解决方案：应用层安全解决方案新篇 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/202/2021_2022__E8_A7_A3_E5_86_B3_E6_96_B9_E6_c40_202920.htm 背景: 金税工程是国家电子政务建设十二个系统中重点建设的一个系统，它的建设不仅有利于强化我国税收管理，促进税收征管改革的深化，而且为国家其它电子政务建设项目提供了丰富的共享数据源，有利于政府部门之间建立信息共享和协作关系，有利于国家电子政务建设的全面推进。随着互联网的普及和安全技术的应用，税务系统面向个人的业务逐步在互联网上开展，目前网上保税包括车船税、代扣税、一般印花税等，而一系列的安全威胁成为税务网络建设中必须要解决的问题，如邮件病毒、蠕虫、间谍软件欺骗等，这些都是税务系统开放面向互联网业务的过程中无法避免的，面对种种的安全威胁华为3Com提出了深度安全解决方案、推出面对应用层威胁的解决办法。 1. 应用层威胁介绍 2000年以前，当我们谈及网络安全的时候，还主要指防火墙，因为那时候的安全还主要以网络层的访问控制为主。的确，防火墙就像一个防盗门，给了我们基本的安全防护。但是，就像今天最好的防盗门也不能阻止“ 禽流感 ”病毒传播一样，防火墙也不能阻挡今天的网络威胁的传播。今天的网络安全现状和2000年以前相比，已经发生了很大的改变，我们已经进入了一个“ 应用层威胁 ”泛滥的时代。 今天，各种蠕虫、间谍软件、网络钓鱼等应用层威胁和EMAIL、移动代码结合，形成复合型威胁，使威胁更加危险和难以抵御。这些威胁直接攻击企业核心服务器和应用，给企业带来了重大损失.攻击终端用户计算机，给用户

带来信息风险甚至财产损失.对网络基础设施进行DoS/DDoS攻击，造成基础设施的瘫痪.更有甚者，像电驴、BT等P2P应用和MSN、QQ等即时通信软件的普及，企业宝贵带宽资源被业务无关流量浪费，形成巨大的资源损失。面对这些问题，传统解决方案最大的问题是，防火墙工作在TCP/IP 3～4层上，根本就“ 看 ”不到这些威胁的存在，而IDS作为一个旁路设备，对这些威胁又“ 看而不阻 ”，因此我们需要一个全新的安全解决方案。 在解决问题之前，我们需要先了解一下应用层威胁的形式和原理。所谓应用层威胁，主要包括下面几种形式: 图1、应用层威胁 我们重点介绍一下蠕虫、间谍软件、带宽滥用这三个典型的应用层威胁。 1.1. 蠕虫 蠕虫的定义是指“ 通过计算机网络进行自我复制的恶意程序，泛滥时可以导致网络阻塞和瘫痪 ”。从本质上讲，蠕虫和病毒的最大的区别在于蠕虫是通过网络进行主动传播的，而病毒需要人的手工干预(如各种外部存储介质的读写)。但是时至今日，蠕虫往往和病毒、木马和DDoS等各种威胁结合起来，形成混合型蠕虫。 蠕虫有多种形式，包括系统漏洞型蠕虫、群发邮件型蠕虫、共享型蠕虫、寄生型蠕虫和混和型蠕虫。我们重点谈谈“ 系统漏洞型蠕虫 ”，系统漏洞型蠕虫利用客户机或者服务器的操作系统、应用软件的漏洞进行传播，成为目前最具有危险性的蠕虫。以冲击波蠕虫为例，它就是利用Microsoft RPC DCOM 缓冲区溢出漏洞进行传播的。系统漏洞型蠕虫传播快，范围广、危害大。例如2001年CodeRed的爆发给全球带来了20亿美金的损失，而SQ@Slammer只在10分钟内就攻破了全球!下面是近5年来针对微软操作系统漏洞的5个最著名的蠕虫: @红色代码(CodeRed): MS01-033，微软索引服

务器缓冲区溢出漏洞，利用TCP 80传播 @SQ@SLAMMER: MS02-039，SQL服务器漏洞，利用UDP 1434进行传播 @冲击波(Blaster) MS03-026，RPC DCOM服务漏洞，利用TCP 135 139等等进行传播 @震荡波(Sasser): MS04-011，LSASS本地安全认证子系统服务漏洞，利用TCP 445等端口进行传播 @Zobot MS05-39，windows PnP服务漏洞，利用TCP 445端口进行传播 上述5个蠕虫都是臭名昭著的蠕虫，其中Zobot到2005年12月还在网络上肆虐着它的余威。由于系统漏洞型蠕虫都利用了软件系统在设计上的缺陷，并且他们的传播都利用现有的业务端口，因此传统的防火墙对其几乎是无能为力。实际上，系统漏洞是滋生蠕虫的温床，而网络使得他们可以恣意妄为。1.2. 间谍软件 网络安全专家对于什么是“ 间谍软件 ”一直在讨论。根据微软的定义，“ 间谍软件是一种泛指执行特定行为，如播放广告、搜集个人信息、或更改你计算机配置的软件，这些行为通常未经你同意 ”。 严格说来，间谍软件是一种协助搜集(追踪、记录与回传)个人或组织信息的程序，通常是在不提示的情况下进行。广告软件和间谍软件很像，它是一种在用户上网时透过弹出式窗口展示广告的程序。这两种软件手法相当类似，因而通常统称为间谍软件。而有些间谍软件就隐藏在广告软件内，透过弹出式广告窗口入侵到计算机中，使得两者更难以清楚划分。 间谍软件主要通过Active X控件下载安装、IE浏览器漏洞和免费软件绑定安装进入用户的计算机中，间谍软件的危害主要体现如下: @间谍软件对企业已形成隐私与安全上的重大威胁。这些入侵性应用程序搜集包括信用卡号码、密码、银行账户信息、健康保险记录、电子邮件和用户存取数据等敏感和机密的公司信息

后，将之传给不知名的网站而危及公司形象与资产。@而由间谍软件所产生的大批流量也可能消耗公司网络带宽，导致关键应用系统出现拥塞、延迟以及丢包的情况。@许多间谍软件写得很差，在进入企业网络后可能产生新的漏洞，或是造成工作站使用时出现性能问题，如屏幕冻结、不定期变慢与通用保护错误等等。由于间谍软件主要通过80端口进入计算机，也通过80端口向外发起连接，因此传统的防火墙无法有效抵御，必须通过应用层内容的识别进行采取相关措施。