高效，从而全方位打造安全高效的上网环境呢？ 一、提升边界防御 防火墙、IDS、IPS，是解决网络安全问题的基础设备，他们所具备的过滤、安全功能能够抵抗大多数来自外网的攻击。配备这些传统的网络防护设备，实现面向网络层的访问控制，是企业安全上网的前提。然而，在应用内容及其格式以爆炸速度增长的今天，许多互联网危害隐患存在于应用层中，仅仅依照第三层信息决定其是否准入，根本无法满足安全的要求，我们还需要细粒度的应用层策略控制。 IDC的调查报告显示，至2006年，有超过90%的病毒将互联网作为其传播入口，通过电子邮件和网络进行病毒传播的比例正逐步攀升，在网络入口处把住病毒入侵的关口成了当务之急，因此，除了上述的防火墙

、IDS、IPS等基础安全设备，你还需要部署一个有效的网关级杀毒引擎。 二、上网终端管理 网络边缘的外围设备再先进也无法保护内部网络，来自局域网内部的滥用、破坏也是威胁上网安全的重要因素。比如，客户端的安全级别往往难以保证，这对于内网用户数量众多的组织更为如此缺乏安全措施的单机，比如使用陈旧的操作系统、长时间不更新个人防火墙和杀毒软件、应用具有潜在安全漏洞的软件，都将成为局域网安全中一颗颗隐藏的定时炸弹。 为上网终端配置网络准入规则，通过对单点的安全评估和访问策略列表是实现客户端全方位安全防护的最佳手段。对终端的安全策略列表应该包括操作系统、运行程序、系统进程、注册表等。 三、有害内容过滤 互联网是一个不可控的黑洞，无数不怀好意的网站使你上网冲浪时如履薄冰：隐藏蠕虫病毒、木马插件的非法网站，各类层出不穷的钓鱼网站……都会让组织在分享互联网便利的同时带来巨大的隐患。 针对这些有害内容，URL库过滤技术近年来得到广泛采纳，采用该技术将包含潜在威胁的网站拦截在外是保障上网安全的有效方式之一，当然，还应该考虑到一些钓鱼网站采用的是SSL加密页面，所以还需要结合证书验证、链接黑白名单等措施。对文件下载传输行为进行规范也是必要的，将关键字、文件类型、网络服务与IP地址组进行关联，规范下载策略，可以控制大部分由主动下载造成的损害。 四、垃圾邮件过滤 还有一些不那么“ 有害 ”的信息垃圾邮件，虽然未必会造成安全隐患，但却能导致带宽利用率，更重要的是工作效率的低下。 为了最大程度的减少这些影响带宽利用率及工作效率的无用信息，必须找到一种区分垃圾邮件、正常邮件、可疑邮件的有效手段，比

如垃圾邮件指纹识别技术，减少误判的随机特征码智能应答技术等。 五、优化带宽资源 不管采取什么方式上网，带宽终究是有限的，在无法改变带宽的前提下，如何优化带宽资源，使其效率最高，是必须解决的问题。但现实的问题是，网管员对自己单位内部的带宽有效利用情况无从获知，就更谈不上改善了。 要做到优化带宽资源，首先要考察内网网络使用情况，并形成可供决策的报表，有些厂商提供的数据中心就已经可以提供丰富的报表分析功能。另外，针对网内一些重要的网络服务，也有必要启用QOS技术，从而保证重要的服务先行，避免垃圾流量挤占重要服务的带宽。 六、全面应用管理 全球每天有120亿条消息通过即时通讯工具（Instant Messaging，IM）被发送，这些IM应用也许是员工在和同事、客户讨论工作，但更多的聊天对象却是家人、朋友甚至是陌生人。此外，网络上还有其它大量的和工作无关网络应用存在，包括网络游戏、在线炒股、P2P下载等，这些工作时间内的“ 丰富应用 ”造成了组织生产效率的巨大浪费。有些组织靠封端口、封服务器地址等方法在一定程度上有效，但由于服务器地址和端口会经常变换，这导致封服务器地址和端口成为一项持续的高成本工作，只能是治标不治本。 在全面应用管理上更有效的封堵方法主要有两种，一种是基于应用协议和数据包的智能分析，另一种是针对流量进行检测。前者是通过分析IP数据包首部的服务类型、协议、源地址、目的地址以及数据包的数据部分，能够更好的发现特定服务。后者则可以针对特定用户的网络连接情况进行分析，当网络流量和网络连接超出规定的阀值时，用户的行为将被限制流量。 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