网络安全隔离与信息交换技术的发展新动向 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/142/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_142703.htm 随着电子政务和各种社会化便民网络工程的建设完成，各政府部门和社会管理服务系统希望通过安全的信息系统建设，提高了办事效率，增加了办公的透明度，加强了监管力度。因此，各种网上便民应用要求相关部门的业务网与互联网实现信息交换，同时业务部门之间的网上办公系统要求相关业务网也要实现信息交换。在这些网络安全需求中，安全隔离与信息交换系统（以下简称“ 安全隔离网闸 ”）得到了广泛应用。 安全隔离网闸市场已经开始进入高速增长期。安全隔离网闸的高安全性已经逐渐地被政府网络管理者所认可，从安全隔离网闸现在在公安专网与其外联网络（如印章制作中心网络、旅店监管网络等），税务专网与互联网、工商专网与互联网等政府部门网络中的广泛应用就可以得到印证，并且数十台以上的集中采购项目已经是经常可见的。除了政府应用外，军队、金融、电力等行业也认识到了安全隔离网闸的安全价值，在重要的网络隔离中采购安全隔离网闸来实现高安全的数据交换。 安全隔离网闸需求量的迅速增长是以产品成熟为前提的！国家相关部门对安全隔离网闸最基本的技术要求有两点：一点是硬件架构为“ 2＋1 ”结构，即由两个拥有独立操作系统的主机系统和一个专有的隔离交换模块组成；另一点是对流经的数据处理方式，对数据包全部在应用层进行重组、深度内容检测之后在网间进行信息“ 摆渡 ”。这两点技术要求已经在主流厂商的安全隔离网闸上得到了严格的执行。 但是，

各安全隔离网闸厂商研发的重点都只是集中在对“ 摆渡 ”数据的深度检测实现和提高处理性能上了，笔者在进行广泛地调研后认识到安全隔离网闸的技术发展忽视了其作为网关级安全设备应该进一步具有适应性、可管理性以及自身安全性。以下笔者将从客户应用需求的角度，展望安全隔离网闸下一步的几个最新发展动向。 多网接入安全隔离需求 现在，交警、电业局、自来水公司等单位在通过银行实现相关费用代收时一般要与多家银行进行网络连接。安全隔离网闸在这样的网络中部署时使客户出现了困扰，原因在于现有各厂商的安全隔离网闸部署时每个主机系统只能连接一个网络，那么在不能将各家银行网络连接到同一个交换设备上的安全要求下，一般的解决方式只能是有几家银行接入就部署几台安全隔离网闸。这样的解决方案很明显是过于浪费的！ 以交警网络与银行网络连接为例，我们仔细分析发现各银行网络相对于交警内网都是相同安全级别的网络。在各银行网络在实现无法互访和分别能与交警内网进行数据交换的前提下，是可以通过一台安全隔离网闸与交警内网相连接的。这就要求安全隔离网闸满足主机系统有多个网络连接接口，从而实现每一主机系统可以同时连接多个相同安全级别的网络，并且每个网络接口之间在系统内部固化实现无法互访。也就要求安全隔离网闸成为多网接入安全隔离平台（如图一所示）。 图一 多网接入安全隔离互联模型 集中管理需求 防火墙从最初作为独立的安全设备部署在网络中，到现在可以通过集中管理控制平台来实现对多台防火墙的统一协同安全防护和设备状态监控等管理。安全隔离网闸作为与防火墙相类似的网关级安全设备，其管理上也必然有相类似的管理技术发展脉络。

当前，市场上的安全隔离网闸还无法实现集中管理功能，但由于安全隔离网闸的规模性部署增多和对管理人员技能要求更高，所以用户对安全隔离网闸的集中管理功能的需求已经相当迫切。 集中式安全管理系统，要以统一的策略和集成的平台对受控网络进行安全配置和管理。集中管理员能通过集中管理中心可以对全局网络中的安全隔离网闸完成集中、统一的配置、管理和系统监视工作。 集中管理模式对于拥有多台安全隔离网闸的网络的安全管理尤为重要。它一方面提高了网络安全规则的一致性，增进网络的安全性，另一方面也为管理员提供了方便的配置和诊断工具，使管理员可以腾出更多精力的关注更高级的安全管理工作。 