破解VoIP安全难题的一体化手段 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/231/2021_2022__E7_A0_B4_E8_A7_A3VoIP_c101_231475.htm 基于互联网的VoIP给企业运营带来了效率的提升，但是其中也隐藏着安全风险。 VoIP在企业通信中的应用范围越来越广，已经深入到了企业的各个管理流程，除了费用的节省之外，整合式的通讯能力直接提升了企业运营效率。企业在部署VoIP系统时，除了对服务质量等问题的关注外，对安全问题最为重视。VoIP所面临的一系列安全隐患，实际上是互联网络上存在的若干安全问题的延续。只有很好地解决了网络的安全问题，同时配合VoIP产品本身的一些安全认证机制，基于VoIP的应用才能够在企业中持久稳定地发挥作用，并成为解决企业话音通信需求的有效方法。 预先防范更重要 预先防范是解决网络安全问题的最好办法，这也适用于VoIP。虽然这是一个老生常谈的话题，但是很多企业却没有在部署VoIP系统时给予安全问题足够的重视，尤其是亚太地区更为明显。有市场研究机构调查表明，目前亚太地区的服务供应商在VoIP安全性方面的支出远远落后于美国和欧洲，并且这一差距未来还将会进一步加大，预计2008年亚太区在该方面的支出约为1.7亿美元，而亚太以外其他地区的总支出将超过3.7亿美元。这充分说明了当前亚太区在VoIP安全意识方面的欠缺。 上海贝尔阿尔卡特业务通信公司高级经理顾均卓认为：“ 为了保证企业VoIP的安全，用户在选择VoIP系统时，应该选用已经内置了安全保护的系统。 ”她进一步说明VoIP安全威胁主要来自于网络的病毒和黑客对数据网络的各种攻击以及网络的硬件设备自身出现的

问题。一般来说，面向语音通信服务器的网络攻击，主要通过远端维护的方式进入，从网络攻击的角度看，主要通过Teln et 方式接入。造成的危害有：影响话音质量、语音系统和应用的连接中断等，最严重时会出现因为数据网络的阻塞和中断，导致语音网络出现通信故障。 Juniper网络公司中国区系统工程师梁小东也认为企业在部署VoIP系统的时候，也应该设定相应的一体化安全防护手段。 企业VoIP实质上只是IP网络上的一种应用，和电子邮件、Web浏览等类似。 如今典型的企业IP电话系统其基本要素包括：呼叫控制服务器；VoIP客户机；VoIP网关。所以理论上说VoIP系统和其他网络数据应用一样容易遭到攻击。面临的一系列潜在威胁包括：拒绝服务攻击、病毒、蠕虫、特洛伊木马、数据包嗅探、垃圾邮件和网络钓鱼等。 就目前来看，业界很少有关于VoIP系统受到大规模攻击的报道，不过这并不代表着VoIP系统比其他网络应用更加安全。实际上，这种情况的发生很大程度上是和VoIP系统本身标准化程度不足，各个厂商之间设备互通性差联系在一起的。VoIP的非标准化虽然增加了企业的使用成本，但是却“ 意外 ”地加大了黑客入侵的难度。但是这并不意味着企业可以削减在VoIP安全上的投资，这是因为随着VoIP使用范围的不断扩大，VoIP标准化也随之增强。 梁小东对《中国电子报》记者说：“ 已经出现了针对目前流行的VoIP通信协议SIP的攻击方式，可以让企业的VoIP通话中断。 ”用老办法解决新问题 VoIP面临的安全威胁类型和大多数互联网应用一样，所以从这个角度来说，人们可以把防护其他应用安全的措施转移到VoIP系统中来。比如在IP传输层使用防火墙，用 IP S / ID S 解决方案进行更深入的分析，使用应

用程序或者协议分析器等。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