

从网关到终端 跨界组合成为安全新命题计算机等级考试 PDF
转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/580/2021_2022__E4_BB_8E_E7_BD_91_E5_85_B3_E5_c98_580456.htm 安全的新形势：终端成为新的边界 传统的网络安全模型中，将网络划分为内网，外网，DMZ等多个安全域，通过在网络边界部署防火墙，来隔离内外网。防火墙的作用类似一道城堡，通过执行访问控制策略，将外部威胁隔离在城堡之外，保护内部网络的安全。随着信息网络技术的发展，网络安全的势态发现了变化。一个明显的特征是：终端成为新的网络边界。首先，随着网络接入技术的发展，终端接入网络的方式已经不再局限于局域网接口，包括双网卡、Modem拨号、WiFi、CDMA/GPRS上网卡、红外、蓝牙……这些接口已经成为企业内部网络的另一道边界。不能管理内部PC通过这些接口上网，就类似在防火墙的城堡下，存在很多没有安全警卫的后门、小道，内部网络的安全性无法保障。其次，传统的企业网络中，终端具有固定的办公位置，内部网络相对是静态的。然而随着移动终端的普及（便携机销售超过台式机），产生了移动办公方式，内部网络上接入的终端变得动态化。一方面，员工的终端可能在多个位置动态接入内部网络；另一方面，各种非公终端也可能接入内网（包括员工个人PC，以及合作伙伴，客户的PC）。随着用户PC的不断接入，内部网络的边界在不断扩充。内部网络的动态化，需要我们从另外一个视角来看边界安全问题。在内网边界动态变化的过程中，我们必须在新加入的PC这一新的边界上，进行必要的安全检察，配置必要的安全防护，才能满足网络安全的需要。再次，USB等存

储设备的大量使用，使得内部主机直接暴露在通过U盘等移动媒介传播的恶意软件面前；同时，内部的关键信息资产，也面临通过移动媒介泄露的威胁。网关设备对此无能为力。终端成为内部网络的另一道边界，网络安全必须同时管理网关终端双重边界，是安全产品必须面对的问题。

安全的新挑战：黑客攻击技术的集成化 随着信息安全的概念逐渐普及，大部分企业都部署了防火墙和防病毒软件。对安全威胁进行了有针对性的防御。与此同时，黑客的攻击手段也在和安全产品的“控制与反控制”斗争中不断发展。举例来说：针对企业防火墙的部署，黑客工具被设计为反弹连接方式，绕开防火墙的安全策略，黑客在内部网络的PC上植入木马后，反弹木马从内部主机上主动发起连接，网关防火墙对这类攻击难以识别。针对终端防病毒软件的部署，黑客工具加强了与防病毒软件对终端系统控制权的争夺，木马病毒被设计成首先上来终结防病毒软件进程。黑客把这些技术结合在一起，形成集成化的新一代攻击工具。单一的安全产品，在抵御这些集成化的攻击工具时，都存在一些脆弱点。针对这种安全威胁，客观上需要多种安全产品相互协同与配合，构筑成系统的防御体系，从而更好地满足企业的安全需求。

安全的新思维：网关终端跨界组合 面对安全的新形势和新挑战，将网关安全产品和终端安全产品组合在一起，形成更加有效的纵深防御体系，这种安全的新思维逐渐成为趋势。通过组合，可以统一管理网络边界，同时在网关和终端同时进行安全控制，对整个网络边界执行统一的访问控制策略、统一配置、统一监控，确保网络安全无盲点，将企业IT管理的范围从网络边界的网关设备推进到终端PC，保证整体的网络安全性，

保证业务的可用性和连续性。在此基础上，形成针对新安全威胁的纵深防御体系，面对集成化的黑客攻击方式，网关与终端互相保护，协同配合，纵深防御，更有效地抵御新的安全威胁。当然，网关安全产品和终端安全产品属于不同的技术领域，两者之间跨界组合的实现，对安全厂商提出了更高的要求。当前实现跨界组合面临的主要挑战有：第一，对产品系列的综合要求。安全市场本身比较细分，大部分安全厂商，都有其比较强的技术领域，也有比较弱的领域，尤其是在网关安全和终端安全这两个领域，技术差异性比较大。客户的安全需求无界，但安全产品的界却是真实存在的。第二，产品协同实现的复杂性。传统的单点安全产品，在数据层面基本不需要与其他设备进行交换。而跨界组合则需要不同的安全产品之间相互保护，协同工作，这种协同要求遵守相同的通信协议。跨界组合对于习惯于单点安全设备开发模式的传统安全厂商，提出了更高的要求。第三，客户对“易用性”的要求。安全产品对用户而言比较专业，简单易用本来就是一项关键要求。而跨界组合的复杂程度超过单一安全产品，客户对“易用性”的要求更加强烈。“部署简单，配置简单，管理简单”是跨界组合必须满足的需求。近年来，国外的信息安全领导企业纷纷开始探索通过产品组合的方式来满足客户的安全需求。例如，Cisco的NAC（Network Access Control）架构在网络设备和端点安全代理之间，通过端点健康检查、准入控制，协同控制安全威胁；Juniper遵从TNC（Trusted Network Connect）标准，将网关和端点安全组合，形成起UAC（统一访问控制）产品。但是，纵观国内安全厂商，在网关和终端安全两个领域都有成熟技术和产品的并不

多，能实现二者协同和易用性的就更寥寥无几。目前只有启明星辰等少数厂家具备跨界产品组合的能力。从网关到终端，跨界组合已经成为信息安全的新命题和新趋势。国内安全厂商能否抓住这一机遇甚至改变与国外厂商的竞争格局，让我们拭目以待。2009年上半年全国计算机等级考试参考答案请进入计算机考试论坛 2009年全国计算机等级考试报名信息汇总 2009年NCRE考试有新变化 2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 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