网络安全技术的局限与未来发展趋势 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/223/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_223474.htm 中国的网络安全技术在近几年得到快速的发展，这一方面得益于从中央到地方政府的广泛重视，另一方面因为网络安全问题日益突出，网络安全企业不断跟进最新安全技术，不断推出满足用户需求、具有时代特色的安全产品，进一步促进了网络安全技术的发展。 从技术层面来看，目前网络安全产品在发展过程中面临的主要问题是：以往人们主要关心系统与网络基础层面的防护问题，而现在人们更加关注应用层面的安全防护问题，安全防护已经从底层或简单数据层面上升到了应用层面，这种应用防护问题已经深入到业务行为的相关性和信息内容的语义范畴，越来越多的安全技术已经与应用相结合。 一、现阶段网络安全技术的局限性 谈及网络安全技术，就必须提到网络安全技术的三大主流防火墙技术、入侵检测技术以及防病毒技术。 任何一个用户，在刚刚开始面对安全问题的时候，考虑的往往就是这“ 老三样 ”。可以说，这三种网络安全技术为整个网络安全建设起到了功不可没的作用，但是传统的安全“ 老三样 ”或者说是以其为主的安全产品正面临着许多新的问题。 首先，从用户角度来看，虽然系统中安装了防火墙，但是仍避免不了蠕虫泛滥、垃圾邮件、病毒传播以及拒绝服务的侵扰。 其次，未经大规模部署的入侵检测单个产品在提前预警方面存在着先天的不足，且在精确定位和全局管理方面还有很大的空间。 再次，虽然很多用户在单机、终端上都安装了防病毒产品，但是内网的安全并不仅仅是防病

毒的问题，还包括安全策略的执行、外来非法侵入、补丁管理以及合规管理等方面。所以说，虽然“老三样”已经立下了赫赫战功，且仍然发挥着重要作用，但是用户已渐渐感觉到其不足之处。其次，从网络安全的整体技术框架来看，网络安全技术同样面临着很大的问题，“老三样”基本上还是针对数据、单个系统、软硬件以及程序本身安全的保障。应用层面的安全，需要将侧重点集中在信息语义范畴的“内容”和网络虚拟世界的“行为”上。二、技术发展趋势分析1.防火墙技术发展趋势 在混合攻击肆虐的时代，单一功能的防火墙远不能满足业务的需要，而具备多种安全功能，基于应用协议层防御、低误报率检测、高可靠高性能平台和统一组件化管理的技术，优势将得到越来越多的体现，UTM（UnifiedThreatManagement，统一威胁管理）技术应运而生。[1] [2] [3] 下一页 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