无反馈单向光安全传输系统

技术白皮书

北京海淀区中关村南大街乙 56 号方圆大厦 9 层

电话：(010)58719666

传真：(010) 58719666-9588

服务电话：(010) 400-810-0868

目录

1. 产品研发背景

2.1 国内现状及需求

计算机网络的开放性产生了许多类似信息泄漏、网络攻击、网上犯罪等层出不穷的安全问题。采用以防火墙为核心的网络边界防御体系只能够满足信息化建设的一般性安全需求，难以解决涉密信息系统等重要网络的保护问题。对于涉密网络的保护，我国一直在采用物理断开的方法，国家保密局在《计算机信息系统国际联网保密管理规定 》中将涉密信息系统的安全防御要求定格为与任何非涉密信息系统必须物理断开。

目前，很多部委、国家机关及企事业单位的重要业务系统都处于涉密网络，而业务系统需要的基础数据却来自外部业务网络，甚至互联网络。物理断开造成了应用与数据的脱节，影响了政府的行政效率和全面信息化。如何实现涉密信息系统与非涉密网络之间的连接，成为我国信息化建设中一个亟需解决的问题。

我国信息安全产业界从 1999 年开始 GAP（网闸）技术的应用，以此希望实现涉密网络与非涉密网络的联网突破。这一思想也影响了信息安全界的厂商和部分主管部门，一时间专注 GAP 技术研究的厂商前赴后继。但在实际应用中，以 GAP 技术为核心的产品市场却始未得到全面推广与长足发展，因为在 GAP 技术产生之初，国家保密局明确指出：“GAP 技术不是物理隔离，不能用于涉密网络与非涉密网络之间的连接”。因此必然需要通过应用新技术方案来解决上述刚性需求，替代 GAP 技术，在涉密网络与非涉密网络之间建立连接。解决重要的业务系统的实际需求。

2.2 国外技术及产品

针对类似问题，国际上出现一种“数据二极管”（Data Diode）的纯单向技术。“数据二极管”技术以其纯单向性，能够保证数据信息从低密级网络向上流动，同时保证高密级信息不可能流到低密级网络中，从而在进行数据单向推移的过程中，完全防止了各种可能的泄密。但是其存在技术成本高，同时性能相对较低等不足。

3 产品介绍

根据目前相关技术的发展现状，以及现实存在的各类应用需求，如：不同密级网间信息交互应用、从互联网采集的基础数据输入绝密网应用等，锐安科技结合多年为涉密领域提供信息安全综合解决方案的行业经验，研发了单向光传输安全系统。

对各系列产品的综合应用，形成解决方案，该方案目前已广泛应用于国家反计算机入侵和防病毒研究中心、公安部信息安全产品检测中心、南昌市公安局等企事业单位及政府部门，单向光传输安全系统的应用，取代了人工手动迁移数据的传统模式，在提高业务信息及时高效传输的同时，也大大提高了安全性。因而得到公安、政府及使用企业等各方客户的好评。

在全面进行市场推广的同时，我们也注意收集除公安等政府部门以外的用户需求。并结合了各行业间不同应用需求，逐步推出除通用基础型系统之外的，其他根据行业应用需求定制的新版系统，将涵盖到大型企业集团及金融、电力等资源系统部门。

3.1 系统应用功能

功能类	功能项	功能说明
单向传输通道	文件单向传输	提供文件的单向传输功能（400 兆/秒）
	多目录文件集传输	提供对多目录文件集的快速单向传输（400 兆/秒）
	高性能数据流单向线速传输	主要用于对性能要求高的项目应用中（千兆线速）
	视频流数据实时传递	能够在高密网络采集互联网或低密级网络视频数据（千兆线速）
安全控制	身份认证	提供系统管理的安全身份鉴别功能，身份鉴别基于用户名/口令、加密狗认证等实现；提供数据发送方和数据接受方身份认证功能（需定制）
	病毒防护	提供内置的病毒防护功能，支持自动和手动的病毒库升级（需要购买杀毒软件授权）
	流量统计	提供关键应用及网络接口的流量统计功能
系统审计	系统监控	提供对系统运行状态的实时监控功能
	日志审计	提供对用户访问行为、安全事件信息、系统日志信息的记录及审计功能

3.2 产品特点

安全！高效！易用！这三点可以说是所有安全产品追求的目标。而无反馈单向光安全传输系统产品通过单向光传输技术真正的做到**高效线速的物理层单向传输**，通过真正的“物理隔离”保证其安全性，同时通过全界面的配置真正的做

到“**轻松应用**”。

3.3 产品特点原理论证

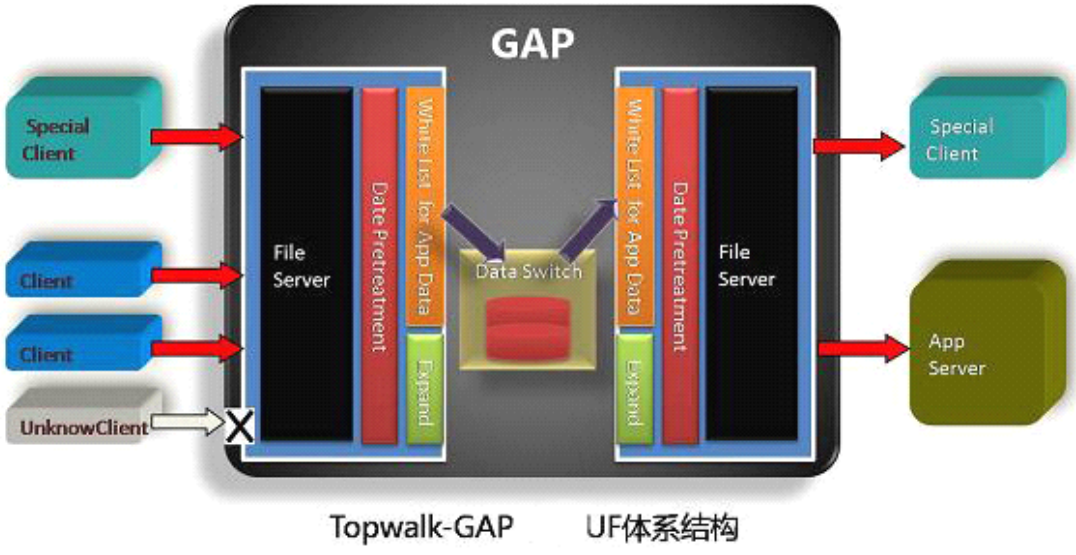
为什么说，无反馈单向光安全传输系统更安全更，更高效，而且易用呢？在这里会通过分析无反馈单向光安全传输系统与传统 GAP（网闸）的应用原理，以及界面展示等让用户真正体会到无反馈单向光安全传输系统的特性。

3.3.1 安全性

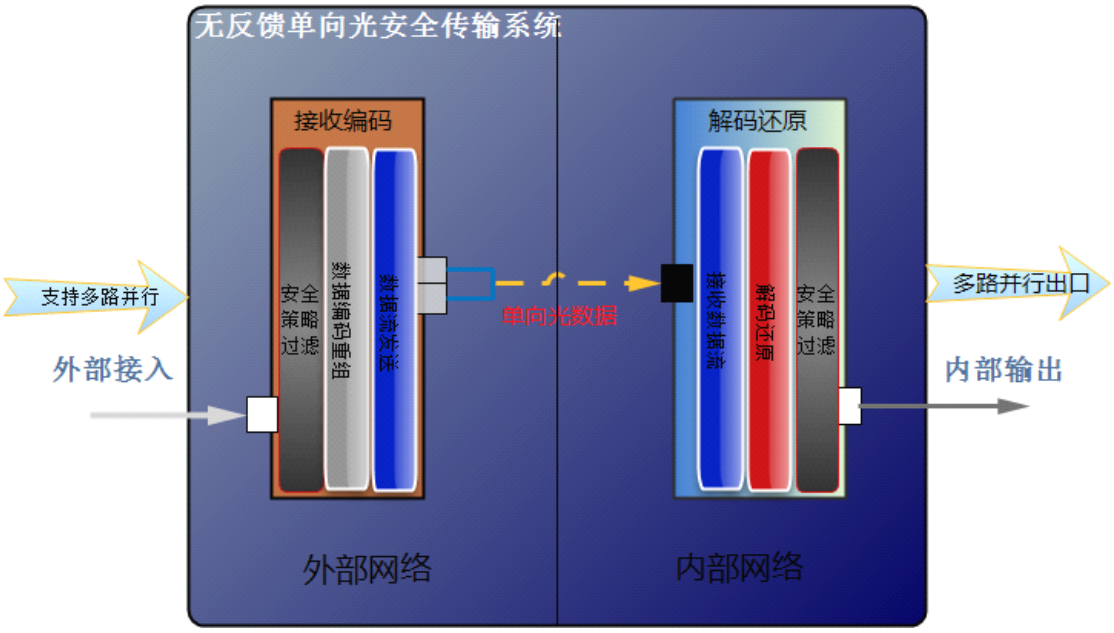
无反馈单向光安全传输系统采用物理层的单向分光传输技术，从最底层切断通信“握手”。形成无反馈的单向传输。单向分光应用早在几年前公安特殊警种已经应用到绝密项目中，安全性得到认证，并一直沿用至今。

3.3.2 高效性

与传统网闸产品相比，无反馈单向光安全传输系统采用的单向光传输技术能够达到千兆 0 延迟线速传输。



（上图 1 传统单向网闸）



（图 2 无反馈单向光安全传输系统传输原理）

区别请注意图 1 与图 2 两图的中线区域。传统网闸的数据需要先从外部处理模块传送到数据交换模块（Data Switch），再到内部数据处理模块。而无反馈单向光安全传输系统直接是以单向光数据的形势从外部模块传输到内部处理模块。这保证了无反馈单向光安全传输系统更能即时高效的传输。

3.3.3 易用性

无反馈单向光安全传输系统的应用配置全部采用 web 图形界面管理。在集成方案应用中无反馈单向光安全传输系统提供可二次开发的接口从而真正做到简单易用。应用管理界面截图如下：

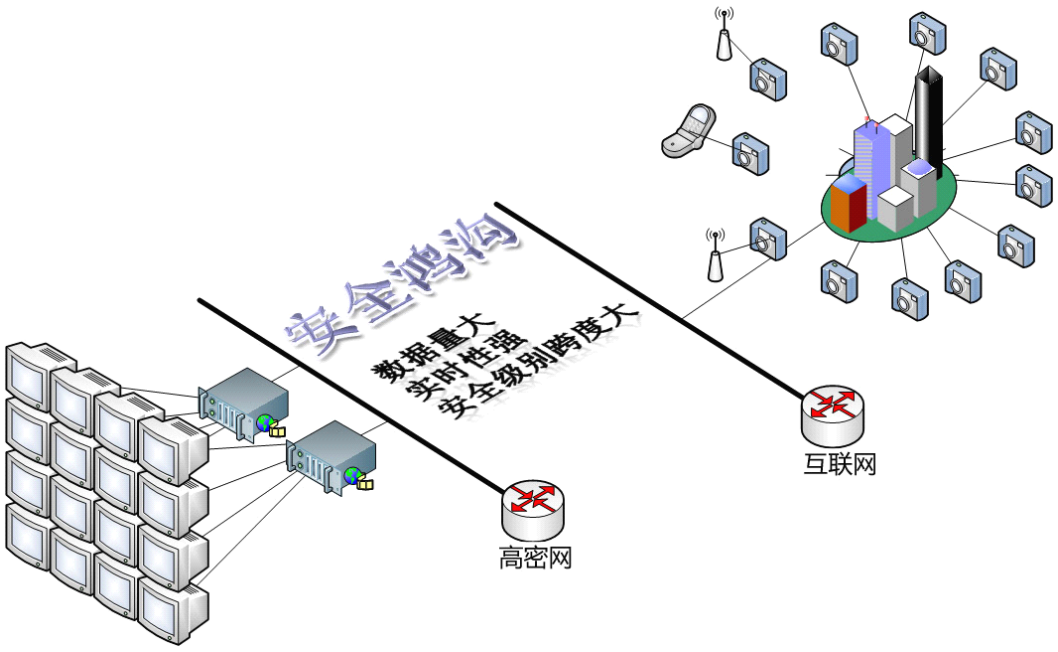

光闸管理登录系统
Shutter Management Login System
用户名：
密　码：
确 定
北京锐安科技有限公司


光闸内网系统
系统监控
安全管理
系统管理
高级功能
审 计
日 志
用户：ADMIN 2010-05-08 [退出]
端口状态
系统状态
系统资源状态 更新时间：2010-05-08
4,000
3,200
2,400
1,600
800
0
8/6/2006
8/8/2006
8/10/2006
8/12/2006
Offline Marketing
Search
Paid Search
From Mail
存储状态 更新时间：2010-05-08

4 无反馈单向光安全传输系统典型应用方案

4.1 视频流传输应用

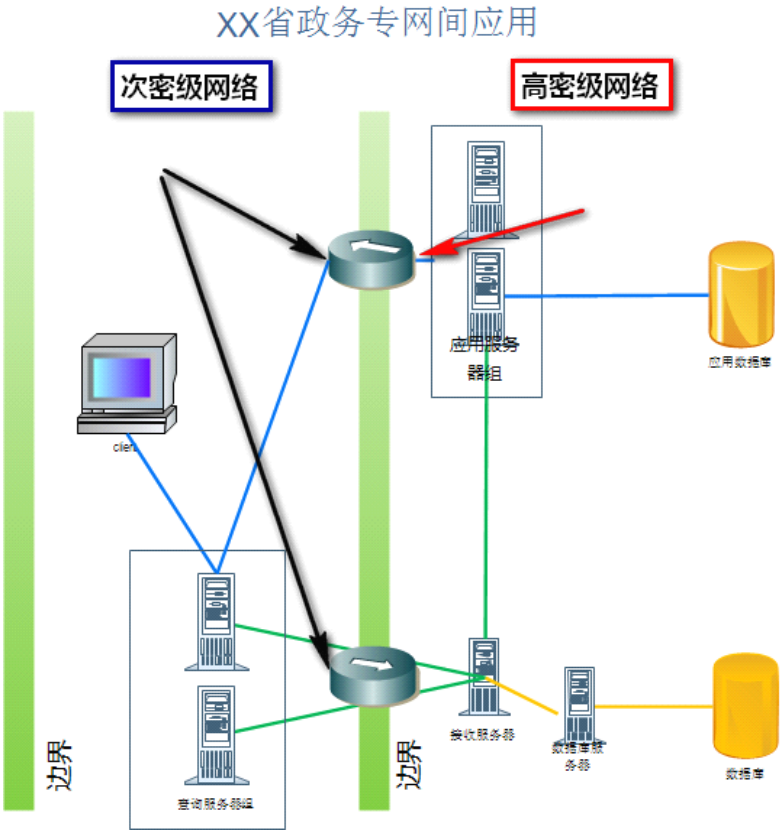
在 3111 工程中通过使用无反馈单向光安全传输系统的高性能线速传输与物理隔离的安全特性，完成将低密级网络数据实时的导入到高密级网络。实现图如下：



在这个应用中，我们充分发挥了无反馈单向光安全传输系统的安全性的同时，还将无反馈单向光安全传输系统的高线速通道利用的淋漓尽致。千兆线速它

解决了传统网闸产品最高达到百兆级别的尴尬问题。

4.2 典型高性能数据交换方案



图中左边网络密级较低，右边为高密级网络。在两个网络之间的边界处，我们使用了一路单向进入的无反馈单向光安全传输系统和一路单向接出的无反馈单向光安全传输系统。整个的数据流向是从次密网络提出申请后查询服务器会通过单向无反馈单向光安全传输系统将数据传递到高密网络，高密网络中的数据库服务器会产生数据并给另外一组服务器进行分析得出结果后在通过单向无反馈单向光安全传输系统返回到外部查询服务器。在这个方案中无反馈单向光安全传输系统保证高性能传输通道的同时，同样起到了高安全性的网络隔离。

安全性保证问题，您可以看图中的两个黑色箭头它代表了外部黑客的企图侵入点。而无反馈单向光安全传输系统的物理单向性保证了在边界的两个企图侵入点根本无法主动去取得内部数据。方案能够向外部主动传送数据的地方只有图中

红箭头指向的位置。也就是说只有“内鬼”才可能像外部传数据。通过无反馈单向光安全传输系统自身的高级安全策略对通信协议进行加密与认证这样整个方案可以保证，即时有“内鬼”他同样很难向外传递数据。

5 产品形态

Run-OneWay-100（1U 设备图示）

Run-OneWay-1000（2U 设备图示）

6 产品技术参数及性能指标

无反馈单向光安全传输系统系统性能指标：

指标类型	指标项	指标值	
		Run-OneWay-100	Run-OneWay-1000
性能指标	网络带宽	400Mbps	1000Mbps
	并发连接数	1000	5000
	丢包率	<=10^{-3}	<=10^{-6}
规格参数	平均无故障运行时间	50000 小时	50000 小时
	工作电压	220 ±5V	
	功率	250W	350W

无反馈单向光安全传输系统设备参数：

操作系统	Linux 专用安全操作系统
硬件配置	机架型改进机箱，高强度钢壳结构
	规格：530（长）×430（宽）×89（高）(mm)
	主板：专用主板
产品接口	Run-OneWay-100（1U）设备： 4 个标准 10/100/1000Base-T(RJ45) 自适应以太网接口 - 输入网络口：用于连接外部网络 1 个 - 管理口：用于管理配置 2 个（分别为输入与输出控制口） - 输出网络口：用于连接内部网络接口 1 个 Run-OneWay-1000 设备（2U）: 在 1000 设备基础上分别增加 1000 兆光口 2 个（分别用于千兆光数据接入与输出）
产品接口	前端发送接入部分： 2 个标准 10/-/-0Base-T(RJ45) 自适应以太网接口 2 块标准千兆光网卡 - 网络口：用于连接外部网络 - 管理口：用于管理配置 - 数据口：单向传输通道 1 个 RS-232 串口

	后端解码导出部分： 2 个标准 10/-/-0Base-T(RJ45) 自适应以太网接口 1 块标准千兆光网卡 - 网络口：用于连接内部网络 - 管理口：用于管理配置 - 数据口：单向传输通道
软件模块	数据发送模块、数据接收解析模块
电气性能	电源类型：AC 220V/50Hz
	电源功率：350W
物理环境	温度（工作）：10℃至 35℃
	相对湿度（工作）：40 - 80%非冷凝