8种手段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_ti2020/166/2021_2022_8_E7_A7_8D_E6_89_8B_E6_AE_B5_c101_166616.htm 编者按：长期以来，组织管理者为了营造一个安全高效的网络应用环境采取的是传统管理方式，如拟定各种规章制度、使用守则、奖惩措施等。实际上，解铃还需系铃人，信息技术带来的负面影响最终还是要靠信息技术来解决。好的上网环境的建设是一个周密的系统工程，以下8种手段及所提供的SINFOR AC上网行为管理解决方案为我们打造安全高效的上网环境提供了一个开阔的思路。 这是一个充满变革的时代，94年一条64k的数据线第一次将我国接入世界，到今天，从政府、企业、医疗、教育……各行各业都广泛的使用互联网来获取无数的信息和机会。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?下面8种手段或许能给你答案。 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。七、外发信息审计 互联网对企业还有一个重要的危害是信息的过度流动。由于它是一个开放系统，只要使用者轻点鼠标，企业与组织的机密信息就能瞬间以光的速度到达竞争对手那里。而一些攻击性、侮辱性的网络漫骂/谣言，则可能会导致组织不必要的内部纠纷。另外，内部员工通过组织网络随意发表的言论，也可能给组织带来法律上的风险。 要防范这些风险，应该从IM、HTTP、FTP、EMAIL等各个可能的出口，对外发信息进行审计和监控。所采取的措施应该包括记录与保存，对关键字的审计，甚至对一些关键的信息进行延迟审计。八、应用权限设置 以上多种手段基本上可以满足一个安全高效的上网环境的建设，然而，一个组织内部，不同部门，不同人员，倘若对网络应用都拥有同样权限，注定会使网络出于低效、危险的境地。所以在这里我们有必要再介绍一下应用权限方面的管理。 对网络用户进行权限设置是一种很好的分级管理的措施。就流量优化而言，传统的带宽管理只能对特定服务分配相应的百分比带宽，属于“ 一刀切 ”行为。更具效力的网络流量优化方式是基于用户的流量控制技术，再

结合各种不同应用的角色分配，可以有更好效果。具体说来，在广域网的访问中，有些部门的特殊应用是应该而且必须获得独占性资源的，例如总部的管理层同各分公司主管召开的视频会议，而有些部门的非工作相关服务则不应获得那么高的带宽，例如采购部门的P2P下载。通过分组流量控制,你可以对不同用户组使用的服务进行精细的带宽分配，保障重要部门的重要服务得到足够带宽。 除了服务管理，时间计划也是网络管理中的重要手段，这包括微观时间管理和宏观时间管理，前者包括将一周中每一天的时间进行划分，在特定时间允许特定部门进行特定活动，后者包括为各个部门的员工设置一周内每天的总上网时间，这是保证网络利用效率最大化的好手段。 长期以来，组织管理者为了营造一个安全高效的网络应用环境采取的是传统管理方式，如规章制度、使用守则、奖惩措施等。实际上，解铃还需系铃人，信息技术带来的负面影响最终还是要靠信息技术来解决。好的上网环境的建设是一个周密的系统工程，以上8种手段给我们打造安全高效的上网环境提供了一个开阔的思路。 当然，以上8种技术手段的应用，往往需要组织购买不同的IT设备：比如“一、提升边界防御”和“四、垃圾邮件过滤”需要购买相应的网关杀毒设备和防垃圾邮件设备，而“二、上网终端管理”则需要部署相应的客户端安全软件，“五、优化带宽资源”目前有一些专门做流量控制的厂商能够提供，如F5、Packeteer，但往往费用很贵，“七、外发信息审计”则涉及到一些监控审计设备.而“三、有害内容过滤”、“六、全面应用管理”、“八、应用权限设置”由于是新兴领域，目前还基本没有专门的厂商涉足。 购买这些不同的IT设备，一

方面动辄几十万甚至上百万的费用投入对于大部分的用户来说都是难以接受的，另一方面由于这些设备分别来自不同厂商，管理界面各异，对IT维护和管理也是个巨大的挑战和难题。 那么，有没有这样的一种解决方案，把以上8种技术手段都融入到一个设备里面，从而便捷灵活的实现对整个局域网上网行为的有效管理呢?我们很高兴的看到国内近几年快速成长的网络安全及边界网络方案供应商深信服科技提供了这样一种解决方案SINFOR AC上网行为管理设备。该设备包含“ 访问控制、带宽流量管理、内监控、安全审计、外发信息管理及数据中心管理软件 ”多个模块功能，并拥有“ 邮件延迟审计 ”、“ 网络客户端准入 ”、“ P2P流量控制 ”等多项专利技术，此外，它还灵活的集成了“ 防火墙 ”、“ 网关杀毒 ”、“ 防垃圾邮件 ”等UTM安全模块，客户可以根据自己的网络环境和实际需求灵活选择是否开启，有效弥补了防火墙等传统安全设备重外不重内、对上网行为缺乏有效管理的不足。 在提升边界防御和有害内容过滤方面，深信服AC设备内置了网关杀毒的模块，同时针对病毒的来源和传播途径，AC上网行为管理设备还可以很好的配合客户原有的杀毒软件实现“ 治标治本 ”的效果。AC网关里面的URL过滤功能，可以对常见的非法网址/非法BBS论坛直接实现过滤，AC网关提供的对HTTP/FTP下载及P2P软件的封堵和管理功能也可以有效减少因为文件下载而引发的病毒传播。尤其值得一提的是AC里面的SSL控制功能，可控制用户通过SSL协议访问的URL，并可对SSL协议的证书做有效性检查，允许或拒绝用户访问持有指定X.509证书的网站，大大降低了用户被伪造的网上银行、购物网站欺骗的几率，避免用户陷入“ 网络钓鱼 ”陷阱。

在上网终端安全管理方面，深信服AC上网行为管理设备提供了一个“客户端准入规则”(Network Admission Rules，NAR)认证的功能，可以通过对客户端安全性的评估来实现网络访问控制，更好的维护网络安全防线。当启用了AC的NAR功能后，内网用户第一次发起互联网连接请求时，NAR将动态分发准入代理(Sinfor Ingress Agent，SIA)至客户端主机。SIA是轻量级软机代理，用于确定终端是否遵从管理员设定的安全策略，SIA可检查预定义的和可定制的标准，比如该PC终端有没有打最新的操作系统补丁、有没有安装杀毒软件、杀毒软件有没有升级到最新版本。当SIA将搜集到的客户端信息传回AC网关后，如果该PC终端的安全状态不符合SIA的规则设置，AC网关将对该用户执行预定义的策略，比如直接禁止上网或弹出警告，从而有效避免某些员工因为忙碌或者偷懒而不安装杀毒软件和打补丁，或者虽然安装了杀毒软件但没有做及时升级而引发的病毒事件。 在用户身份认证、应用权限设置和外发信息审计方面，深信服AC网关采用了严格的身份认证和不同的访问权限策略，并可根据不同的时间段做灵活的时间管理，具有URL过滤、关键字过滤、上传下载限制、深度内容检测、邮件过滤功能和独特的邮件延迟审计功能等众多功能，从而方便组织和企业把与工作无关的上网行为降到最低，让员工更专注于工作，提高工作效率，并在技术措施上配合制度管理杜绝了内部机密可能通过Internet泄漏的隐患。 在优化带宽资源方面，AC设备网关除了提供智能QOS，还为用户展现了强大的流量控制功能，可以对内网用户组或终端进行流量控制，使得组织的网络带宽得到最充分有效地利用。 此外，深信服AC网关丰富的数据报表中心还能支持以

图表的方式对局域网内人员的上网行为进行分析和归纳，如：每天上网情况的分析、访问最频繁的网站分析、应用和流量排名等，并提供时间、服务、网站访问、使用网络流量等多种分类排行榜，为网络管理员和决策者提供了最直观的数据统计。