天行安全隔离网闸

技术白皮书

北京天行网安信息技术有限责任公司

二〇〇七年二月

目 录

一 公司简介

1.1 公司概况

北京天行网安信息技术有限责任公司，专业从事网络与信息安全研究开发、技术支持、产品销售和安全服务，是中关村科技园区认定的高新技术企业和北京市科委认定的软件企业。

公司核心产品“天行安全隔离网闸（Topwalk-GAP）”由天行网安公司与公安部信息通信局联合研制，属国内首创（最早于 2000 年 10 月推出国内第一款网关级隔离产品，2000 年 11 月获得公安部颁发的销售许可证），并达到国际先进水平。天行网安公司拥有这一产品的全部知识产权，并已获专利证书。天行安全隔离网闸（Topwalk-GAP）为电子政务等安全性要求较高的应用提供了全新的安全解决方案。目前天行安全隔离网闸（Topwalk-GAP）产品成熟稳定，在各个政府部门拥有广泛的客户基础和首屈一指的市场占有率。

“以我为主，积极防御”是公司信奉的技术理念。在这一技术理念指导下，天行安全隔离网闸（Topwalk-GAP）系列产品获得了符合需求、安全性高的赞誉；此外，天行网安的补丁管理产品（Topwalk-PMS）为用户提供了全网自动化的补丁更新和管理系统，在病毒蠕虫等安全风险来临之前就进行积极防御，避免了病毒出现了才去杀毒的“亡羊补牢”的做法，极大提高了用户网络主机系统的安全防御水平；IT 架构管理平台（Topwalk-IM）产品综合管理用户的网络、系统平台和业务系统，并提供了符合 ITIL 理念的流程管理和服务管理，为用户屏蔽技术细节、专心业务应用，极大提高用户的 IT 系统使用效率和业务处理能力。

广泛的信息资源、强大的技术力量，天行网安将为您提供品质卓越的安全产品和专业化的安全服务。

公司资质：

- 北京市新技术产业开发试验区　　新技术企业
- 北京市软件企业认证　　软件企业
- 国家级火炬计划项目　　承担单位
- 科技型中小企业技术创新项目　　承担单位
- 北京市高新技术成果转化项目　　承担单位

1.2 “以我为主、积极防御”的技术理念

作为专业的安全产品以及安全服务提供商，天行网安与用户一起，深入实际进行调查分析，总结了政府用户各个方面和层次的网络安全需求，并针对政府用户网络边界的信息交换这一突出问题提出了既能保证高安全强度，又能提供信息交换功能的安全隔离方案。与用户一起、基于用户具体网络安全需求基础上提供解决方案的思路即为“以我为主”的技术理念。“我”即天行网安所面对的用户和用户的网络安全需求。天行网安认为，必须从用户实际的、具体的网络安全需求出发，才能提出切实可行的解决方案。

“积极防御”是中央《关于加强信息安全保障工作的意见》提出的指导方针，也是天行

网安在产品研发、方案提供的工作中一贯遵循的技术理念。随着各种系统漏洞不断增多、各种蠕虫病毒不断泛滥，网络安全形势日益严峻。但电子政务的建设不能因此停滞和减缓，政务部门的网络也不能隔断信息交换途径成为孤岛。积极面对网络安全形势，基于具体应用实际中的安全需求，将防御措施“嵌入”到应用系统之中，有针对性的解决实际安全问题，是为“积极防御”。

“以我为主，积极防御”技术理念不仅代表了天行网安主打产品“天行安全隔离网闸（Topwalk-GAP）”的技术思路，还指导着天行网安继续研究新的安全防御技术、开发新的网络安全产品、提供各种安全技术和服务。在这一技术理念指导下，天行网安和用户一起，追求网络安全的新境界。

二 网络安全概述

开放系统的安全问题与系统本身相生相伴。随着系统的规模和复杂性的增大，系统运行中的安全问题随之增多增强。作为保障系统正常运行的必要措施，安全手段的应用不仅应该随着系统的规模的增大而增多，而且要随着复杂程度的增大而增强。当前，作为主流的安全防御手段，防火墙、防病毒和入侵检测这网络安全的“老三样”至今为止还是安全市场的主流。而日渐增多的“蠕虫病毒”的流行，对传统防御手段提出了挑战。

2.1 信息网络系统的发展

信息网络系统从规模和应用复杂性两个维度上都有迅速的发展和扩展，数字世界是有史以来最复杂的人工系统。

规模的扩展

根据中国互联网络信息中心（CNNIC）的统计，中国互联网用户从 1997 年 7 月的 62 万增加到了 2006 年 12 月的 1.37 亿，增长了 221 倍，在 2006 年的一年中就增加了 2600 万；占中国人口总数的 10.5%，而北京则超过 30%。另外，根据著名的 Netcraft 公司的统计，全球互联网上的 Web 站点从 2000 年 2 月的 1100 万增长到 2007 年 2 月的 1.08 亿，增长 9.9 倍。目前的上网计算机数年增长率稳定在 25%左右，上网用户数年增长率稳定在 20%以下。

复杂性增加

以因特网、内联网为代表的信息网络已经从以学术研究为目的的数字化网络，变成了包罗万象的现实社会的信息化、数字化缩影。网络应用从最初的浏览简单网页、使用搜索引擎和收发邮件，发展出了各种各样的应用：

- 公众：即时信息通讯、网络视频、论坛、博客/播客、搜索引擎
- 企业：网上银行、网上商店、网上拍卖、企业管理系统（ERP/协同办公等）
- 政府内部：内联网办公系统、与因特网相连接的数据采集、处理、查询系统；国家“金”字系列工程
- 电子政务：跨越不同的政府部门、面向公众的信息系统。

2.2 安全威胁

信息网络上的安全威胁随着网络和信息系统的产生而产生，也随着其发展而发展。从 DOS 时代的病毒，到现在的网络黑客攻击、能够自动复制蔓延和攻击的蠕虫病毒、到各种各样的“特洛伊木马”，以及各种内部人员的恶意泄密或破坏。信息网络安全所面临的问题种类越来越多，内容越来越复杂。以下是一些事件统计：

- 1996 年 4 月 因特网上平均每 20 秒发生一起入侵计算机的事件（英国金融时报）
- 1997 年 几乎所有世界排名前一千家的大公司都曾被黑客们成功地闯入，有 56%的公司被闯入过 30~40 次；美国国防部、空军、司法部、商务部、中央情报局都曾经被黑客入侵
- 2000 年 1 月 Yahoo 等网站遭受 DDOS 攻击，陷入瘫痪

- 2003 年 8 月 MS Blaster 蠕虫在仅数天之内就使国内 200 万台以上的计算机陷入瘫痪
- 2004 年 1 月 MyDoom 蠕虫，入侵和感染了数十万计算机；产生和发送了数以千万计的病毒邮件，在全球直接造成了 261 亿美元的损失，蠕虫发作时的攻击使得 SCO 网站被迫关闭
- 2006 年 8 月光大证券网站多款软件被捆绑木马，威胁用户工商银行网上银行的帐号密码安全
- 2006 年 12 月爆发的“熊猫烧香”病毒，导致至少上百万人受此病毒威胁

可以看出，目前，危害最广、破坏性最大的安全威胁当属“蠕虫病毒”。如上所列的 CodeRed、Nimda、SQL Slammer、MS Blaster、MyDoom、Sasser 都属此列。这一现象与用户所采用的安全防御技术有关：目前主流的防御技术不能有效防止“病毒蠕虫”。

2.3 传统防御技术及其缺点

随着用户对网络安全的重视，作为安全防御手段的各类网络安全产品得到了越来越广泛的使用。据 IDG 的统计，目前网络安全投资年增长率 34%。这个数字已经大大超过了信息网络系统规模的年增长率 20%。

2.3.1 传统防御技术

目前作为主流的网络安全防御技术主要有三类：防火墙、防病毒和入侵检测/防御系统(IDS/IPS)。

防火墙技术包括包过滤、状态检测、应用代理等技术。包过滤技术根据 IP 报文的包头信息（如源地址、目的地址、目的端口）等信息对所通过的 IP 包是否能够通过进行判定，属于网络层的安全防御手段。状态检测技术可以根据 IP 报文之间的关系区分出不同会话，可以基于会话进行访问控制，属于会话层的安全防御手段。应用代理为防火墙增加了认证机制，并可以对应用数据进行简单、静态的检查，识别有害数据，进行防御。

防病毒软件的基本技术是病毒特征码的检查。病毒特征代码需要进行及时更新，才可能检查出新出现的病毒。虽然有些防病毒技术可以针对行为特征进行检查，但是对未知病毒基本上是无能为力的。

IDS/IPS 通过抓取网络上数据报文，对其内容进行比对，如果符合称为 Signature 的特征库所描述的内容，就认为是攻击行为，进行报警和拦截。特征库可以通过网络进行更新和升级。IPS 采用串连的部署方式，对攻击行为的阻止和拦截更为主动有效，但发现攻击行为的机制与 IDS 基本相同。最新的 IDS/IPS 技术增加了异常流量分析、DoS/DDoS 攻击防范等技术，但是对于最新的、未知的攻击行为，IDS/IPS 也一样基本上无法防范。

综上所述的防火墙、防病毒、IDS/IPS 等技术手段不针对任何特定的网络、信息系统，比较通用，无论何种网络、信息系统，都可以采用这些技术，发现安全威胁然后进行阻止，保证网络、信息系统的正常运行。这些技术手段的共同特点是采用“黑名单”方式进行防御，即，定义某些数据特征，并将其列入访问控制列表，符合这一特征的数据的为禁止、否则允许。这样的访问控制列表成为可简称为“黑名单”。对这种防御手段最简单的描述是：“兵来将挡，水来土掩”，发现一种新的攻击行为或者新的病毒、蠕虫，就将其列入“黑名单”，进

行防范。

2.3.2 传统防御技术的缺点

亡羊补牢、事后防御，不能防患于未然

安全威胁是变化多端的动态、持续的过程。当一种最新的攻击技术出现时，这些技术手段都难以在第一时间进行防御，只能起到“亡羊补牢”的作用。从安全威胁的发展趋势上看，新的攻击手段和新病毒、蠕虫才是对网络和信息系统的最大威胁。新的恶意代码的形成和新型攻击行为的发生永远早于“黑名单”的形成。因此，传统防御手段无法有效防止针对未知漏洞的攻击和针对已知漏洞的新型攻击。

作为目前安全威胁的主流，80%以上的有效攻击是新型恶意代码和新型攻击行为导致。因此，传统防御手段不能抵挡 80%的攻击，其防御能力令人置疑。

需要实时监控和即时维护更新，管理代价巨大

防火墙需要及时查看日志；IDS/IPS 需要及时更新标记文件；查病毒软件需要及时更新病毒代码库。信息网络安全要以管理为核心。安全产品是作为安全管理的技术手段得以实施、为管理服务、减轻管理工作量的。由于管理上难以做到进行 7*24 的维护、监控和更新，所以，防火墙等传统防御手段的防御效果经常大打折扣。

2.4 传统防御技术问题的分析及安全隔离技术的提出

由于传统防御技术本身的实现机制，一种新型攻击的出现时间和这种防御技术具备防御能力的时间存在一个时间差。这个时间差我们暂时称为“攻击－防御”时间差。随着信息网络系统规模的增大，以及其上运行应用系统的复杂性的增大，未知安全隐患在加速积累，并越来越多、越来越快的暴露；同时，防火墙等传统防御手段越来越多地采用，需要的管理工作(维护、监控和更新)越来越多；另外，恶意代码的开发随着网络协作，开发周期越来越短。因此，“攻击－防御”时间差越来越大。

另外一方面，同样的时间差，其危害却越来越大。这主要是因为：一、越来越快速的网络系统和计算能力不断放大攻击行为；二、越来越多的重要应用开始运行，用户对网络和信息系统的依赖越来越大，导致同样的攻击造成危害和损失越来越大

由于这些原因，虽然网络安全的投入快速增长(34%，IDG 统计数据)，甚至超过了信息网络系统规模的增长速度(20%)，但网络安全威胁和事件发生频度没有得到有效抑制(50%-100%)。传统防御技术不能有效防范的“蠕虫病毒”如最新的 MyDoom/NetSky/网络钓鱼等，成为网络安全威胁的主流，正在不断造成巨大损失。

“以我为主，积极防御”

从积极防御的角度看，静态的、“兵来将挡，水来土掩”式的防御显然属于“被动防御”的范畴。另一方面，物理隔离作为一种安全管理和技术手段，能够比较有效的防范来自外界对网络和信息系统的安全威胁。但是物理隔离隔断了网络，禁止了数据交换，造成信息化工作无法开展，可以称之为“消极防御”的手段。

那么，从物理隔离提供的高安全性和用户数据交换的实际需求出发，并对安全需求和应用需求进行深入分析，以“积极防御”的方式，即保持物理隔离所提供的高安全性保证，又能够满足业务应用系统的数据交换需求。

三 安全隔离网闸设计理念和特点

3.1 业务需求和安全需求分析

从实际需求出发，分析所需要防御的网络和信息系统的安全需求，才能做到有的放矢，采取积极主动的手段进行防御。

对于电子政务的业务特点，沈昌祥院士曾指出：“在电子政务的内外网中，要处理的工作流程都是预先设计好的，操作使用的角色是确定的，应用范围和边界都是明确的。” 审计部门需要财政部门定期提供财政预算数据，税务部门需要定期向财政部门提交税收数据。电子政务涉及到的网络间和信息系统间的数据传输大都是固定模式、可以明确定义的：

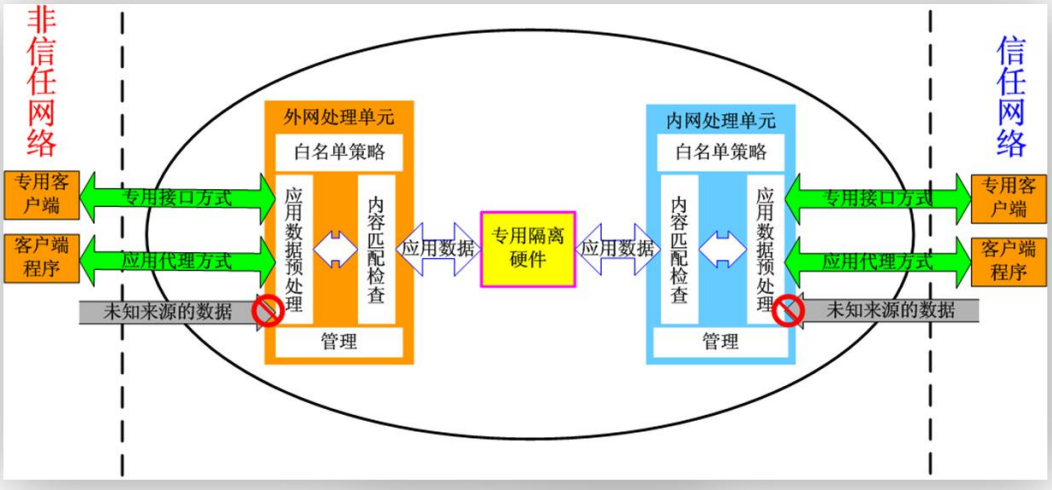
- 网络的边界明晰，隔离点可确定
- 网络间传输和交换的数据可定义
- 只传输明确定义的、需要传输的、确保安全的信息和数据，其它数据一概不传

根据以上需求特点，对需要传输的数据进行定义，称为“白名单”：符合定义的数据是允许的，其余的禁止。这一采用“白名单”的思路进行积极防御的技术即为安全隔离技术的核心理念。

安全隔离技术在物理隔离（Air Gap）的前提下，提供了安全适度的信息交换，因此又称为 GAP 技术。

3.2 安全隔离（GAP）技术要点和体系结构

“隔离->定义应用数据“白名单”策略->安全方式获取数据->数据内容检查->安全方式发送数据”，是 GAP 技术实现思路的核心。为体现这一技术思路，GAP 技术采用了独特的体系架构，如下图所示：



Topwalk-GAP 体系结构示意图

以上的 GAP 体系结构示意图体现了 GAP 技术的要点：面向应用数据，采用白名单策略，进行高度可控的数据交换。实现机制上，GAP 技术采用以下三点设计确保核心机制的实施。

一、采用多主机结构设计和专用硬件切断 TCP/IP 协议通讯，形成网络间的隔离

GAP 硬件采用多主机架构。GAP 设备需要对在网络间交换的数据进行预处理。预处理过程包括：将网络上传送的数据还原为应用层数据；对这些数据进行由用户所定义的检查；读取和发送这些应用数据。这些预处理操作在进行数据交换之前必须在独立的主机系统中进行，保证数据的隔离。另外，多台主机用专用硬件串联的架构形成纵深防御，即使外部主机被攻击，也可以保证内部主机的安全。

GAP 硬件架构中采用专用防篡改硬件隔断 TCP/IP 协议通信，保证数据传送和检查机制固化、防篡改，保证网络隔离的有效性。

二、不接受任何未知来源的主动请求；应用层数据的读取和发送通过专用 API 接口或者应用代理的方式进行

GAP 的“白名单”策略面向应用数据，并对未知来源的主动请求一律拒绝。因为用户对所传输的数据的定义只能是面向应用而不可能面向网络会话或者 IP 报文。读取和发送这些数据时，GAP 采用专用安全接口或专用客户端的方法。内部网络的服务端口暴露在各种各样的未知请求面前时，很难避免遭受堆栈溢出、绕过安全检查、拒绝服务等的攻击。GAP 通过专用安全接口或者应用代理进行数据读取和发送可以避免接收未知数据，同时对外部网络完全屏蔽内部网络信息。这样可以避免绝大多数隐患。

三、通过可进行扩展定义的内容检查机制为白名单策略提供进一步的保障机制

GAP 提供内容检查机制。内容检查机制首先采用病毒查杀引擎对已知病毒进行查杀。其次内容检查根据用户对数据的定义检查数据的格式和内容是否匹配。

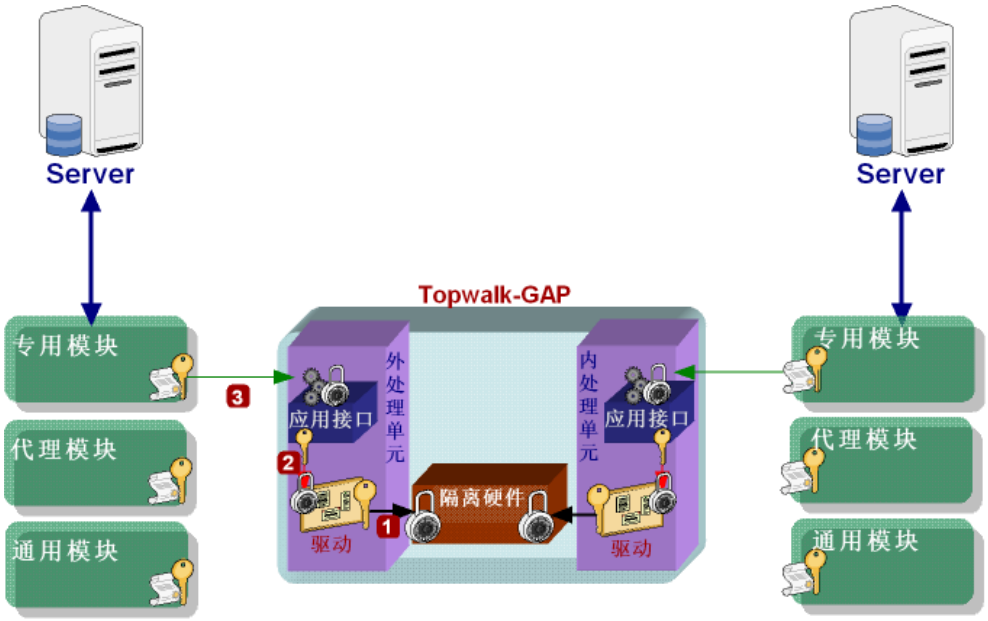
综上所述，GAP 技术隔断了从物理层到应用层所有网络层次的协议通信，因此，可以把 GAP 理解“the **G**ap of **A**ll **P**rotocol”的缩写。

作为全新的网络边界防御技术，GAP 技术与防火墙技术有明显的区别。以下是两种技术的对比：

项目	安全隔离(GAP)技术	防火墙(Firewall)技术
访问控制特点	基于物理隔离的应用数据白名单控制	基于连通网络的网络层或会话层黑名单控制
硬件特点	多主机形成纵深防御，保证隔离效果	单主机多宿主
	专用隔离硬件	无专用数据交换硬件
软件特点	不允许未知 TCP 会话	允许 TCP 会话
	不允许穿透 GAP 设备的直接访问	允许穿透防火墙的访问
安全性特点	可以最大程度防止未知攻击	不能防止未知攻击
性能与应用特点	确保安全性能所需的管理和维护工作量小	需要 7x24 监控，确保安全性能
	性能适中	高性能
	需要与应用系统结合，能够支持绝大部分参见应用	对应用完全透明

3.3 GAP 信任链

“硬件保障安全，软件提供功能”是 Topwalk-GAP 这一解决方案的核心思想。Topwalk-GAP 的核心是一个"专用隔离硬件"。专用隔离硬件首先保证隔离；其次，专用硬件实现可信的数据交换。硬件的特性在于不可篡改，这是软件无法替代的安全性保障。Topwalk-GAP 通过从专用硬件、专用安全协议和驱动接口、服务器端程序，直到客户端程序的信任链保障，实现硬件级别的数据 交换的安全保障，即：



如上图所示：

1. Topwalk-GAP 的专用隔离硬件通过共享密钥的方式，只信任和允许 Topwalk-GAP 内部的专用驱动通过专用安全协议提交的数据；
2. Topwalk-GAP 内部的专用驱动通过内核级安全控制的方式，只信任和允许 Topwalk-GAP 的服务器端程序调用其提供的硬件数据传输接口；
3. Topwalk-GAP 内部的服务器端程序通过认证和访问控制的方式，只信任和允许 Topwalk-GAP 的客户端、调用的 Topwalk-GAP 安全 API 的客户端和其它信任的客户端交换的数据。

网闸所信任的客户端由 Topwalk-GAP 所提供，包括：文件同步、数据库同步、消息传递、Web 代理、邮件代理、FTP 代理等；所有这些应用软件模块与网闸之间通过基于 PKI 证书的身份认证、用户名口令认证、IP/MAC 认证。

以数据库同步模块为例：

1. TopDB 数据库同步模块采用 JDBC 数据库驱动，连接需要同步的数据库，另外一端连接网闸设备。网闸两端的 TopDB 程序与网闸的连接采用基于证书认证的 SSL 加密连接，认证的证书为网闸生成和颁发，也可以根据需要重新生成；同时，TopDB 程序根据管理员的配置如需要同步的数据库、同步的表、字段、条件判断等主动获取数据。TopDB 获取到的数据以 SSL 加密以后以消息方式发送到网闸。此过程中通过两种手段保证安全：首先，需要传输的数据主动获取，避免被动接受未知数据；其次，数据在传输至网闸时有证书认证、SSL 加密保证数据的安全和完整性。

2. 数据在到达网闸以后，网闸根据内容检查策略判断是否符合内容检查策略，如果符合这进行交换，否则丢弃或按照管理员指定的方式处理。交换的过程由网闸上的应用接口调用网闸设备底层驱动程序，调用的过程依然通过严格的认证来保证合法性。网闸设备的底层驱动会驱动整个设备的安全核心：隔离硬件，以静态数据方式摆渡数据，数据摆安全摆渡。
3. 数据到达网闸另外一边的系统以后，按照同样的流程被处理，最终写入目的端的数据库。

整个过程中，所有的安全手段和措施的使用，信任关系被维持，数据传输的各个环节最大限度的保证不受到非授权的访问和攻击。

在上述安全策略由硬件全权控制的基础上，Topwalk-GAP 提供丰富的客户端软件、接口和代理服务，为各种应用系统提供了丰富的数据交换方式。包括：专用数据库同步客户端、专用文件同步客户端、专用 API 消息开发接口、HTTP/HTTPS 协议应用代理、POP3/SMTP 协议应用代理、FTP 应用代理、Socks/流媒体应用代理等，并在不断增加。

Topwalk-GAP 广泛的应用证明，这些软件提供的功能已经满足了大部分的网间数据交换需求。并且，Topwalk-GAP 解决方案中的软件还在不断的增加系列、增强功能，包括数据交换的审计、统计查询等，成为功能全面、使用方便的网间数据交换解决方案。

3.4 安全隔离技术的防御能力和特点

防御能力

- **多主机架构和专用硬件：**纵深防御架构和防篡改隔离硬件保证网络隔离，是实施应用数据白名单的基础。
- **对所交换的所有数据进行包括病毒查杀在内的内容检查：**确保所传输的应用数据符合 “白名单”的定义。
- **对 TCP 会话：**大多数的蠕虫通过在内外网之间建立 TCP 会话来进行攻击和数据窃取等非法行为；GAP 技术是在隔离基础上传输“白名单”所定义的应用数据。在网络间进行数据交换的过程中 GAP 内部不存在内外网之间的 TCP 会话。
- **其它未知的数据：**对于未知数据，“白名单”访问控制规则的缺省行为是禁止，而“黑名单”访问控制规则的缺省行为是允许。当未知数据是有害或恶意信息时，采用“白名单”方式的 GAP 技术可以有效防止。

特点

- **高安全性：**最大程度防止未知攻击。
- **低管理代价：**白名单一旦确定即可安全运行，无需针对新出现的安全威胁进行监控和更新；真正做到“Set and forget”和“Zero Administration”。
- **专用：**GAP 技术隔断了从物理层到应用层所有网络层次的协议通信，为每一个特定应用建立和维护一个专用数据交换机制。因此，GAP 也可理解为“the Gap of All Protocol”的缩写。

四 天行安全隔离网闸 V3.0

4.1 概述

早在 2000 年公司成立之初，天行网安公司就开始安全隔离与信息交换技术的研究，并与公安部信息通信局合作，进行了长时间的需求调研和分析，于 2000 年 10 月推出了当时名为“物理隔离系统”的第一款安全隔离与信息交换系统产品，并于 2000 年 11 月通过了公安部计算机信息系统安全产品质量监督检验中心的检测，取得了“计算机信息系统安全专用产品销售许可证”，是国内首家安全隔离基础上实现了安全适度信息交换的产品。

迄今为止“天行安全隔离网闸（Topwalk-GAP）”还先后通过了包括国家保密局、国家信息安全测评认证中心、解放军信息安全测评认证中心在内的所有权威测评和认证机构的检测、测评和认证，取得了相应证书。

在 2002 年 12 月举行的公安部科技成果鉴定会上，与会包括院士在内的多名专家一致认为，天行安全隔离网闸（Topwalk-GAP）“安全性高，功能齐全，技术上有创新，产品化程度高，运行稳定可靠”，“属国内首创，达到国际先进水平”，并建议尽快推广使用。

2000 年至今，天行安全隔离与信息交换系统分别在外经贸部（现商务部）许可证管理局、公安部、北京市包括公安局在内的多个委办局、成都、广州、深圳、成都、厦门、山东公安系统、河南公安系统等数百家政府单位成功应用，为全国各行业用户业务系统安全稳定运行提供了强有力的保障。

天行安全隔离网闸（Topwalk-GAP）经过持续开发、改进和多年来的应用实践，证明了产品成熟稳定、功能齐全，已经成为“安全隔离与信息交换”产品技术领域内的带头人、技术领先者和市场领先者。根据多年的市场和用户反馈，天行网安不断增加技术和研发投入，天行安全隔离网闸（Topwalk-GAP）推出了功能全面、界面友好、性能卓越、适应需求、简单易用的 3.0 版本。

按照不同的硬件划分，天行网安于 2007 年初推出了基于 Topwalk-GAP V3.0 平台的全新系列。包括：TG5000、TG6000/6500、TG7000、TG8000/8500 系列，功能丰富齐全，能够全面满足各个行业、各种应用的对网闸的需求。

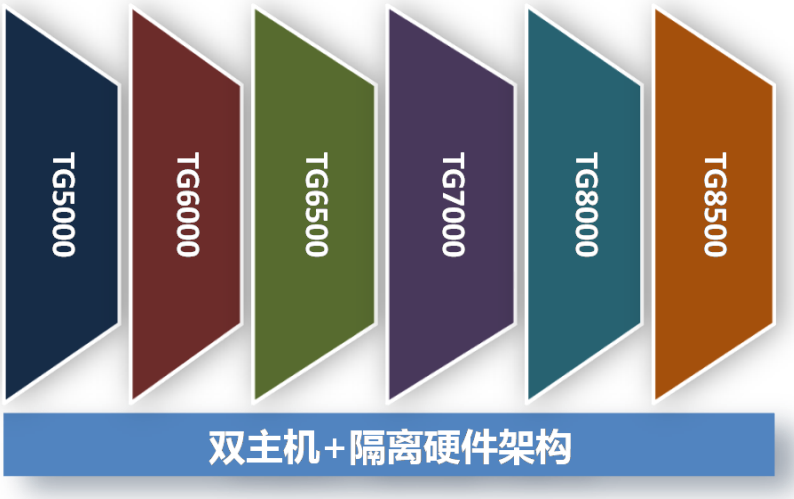
- 国内首创的基于 GAP 技术的安全隔离产品，达到国际领先水平
- 国内第一款拥有专利技术的安全隔离产品
- 国内第一款通过国家保密局和公安部等主管部门鉴定的安全隔离产品
- 国家科技部、国家火炬计划唯一支持的安全隔离产品
- 唯一获得公安部科技成果鉴定的安全隔离产品

4.2 产品介绍

由于职能和业务的不同，用户的应用系统及其数据交换方式也多种多样：各种审批系统、各种数据查询系统需要在网络间传输和交换指定数据库记录；各种汇总系统、各种数据采集系统需要在网络间传输和交换指定文件；各种复杂的应用系统需要传输和交换定制数据；内

外网之间的邮件互通和网页浏览需求要求网络之间能够进行邮件转发和网页转发。

针对以上典型需求，天行网安以安全隔离技术为基础，正式推出了 3.0 版本，有针对性的开发了 TG5000、TG6000/6500、TG7000、TG8000/8500 系列的安全隔离网闸产品，以满足不同业务系统的需求。



Topwalk-GAP 产品系列

天行安全隔离网闸（Topwalk-GAP）V3.0 全系列产品均采用双主机加专用隔离硬间（2+1）的底层基础硬件架构设计。Topwalk-GAP V3.0 版本的产品四个系列按不同的硬件性能进行划分，并针对不同的硬件平台进行软件系统优化，达到最优性能。

TG5000 采用 32 位嵌入式硬件平台，专门针对安全隔离网闸设计的硬件架构，提供低功耗、高稳定性、高可靠性、高集成度解决方案，是 Topwalk-GAP V3.0 系列的入门级产品。

TG6000/6500 采用基于 Intel X86 架构的 32 位 PIII/PM 硬件平台，经过天行网安超过三年数百家用户的使用考核，产品成熟度高、可靠性高，是 Topwalk-GAP V3.0 的中端产品，有最广泛的客户使用基础。

TG7000 采用基于 Intel X86 架构的 32 位 PIV 平台架构，是 Topwalk-GAP V3.0 系列第一款提供千兆以太网处理能力支持的产品，性能适中，能满足决大部分企业级应用数据处理需求。

TG8000/8500 采用基于 Intel X86 架构 64 位至强平台架构，分别采用 2CPU 或 4CPU，提供超强的真千兆处理性能，为 Topwalk-GAP V3.0 的高端产品，支持模块化扩展。专门针对高端用户需求对操作系统、系统指令、系统软件、应用软件进行了优化。

Topwalk-GAP V3.0 系统软件架构图如下：

如上图所示，系统底层软硬件是整个安全隔离网闸的核心部件，是其他软件、功能模块的支撑平台。Topwalk-GAP V3.0 所有的软件模块可以根据用户需求进行定制，提供极大的灵活性和功能扩展性支持。

这些软件模块包括：通用模块、专用模块、代理模块、扩展模块全文件模块、全模块。可以自由组合，能够支持文件同步、数据库同步、消息传输、FTP 文件传输、HTTP/HTTPS 协议传输、数据库访问、Socks 代理访问、邮件代理、双机热备、日志管理、简单网络管理协议、流媒体、视频（H.323）协议以及其他常见的应用协议。各个功能模块的访问控制方式各有不同，可以分别用户身份等属性进行访问控制。

每个软件模块根据硬件平台的不同进行了相应的优化设置，如提供更高内存的支持、更大并发数的支持、64 位操作系统的支持等，在每个硬件平台上实现软件功能的最优配置。

在安全隔离网闸内部不存在 TCP 会话，所谓协议数据均还原到应用层进行处理，，通过专用安全隔离硬件摆渡，对应用层数据处理方式和内容检查方式随产品、功能模块的不同而不同。

4.2.1 系统软硬件和专用隔离硬件

系统底层硬件包含的专用隔离硬件由天行网安公司自主设计，拥有自主知识产权。专用隔离硬件通过独立控制电路和读写保护电路保证信任网络和非信任网络之间链路层的断开，从而保证网络间的安全隔离。通过硬件实现安全隔离，彻底阻断 TCP/IP 协议以及其他网络协议，通过自定义的通讯机制进行数据的读写，实现可控的信息交换。

专用隔离硬件是独立与内外网处理单元（主机）的单板机。主要特点有三：

1. 独立工作的时钟。隔离硬件电路工作的时序有自己的时钟来控制，与内外网处理单元的时钟无关。内外网处理单元的时序不能影响隔离硬件电路自己的时钟，这在硬件设计上已经加以保证，防止了内外网处理单元通过控制隔离硬件电路的时钟，进而控制切换时间。
2. 电子开关。独立时钟控制下的读写保护电路中的电子开关采用固定电路来控制数据

线的通断。链路层的断开由开关切断数据信号，任何数字信号处理芯片可识别的低电平和高电平被开关处理之后，都变成不可识别信号或者缺省信号。这样保证内外网处理单元之间的数字链路层是断开的。

3. 独立处理器。硬件隔离电路的处理器独立于内外网处理单元工作。其切换工作，对数据的处理工作不受到内外网处理单元的影响，不可编程，也不接受内外网处理单元的任何命令。

同时，该电路的设计通过长时间的测试，保证其无故障工作时间在 5 万小时以上，其独特的设计保证即使系统硬件出现故障也不会导致安全问题产生，这其独特之处。

专用隔离硬件的切换速度小于 1 毫秒，每个切换周期最多可传输 4Mbit 的数据，因此，硬件数据传输速率大于 4GMbps。

专用隔离硬件与经过了安全定制的 Linux 操作系统结合，提供一个可信数据交换平台。在此平台基础上，各个软件功能模块可以公用日志和审计服务和管理服务。

日志处理系统可为各产品、功能模块提供统一的日志生成、存储、分类和备份功能。基于此日志和审计服务，各产品、功能模块实现了不同的报警机制。

基本模块提供基于 C/S 架构的管理界面，通过这一管理界面，用户可以对多台安全隔离网闸进行集中管理。管理客户端的连接方式为 SSL 方式，即对管理数据的传输进行了加密保护。通过加密连接的客户端管理界面可对不同的产品、功能模块进行灵活的配置管理。

底层软硬件系统还提供串口方式，用户可以通过串口方式对单台设备进行本地维护管理。

由于天行安全隔离网闸对数据的读取和发送方式采用专用接口以及应用代理两种方式，只接受明确允许的数据请求，对未知来源的数据报文一概丢弃，因此，一定程度上 DoS/DDoS 对安全隔离网闸是无效的。同时，天行安全隔离网闸不允许外部网络与内部网络的主机建立会话，因此，基于会话的 DoS/DDoS 攻击无法进入内部网络。

4.2.2 专用模块

天行安全隔离网闸专用模块是为了解决用户对系统安全性的最高要求而推出的产品系列，包括数据库交换、文件交换、消息交换功能子模块，可自由组合。在专用模块上，只有允许的、需要传递的数据才能进入网闸内部，同时在网闸内部通过一系列的安全访问控制手段对数据进行检查、交换，最终安全的将数据交换到目的端。

4.2.2.1 数据库交换模块

天行安全隔离网闸(Topwalk-GAP)V3.0 数据库交换模块以安全隔离硬件模块为基础，在保证信任网络业务系统安全运行的同时，提供与不信任网络进行同异构数据库之间安全数据交换的功能。

功能特点：

- 多种灵活机制的数据提取功能。可选远程提取或者本地专用数据库客户端方式；
- 可灵活配置数据配置提取方式、传输方向、读写预处理等多种策略；
- 支持双向、主从表、大字段数据、字段级条件传输，而无需修改数据库表结构，全面兼容各种应用系统；

- 良好的兼容性，支持所有主流关系型数据库，包括各种平台和版本的 Oracle、SQL Server、Sybase、DB2 数据库；
- 完备的日志查询系统。

4.2.2.2 文件交换模块

天行安全隔离网闸(Topwalk-GAP)V3.0 文件交换模块以安全隔离硬件模块为基础，在保证信任网络业务系统安全运行的同时，提供与不信任网络进行安全文件交换的功能。

功能特点：

- 基于用户权限的访问控制；
- 方向可控选择；支持多文件并发传输；
- 可灵活配置的读写规则，包括对所传输文件的文件名的配置；
- 实时及定时传输选项；
- 灵活的传输冲突选项；
- 完备的日志查询系统。

4.2.2.3 消息模块

消息模块以安全隔离硬件模块为基础，针对高级 GAP 用户需求定制的一套隔离数据传输解决方案。它在原有 Topwalk-GAP V3.0 的硬件架构上，设计了性能更优秀的传输机制，并为用户提供高强度安全可靠的客户端开发接口，使用户能够在享受 GAP 的强大安全性的同时,可以根据自己需要更加灵活的实现隔离网络间的数据交换。

功能特点：

- 基于数字证书技术的身份验证以及加密传输保证传输安全性；
- 基于用户的授权访问和灵活的权限管理；
- 集成安全性，灵活性，可靠性以及可管性于一体；
- 跨 Windows、Linux、Unix 平台环境支持，兼容性和适应性优异；
- 开发接口灵活（提供 C 与 Java 接口）。

4.2.3 通用模块

天行安全隔离网闸(Topwalk-GAP)V3.0 通用模块运行在安全隔离网闸软硬件基础上，具备 GAP 技术的多种安全特性，如多主机架构形成的纵深防御等。通用模块提供了内外网之间的互操作功能，注重通用性和高性能，可以更好的兼容应用系统和各种应用协议，使部署和使用更为方便。通用模块版本适用于网络边界的安全隔离与各种协议的数据交换。

通用模块采用了独特的内容检查和过滤技术。其检查方式和机制类似网络防御系统。不同的是，网络防御系统建立了一个黑名单特征库，当发现数据流中有符合特征的数据，就认为是非法数据，进行拦截和记录。而天行安全隔离网闸通用模块建立的是一个白名单特征库，只有符合特征库描述的数据才能通过，其它的一律禁止，这一点正是 GAP 技术所特有的高安全性特征。

4.2.4 代理模块

天行安全隔离网闸代理模块既保持了 GAP 产品的高安全性特点，又提供了对不同应用的良好适应性。代理模块在安全隔离的基础架构上，首先确保信任网络的高度安全，在此基础上通过对各种应用的代理机制实现对多种应用的支持，同时进行细粒度的访问控制。

功能特点：

- 支持 HTTP 应用代理，实现通过网闸安全浏览网页的功能。同时可对页面内容进行脚本、内容、URL、时间段、用户身份等控制；支持交互式动态页面访问；
- 支持数据库应用代理，包括 SQL Server、Oracle、Sybase、DB2 等数据库的数据应用代理功能，实现对数据库的安全访问，并彻底保障数据库本身的安全；
- 支持 FTP 文件传输应用代理，支持通过 FTP 进行文件安全传输；
- 支持邮件功能，实现通过网闸安全收发电子邮件的功能，可对邮件内容、附件类型进行检查，采用病毒查杀技术；
- 支持基于 Socks 的应用代理，满足多种基于 Socks 的应用需求，支持身份认证；
- 支持常见流媒体协议，包括 RTSP、MMS 协议等；
- 支持其它常见应用协议，包括常见的 TCP、UDP 等协议数据交换功能。

4.2.4 全文件模块

天行安全隔离网闸全文件模块是专门针对高可靠性文件传输、多种文件传输方式需求而开发的一个专用模块。广泛支持多种文件交换方式，包括：专用文件客户端方式、FTP 文件传输方式、SAMBA、NFS 文件交换。所有文件传输方式均提供高可靠性支持：文件完整性、正确性通过缓存校验机制、断点续传等功能加以保障。

全文件模块在文件传输的基础上实现对文件内容加密、内容检查过滤、文件类型检查、文件内容病毒过滤。

4.2.5 全模块

天行安全隔离网闸全模块包含多个模块的功能，是 Topwalk-GAP V3.0 产品中功能最为丰富系列之一，包含有绝大部分普通模块的软件功能。支持文件同步传输、数据库同步传输、消息定制开发接口、各种应用代理功能等，支持目前绝大多数应用数据同步摆渡传输。

4.2.6 扩展模块

天行安全隔离网闸扩展模块包括数个扩展增强功能子模块。

- V：视频模块，是天行网安公司专为支持视频会议功能而开发的一个嵌入式扩展功能模块。全面支持现有视频会议系统数据通信，包括 H.323 协议族、H.264 等。通过此模块的扩展，实现在安全隔离的前提下不同网络之间的视频会议通信。
- T：日志模块，此模块是在天行安全隔离网闸提供的高级日志审计扩展功能模块，包括日志的分级处理、审计、导入/导出、过滤等强化功能，并提供文件型日志数

据库记录系统日志。

- S：简单网管协议模块，通过加载此功能模块，天行安全隔离网闸能够全面支持现有的 SNMP 简单网管协议，实现通过网管平台进行统一管理部署，与网络设备管理全面整合。
- H：双机热备模块，实现两台天行安全隔离网闸之间的自动热备切换，提高网络关键部位可靠性，避免单点故障。在主设备失效时，通过双机热备模块自动切换到备用设备，保持业务系统持续运行，同时对故障进行报警、日志提示。

4.3 产品资质认证情况

- 公安部销售许可证书
- 国家保密局认证证书
- 国家测评认证中心认证证书
- 公安部科技成果鉴定证书
- 军队测评认证中心认证证书
- 安全隔离网闸专利证书
- 国家级火炬计划项目证书

4.4 应用情况

天行安全隔离网闸以其安全的体系架构和出色的表现，在政务行业和公安行业拥有大量的成功案例，得到了用户的广泛好评。见下表：

电子政务行业	公安行业
➢ 新华通讯社	➢ 公安部第 23 局
➢ 国家环保总局核安全中心	➢ 广东省公安厅
➢ 河北省政府	➢ 山东省公安厅
➢ 云南省政府	➢ 山西省公安厅
➢ 湖南省政府	➢ 福建省公安厅
➢ 北京市西城区政府	➢ 河南省公安厅
➢ 山东省国税局	➢ 湖南省公安厅
➢ 青海省国税局	➢ 辽宁省公安厅
➢ 湖南省地税局	➢ 吉林省公安厅
➢ 河南省国税局	➢ 江苏省公安厅
➢ 辽宁省地税局	➢ 北京市公安局
➢ 大连市国税局	➢ 上海市公安局
➢ 南京市国税局	➢ 浙江省公安厅
➢ 昆明市政府	➢ 重庆市公安局
➢ 中国人民解放军总装备部	➢ 天津市公安局
➢ 中国人民解放军总后勤部	➢ 青海省公安厅
➢ 中国人民解放军 XX 军区	➢ 云南省公安厅
➢ XX 市国家安全局	➢ 贵州省公安厅

➢ 北京市城市规划设计研究院 ➢ 唐山市国土资源局 ➢ ……	➢ 宁夏回族自治区公安厅 ➢ 内蒙古自治区公安厅 ➢ 拉萨市公安局 ➢ ……

五 天行安全隔离网闸 V3.0 系统参数

项目	描述	
产品名称	天行安全隔离网闸（Topwalk-GAP）V3.0	
产品（系统）形态	尺寸 2U~4U 重量 12~28 千克 标配颜色 银灰、黑色	
接口类型	TG5000	3 个 10/100BASE-TX 接口 2 个 COM 口
	TG6000/ TG6500	5 个 10/100BASE-TX 接口 2 个 COM 口
	TG7000	5 个 10/100/1000BASE-TX 接口 2 个 COM 口
	TG8000	4 个 10/100/1000M SFP 模块接口； 2 个 10/100/1000BASE-TX 接口 2 个 COM 口
	TG8500	8 个 10/100/1000M SFP 模块接口 2 个 10/100/1000BASE-TX 接口 2 个 COM 口
OS 类型、版本	TopOS 安全服务平台 3.2 版	
升级方式	内容检查可在线升级，免费；	
常规工作环境	输入电压和频率 220VAC/50HZ 消耗功率 300~460W 工作温度 0-60℃ 存储温度 -20-70℃ 工作湿度 10%-90% 存储湿度 5%-95%	
性能	吞吐量：75Mbps（TG5000） 90Mbps（TG6000） 92Mbps（TG6500） 350Mbps（TG7000） 600Mbps（TG8000） 650Mbps（TG8500） 延时： 1~5ms 平均最短无故障工作时间：50000 小时	

六 典型方案

6.1 电子政务应用案例

方案背景

政府信息化作为信息流的“中心节点”，已成为带动国家信息化建设的重要力量。电子政务为改善政府职能、提高公众服务，协调社会经济，进一步推动国家各行业建设有着重大意义。电子政务的安全关系国计民生、社会稳定等方面，重要性不言而喻。尤其对于核心政务平台所依赖的硬件、软件、网络系统等，都不同程度地存在着各种安全漏洞和隐患，来自数据泄秘、外部攻击破坏等威胁犹为严峻，基于 GAP 技术的安全隔离解决方案应运而生。

方案特点

1. 积极防御、综合防范

随着攻击方式的多元化、复杂化、融合化和隐蔽化趋势，电子政务面临的安全威胁来自多个层面。本方案以领先的 GAP 技术为基础，并集成了多种安全技术可以防范不同层面的安全威胁，为用户创建可靠稳定的内部网络环境。

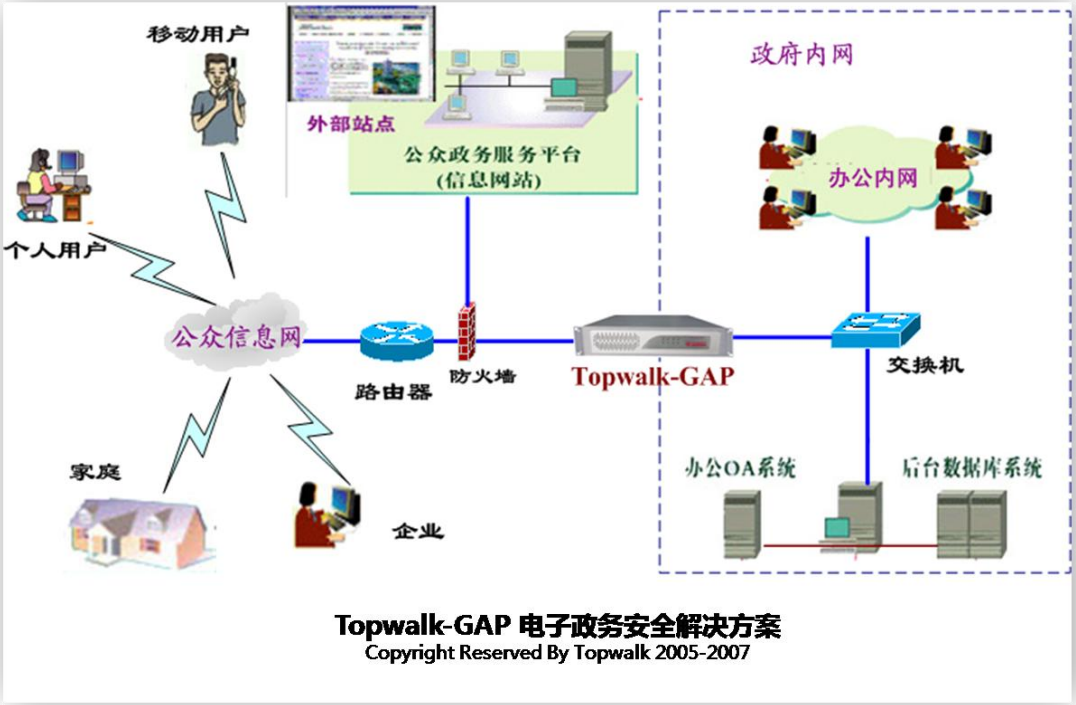
2. 内外隔离，适度交换

互联网“Code Red”“SQL Slammer”“冲击波”“MyDoom”等蠕虫的泛滥，表明漏洞攻击已成为主要威胁。方案首先确保政务内网与外部在链路层不存在通路，同时根据满足业务需要进行适度数据交换与共享，完美平衡了隔离与信息交换的矛盾。

3. 确保安全，应用为本

安全的目的是为了保障应用更健康和稳定，天行安全隔离网闸可以提供灵活多样的数据交换方式，如底层同异构数据库交换、标准公文交换、邮件交换、消息传输等，确保了与上层应用系统的融合。

电子政务安全隔离方案 （如图）



方案分析

该图表示了典型 G2C、G2B 模式的电子政务系统，政府外网包括公众信息服务平台及门户网站，内网主要满足内部办公等核心政务系统，实现内外网之间安全“信息摆渡”是跨越数字鸿沟、实现政务一体化应用平台的关键。在业务系统所需交换数据量较大时，可采用千兆网闸设备以提供高数据吞吐量。本方案通过将天行安全隔离网闸(Topwalk-GAP)设在内网与外网之间，在确保内外物理链路不存在通路的前提下，完成安全可控的数据交换，实现了“外网受理、内网办理、外网反馈”的政务统一应用，从而更有效发挥政府对公众的服务与沟通职能，推动电子政务取得实质性突破。

6.2 公安系统应用案例

方案背景

金盾工程建设对数据和网络平台的安全性要求非常敏感，同时业务系统对快速准确性和平稳性有很高要求。天行网安公司凭借对公安行业的丰富实施经验和深刻理解，紧密结合公安信息化现状、敏锐把握发展趋势，始终坚持贴近用户、注重个性化需求的原则，推出了具备安全稳定、灵活高效、易用可扩展等优势的公安系统安全隔离解决方案。

方案特点

1. 软硬一体化平台提供最高的安全性

公安业务系统最大的特点是复杂程度高，地域、信息点多且分散，安全威胁来自从物理

层到应用层多个方面。本方案集成了边界访问控制、GAP(安全隔离)、数字证书、安全审计管理、病毒及恶意代码过滤等多种技术，构建软硬一体化平台从容应对日趋复杂化、混合化、智能化的网络攻击。

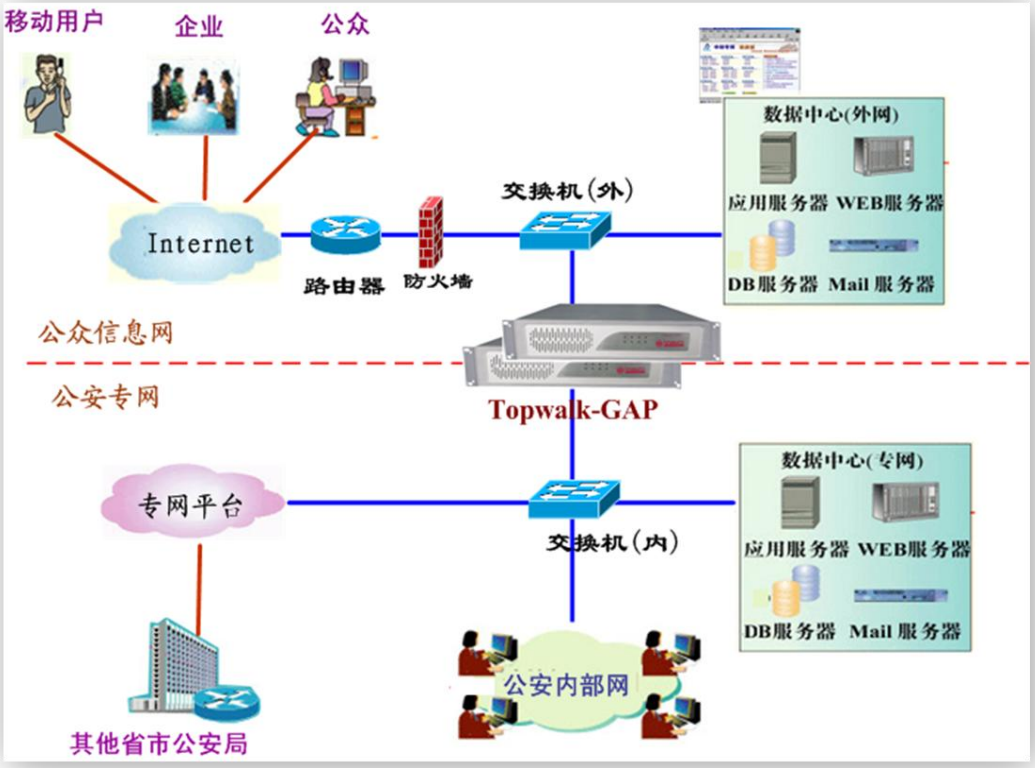
2. 可适应性、灵活性及可扩展性优异

本方案提供了多种数据交换方式以满足用户应用需求，如数据库交换可以满足内外网之间数据中心同异构数据库安全数据交换，消息模块提供了用户应用程序的 C、Java 等 API 开发接口，实现了与上层业务应用的无缝集成，具有很好的灵活性可扩展性。

3. 强大的数据交换性能，良好的平台兼容性

本方案所采用的天行安全隔离网闸在数据交换性能上具有传输速率高、延迟小等优势，符合公安业务系统“快速反应、协同作战”的要求，同时本产品的各个模块可以适应各类微软视窗、Unix、Linux 平台下的多种数据库、邮件等平台环境，具有良好的兼容性。

公安行业解决方案



Topwalk-GAP 公安系统安全解决方案

方案分析

该图表示了公安信息系统的典型布置，公安信息系统有信息点分散，业务复杂等特点，为发挥“统一指挥、快速行动”的目标，首先这些信息需要通过外部网络提交到公安外网的数据中心服务器，然后安全快速传输到公安专网数据中心进行比对确认等操作。为了保障系统的高可用性，通过 2 台网闸设备组成双机热备。本方案将天行安全隔离网闸设在专网与外部数据中心之间，在专网与外部链路层断开的前提下，实现了公网与专网之间数据交换的灵活高效，从而解决了物理隔离导致的“信息孤岛”问题。