腾飞中的杭州奔浪信息技术有限公司

□ 张 明

杭州奔浪信息技术有限公司成立于2007年，是一家专业从事计算机信息系统安全集成的科技型企业，拥有多项自主知识产权，公司注册资本1050万元。主要经营的范围为网络安全产品、网络流量分析系统。公司专门为政府、企业提供适合、优质、可靠的与网络相关各种类型的解决方案，包括计算机网络系统集成、信息系统安全设计和建设、信息安全服务、网络防护系统、安全防护系统的设计、施工、安装调试、培训、服务等。公司成立至今，为G20杭州峰会、雪亮工程、第十三届全国大学生运动会、杭州第十九届亚运会、第四届亚残运会等重大会事活动提供网络安全保障技术支持，为国家的网络安全建设做出积极贡献。

主要产品

1.数据安全隔离与信息交换系统。

主要部署在两个不同级别安全域之间，设备结构采用的是“2+1”硬件架构，中间的核心隔离部件是基于映射GAP技术的高速数据隔离交换部件，在应用层只对交换的纯数据进行解析，过滤和搬运，从而保证了内外网信息通信的安全，在物理上将攻击彻底阻挡在网络以外。

2.视频安全隔离与信息交换系统。

部署在两个不同级别安全域之间，设备采用“2+1”硬件架构，中间的核心隔离部件是基于映射GAP技术的高速数据隔离交换部件，产品对视频流进行单向传输处理，具备物理级视频单向传输通道，确保视频流通道安全，防止机密信息泄露。同时采用协议深度过滤技术和行为模式分析技术相结合，能够深入视频协议内部检查视频协议传输内容。具备深度视频协议分析能力，能够针对不同视频监控厂商的SIP/非SIP信令、控制信令的参数、信令内容、云台实时控制指令（云台转动、对焦等）、视频流编码格式和传输格式进行深度安全检测，实现信令、视频流传输安全。

3.数据单向安全导入系统。

部署于两个不同级别安全域\网络之间，设备结构采用的是“2+1”硬件架构，中间的核心隔离部件是采用无回馈光单向传输的高速数据隔离交换部件，在应用层只对交换的纯数据进行解析，过滤和搬运，从而保证了内外网信息通信的安全，在物理上将攻击彻底阻挡在网络以外。

4.集约化跨网跨域安全边界接入平台。

用于在两个不同级别安全域之间，为集约化平台型边界安全隔离与数据交换产品，既能满足新一代公安信息网跨网数据交换的需求，也能满足当前公安信息网跨网数据交换的需求，并可满足现有应用系统升级改造后平滑迁移的需求。

集约化跨网跨域安全边界接入平台由一系列产品组成：下一代防火墙、设备准入控制系统、数据交换系统、请求服务系统、安全交换系统、隔离设备、蜜罐系统、入侵检测系统、集控探针、网络监测系统、审计系统等。

5.安全隔离网闸（视频网闸）。

“2+1”安全体系架构，通过ASIC芯片技术设计的专用物理链路开关系统，实现用户关键网络及服务系统与外界的安全隔断，实现链路层与网络层的彻底断开。无协议的“GAP Reflective”技术，实现开放应用通讯协议的彻底剥离与重组，阻断来自网络层及服务器OS层的各类已知、未知攻击，弥补其它安全技术对网络未知攻击的防御盲区。广泛支持各类应用协议（HTTP、FTP、SMTP、DNS、SQL等），无需另外购买模块，包括支持视频会议、流媒体以及SSL等特殊应用代理以及用户定制协议，可灵活定制二次开发。提供数据库、文件访问应用，支持主流数据库同构、异构同步，支持多种文件同步应用，同步模式灵活定制。提供SAT安全映射服务，内置IDS，通过隔离系统的不可信端虚拟端口对外提供服务，访问者仅能访问虚拟端口而无法直接连接内部服务器，对外屏蔽内部网络和服务器系统，避免遭到攻击。支持负载均衡技术以及基于应用协议连接资源保护的QOS服务质量控制技术消除单点故障和网络实现对网络服务的高可靠性及可用性保证。

6.边界安全平台。

第二代防火墙；入侵防疫系统；安全隔离与信息单向导入系统；安全隔离与信息交换系统。

7.运维安全平台。

运维安全审计系统；数据库安全审计系统；日志审计分析系统；网络安全漏洞扫描系统。

8.终端安全平台。

网络接入控制系统。

9.视频安全平台。

视域边界安全平台；视域数据安全平台；视频安全接入控制系统；视频数据安全访问控制系统；视频水印网关系统；网络信息资产安全管理系统；视频监控安全检查平台；视频综合安全审计系统。

10.机房设备。

UPS不间断电源；精密空调。

部分解决方案

1.公安信息通信网边界接入方案。

包括数据链路接入方案：针对外部企事业单位/党政军链路安全接入到公安内网，采用数据链路边界接入平台方式接入，由数据交换系统前置、后置和安全隔离设备组成，提供落地数据库、文件的同步交换。数据交换系统与安全隔离设备采用可信私有通信协议、通信内容加密，保障数据交换的机密性和完整性。视频链路接入方案：针对平安城市的“天网工程”，公安建设视频专网，采用视频链路边界接入平台与公安内部网络接入。系统支持国标28181，实现非结构化的流媒体音视频等数据的实时、高速跨网数据交换，实现视频接入终端、接入链路、网络传输，以及接入用户的身份认证和访问控制。符合国家标准、地方标准及行业规范，适用视频会议、平安城市和智慧城市等高清视频应用环境。互联网信息采集接入方案：针对公安机关需要通过公共网络（公网）开展社会信息采集业务，目前通过公网接入的业务系统，如出入境、交通和户政、危爆物品管理系统、舆情系统、病毒库更新及操作系统补丁升级服务等。在互联网链路部署防火墙、IDS、探针、集控平台、可信边界安全网关、数据交换前后置机和单向光闸等设备，实现公网数据单向导入公安网；通过公网采集社会信息，以格式化数据文件的方式单向导入公安信息通信网，不允许公安信息通信网内数据向外传输至公网的情况；单向隔离光闸部署在安全隔离区，用于实现应用服务区和公安信息网的数据单向传输；数据交换系统实现对源端数据的采集和目标端数据的装载，并对数据进行深度的检测与过滤处理。

2.法院行业边界数据安全交换方案。

法院系统现有一套完整多级网络，在纵向分为最高人民法院、高级人民法院、中级人民法院和基层人民法院四级网络，在横向上分为法院业务专网、外部服务区网络、外部专网和互联网等网络区块。为实现法院业务信息互通系统建设目标，需要打破法院专网与外部专网系统之间的信息孤岛，需要在法院专网的数据共享区、外部专网的安全接入隔离区之间进行安全隔离和高度可控数据交换，建设成一个数据可信、链路可信、网络可信、应用可信、计算可信的具有良好扩展性的安全隔离数据交换平台。法院专网根据业务需求需要进行数据安全导入与导出，具体分为以下四类应用边界安全需求，每个边界针对不同的数据交换类型提供不同的边界安全接入链路方案。

3.检察院移动APP等业务接入方案。

依托电子政务网作为移动APP数据接入的中间网络做为跳板，实现APP数据从无线互联网到电子政务网，从电子政务网到检察院内网的跨网接入。将“检察院移动APP”的应用服务器部署在电子政务网中，使用电子政务网原有互联网出口线路实现手机终端“检察院移动APP”的业务访问。在电子政务网与检察院内网之间依照正反不同方向依次部署两套单向安全导入系统，以文件同步、数据库同步的方式实现部署于电子政务网的APP应用服务器与检察院内网的核心业务系统间的实时数据交换。其中，每一套单向安全导入系统都以纯单向无反馈的方式将数据信息由导入前置机定向传输至导入服务器，之后再由导入服务器同目的网络的业务系统服务器之间进行数据导入。每套单向安全导入系统都提供安全隔离下的纯单向数据通信。仅使用同步的方式实现数据的跨网传输。且在整个数据的交换过程中，数据的进入和导出过程彼此独立，互不影响。方案中所部署的单向安全导入系统还可与防火墙、入侵防御系统、防毒墙等传统网络安全设备相配合，从而实现移动终端APP接入时整条安全接入链路的网络访问控制、服务端口控制、入侵行为、病毒行为监测与防护等。

曾经服务单位

浙江省委办公厅信息中心、浙江省人民政府首脑机关信息中心、浙江省保密局、浙江省公安厅、浙江省公安厅机场分局、浙江省高等法院、浙江省检察院、浙江省安全厅、浙江省税务局、浙江省监狱管理局、浙江省国土资源厅、浙江省卫生厅、浙江省军分区、浙江省交通运输厅、浙江省公路局、浙江省道路运输管理局、浙江省交通科学研究院、浙江省特种设备检测院、中国电信浙江省分公司、中国移动浙江省分公司等。