网神
SECWORLD

可控安全
Controllable
Security

技术白皮书

网神 SecSIS 3600 光单向安全隔离数据自动导入交换系统

网神信息技术（北京）股份有限公司
http://www.legendsec.com

● 版权声明

● 文档信息

文档名称	网神 SecSIS 3600 光单向安全隔离数据自动导入系统技术白皮书		
扩散范围	销售/售前/客服/渠道商/用户	**文档版本号**	V8.9.1
作者	黄熙	**日期**	2014/09/09
初审人	王起立	**复审人**	

● 版本变更记录

时间	版本	说明	作者
14.09.09	V8.9.1	新增 V8.2.14.1 版本新功能	黄熙
2016/05/10	V9.2.15.2	型 号： L1500-E026P 、 L1500-E026M L5000-TG12P 、 L5000-TG12M 、 L9000-TV12P、L9000-TV12M	赵鹏

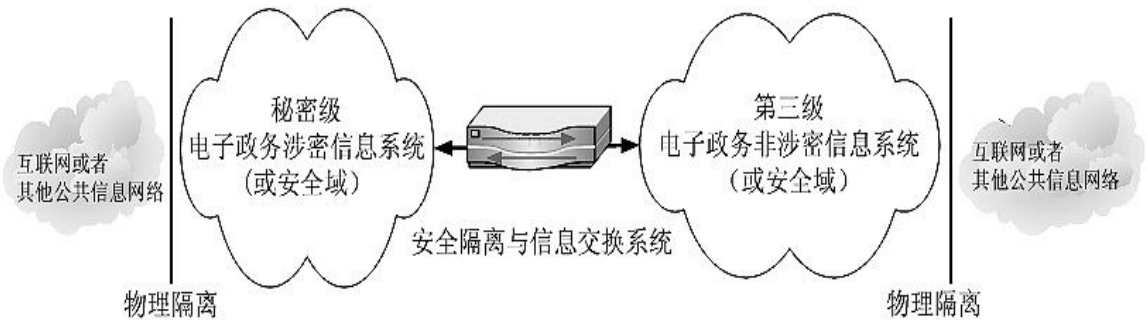
目 录

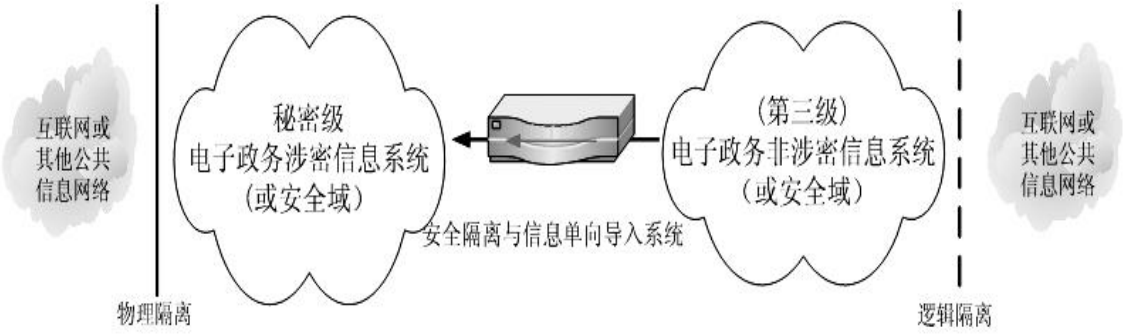
1 .产品概述

随着网络应用范围的不断扩大和网络应用技术的不断深入，网络用户也更加意识到网络安全的重要性，同时各个网络安全厂商也不断发布新的产品以适应用户日益增长的网络安全需求。但无论网络安全技术如何发展，网络及网络上的信息资源依然存在着相当的安全风险，网络攻击技术和网络安全技术正如中国古代矛与盾的比喻，攻防永无止境，发展永无止境。

防火墙、防病毒、漏洞扫描和系统风险评估、入侵检测等技术都可以在一定程度上提供安全防护，但这些安全手段还不足以保障用户网络系统、信息资源的安全。据美国《金融时报》报道，现在平均每 10 秒就发生一次入侵计算机网络的事件，超过 1/3 的互联网防火墙被攻破。目前政府机关内部网络可能所受到的攻击包括黑客入侵，内部信息泄漏，不良信息的进入内网等方式。因此，对于高速发展的电子政务系统来说，最迫切要解决的安全问题应该是政府内部机密信息的数据安全，如果使内外网物理上的通路断开，不失为一个最有效的解决办法。

2007 年 3 月份，国家保密局和国务院信息化工作办公室联合发布了《电子政务保密管理指南》。《指南》中规定：按照信息保密的技术要求，涉密网络不能与互联网直接连通；涉密网络与非涉密网络连接时，若非涉密网络与互联网物理隔离，则采用双向网闸隔离涉密网络与非涉密网络；若非涉密网络与互联网是逻辑隔离的，则采用单向网闸隔离涉密网络与非涉密网络，保证涉密数据不从高密级网络流向低密级网络。如下图所示：

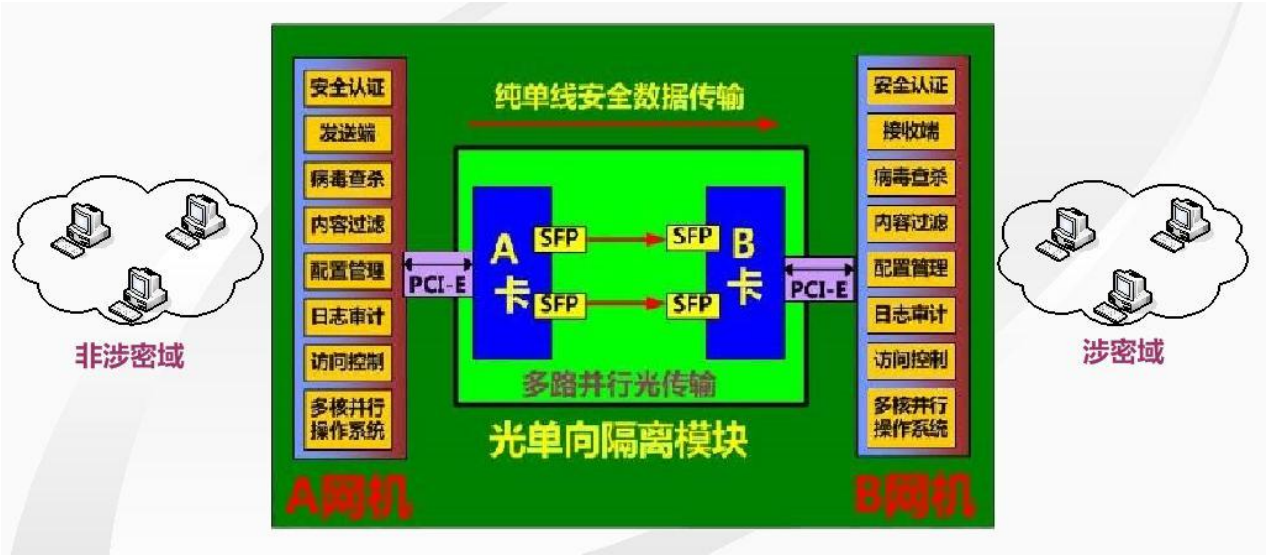




政府涉密网络、军工、电力等行业中含有大量的敏感信息及涉密数据（可能定级为涉密网或含有敏感数据的非涉密网），这些涉密数据是绝对不能流入比它密级低的网络中的，但这些网络通常又需要能从密级低的网络中获取数据。目前大多是采用人工拷盘的方式，但是人工拷盘存在安全隐患、效率较低。随着网神安全隔离技术的沉淀与积累，通过 2 年多的探索与研发，推出光单向安全隔离数据自动导入系统（简称单向网闸），通过此产品可以完美替代人工拷盘。网神信息技术（北京）股份有限公司的单向网闸可以满足电子政务网中的上述数据单向流动的要求，保证单向的数据流，实现数据保密性要求。

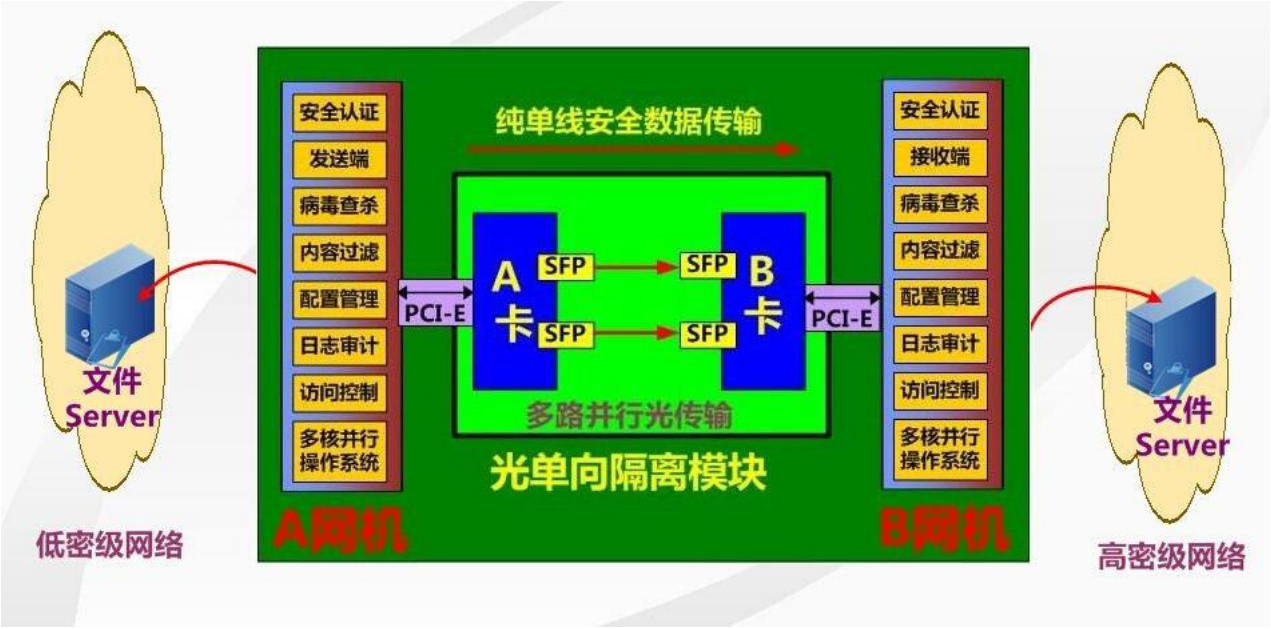
2 .产品原理

网神 SecSIS 3600 光单向安全隔离数据自动导入系统采用“2+1”模块结构设计，即包括 A 网主机、B 网主机模块和光单向隔离交换模块。A、B 网主机模块具有独立运算单元和存储单元，分别连接可信及不可信网络，对访问请求进行预处理，以实现安全应用数据的剥离。光单向隔离交换模块采用专用的单通道隔离交换卡实现，通过内嵌的安全芯片完成 A、B 网主机模块间安全的数据单向传输。A、B 网主机模块间不存在任何网络连接，因此不存在基于网络协议的数据转发。光单向隔离交换模块是内外网主机模块间数据交换的唯一通道，本身没有操作系统和应用编程接口，所有的控制逻辑和传输逻辑固化在安全芯片中，自主实现 A、B 网数据的单向传输及验证。在极端情况下，即使黑客攻破了外网主机模块，但由于无从了解光单向隔离交换模块的工作机制，因此无法进行渗透，内网系统的安全仍然可以保障。系统结构如下图所示：



光单向安全隔离数据自动导入系统体系结构图

网神 SecSIS 3600 光单向安全隔离数据自动导入系统部署在低密级网络与高密级网络之间，部署如下图所示：



网神 SecSIS 3600 光单向安全隔离数据自动导入系统工作过程分为三个步骤：定向数据获取、单向数据搬运、定向数据推送。

- **步骤一：数据定向获取**

低密级网络存放特定文件服务器。光单向导入系统 B 网机主动连接到外网文件服务器，确保从指定数据源获取数据。光单向导入系统将获取到的数据进行深度内容过滤及病毒过滤，保证传入数据纯洁安全。

- **步骤二：单向数据搬运**

网神 SecSIS 3600 光单向安全隔离数据自动导入系统会将数据文件通过光单向隔离模块

单向导入系统 A 网机。光单向隔离模块使用光纤中的一根，一端发，一端收，通过光的盲发机制，保证数据流向的单向性，从而在硬件上保证涉密网里的涉密数据或敏感信息绝对不会泄露。

- **步骤三：数据定向推送**

网神 SecSIS 3600 光单向安全隔离数据自动导入系统 A 端机将主动连接高密级网络里指定文件服务器，连接成功后将数据文件推送到服务器指定目录下。

3 .产品功能说明

3.1 多样的文件同步方式

网神 SecSIS 3600 光单向安全隔离数据自动导入系统采用模块化的系统结构设计，根据不同的应用环境，量身定制多种文件同步方式，以满足用户的不同需求，主要包括：

- **FTP 文件交换协议模块**

支持 FTP 文件传输协议，B 网主机可通过 FTP 协议获取 FTP 服务器文件，A 网主机可通过 FTP 协议推送文件至外部 FTP 服务器。

- **SMB 文件交换协议模块**

支持 SMB 文件传输协议，B 网主机可通过 SMB 协议获取服务器中的文件，A 网主机可通过 SMB 协议推送文件至外部服务器。

- **专用客户端文件交换协议模块**

专用文件单向导入客户端，通过与网闸之间认证、数据加密后实现文件交换；不需要用户将需要同步的文件以 SMB、FTP、NFS 等方式共享出来，保证文件服务器的安全保密。

3.2 深度内容过滤

通过 FTP 或者专用客户端等方式进行数据获取并摆渡的同时，能够对获取的数据进行深度内容过滤。包含：发送或接收文件的文件名的格式进行过滤；发送和接收文件的文件扩展名进行过滤；系统根据文件中是否包含不可显示字符将文件分为纯文本文件和二进制文件两类，用户可选择是否允许发送或接收二进制文件；用户通过对发送白名单、发送黑名单、接收白名单、接收黑名单功能对发送或接收文件的关键字进行过滤。

3.3 灵活的文件同步方式，用户可按需使用

网神 SecSIS 3600 光单向安全隔离数据自动导入系统采用多种文件同步方式，包含源端复制同步方式、源端移动同步方式、源端删除同步方式等多种同步方式，用户可以根据实际需求按需使用。

3.4 内置的单向数据库导入模块

网神 SecSIS 3600 光单向安全隔离数据自动导入系统，内置数据库导入模块，独立自主开发完成，完全内置于网闸内部，所有的同步操作由网闸自己独立完成。不在用户数据库中安装任何客户端软件，不需要在用户网络中部署专用服务器，对用户数据库不作任何改变。在高速运行的基础上解决了字段级数据同步、大字段同步等技术难题，适合于各种数据库同步工作的需要。

由于是网闸自身发起的动作，所以网闸两侧不开放任何基于数据库访问或者定制 TCP 的网络服务端口，避免网络安全漏洞。

3.5 分发访问

网神 SecSIS 3600 光单向安全隔离数据自动导入系统，部署两台光单向由网闸自身完成基于标准 TCP 访问应用；

3.6 多样协议的传输支持

网神 SecSIS 3600 光单向安全隔离数据自动导入系统，分别根据不同的协议，开放不同的功能模块，包括：

- 单向 TCP：支持 TCP 协议的单向传输；
- 单向 UDP：支持 UDP 协议的单向传输；
- 单向 JMS：支持基于 JMS 消息应用的单向数据传输；

3.7 多样化的身份认证

网神 SecSIS 3600 光单向安全隔离数据自动导入系统支持多样灵活的身份认证方式，包

括：本地用户名及口令认证、U-Key 认证、基于数字证书的认证多方式结合的双因子认证。

- **本地认证**

系统内置认证数据库提供本地的用户名、口令认证，支持 HTTP/HTTPS 方式实现认证信息的获取。

- **U-Key 认证**

提供随机 U-key，存储私钥以及数字证书，利用 U-Key 内置的公钥算法或根证书实现对用户身份的认证；

- **数字证书认证**

网闸支持数字证书认证，允许客户端通过 HTTP 连接向服务器发送访问请求。网闸可导入根证书，通过检查用户证书格式、证书的过期时间、签发者等信息以确认访问者身份的合法性，还可依据用户身份属性判断其是否具有适当的访问权限。

- **双因子认证**

网闸支持用户/密码+U-Key 方式、用户/密码+数字证书方式的双因子认证，认证强度更高，安全性更强；

3.8 防病毒

网神 SecSIS 3600 光单向安全隔离数据自动导入系统内嵌文件病毒查杀模块，支持多种杀毒引擎，并能够灵活地支持在线、本地病毒库升级；能够对需要摆渡的文件进行病毒、恶意代码程序、木马等进恶意程序进行过滤。

3.9 高可靠性设计

网神SecSIS 3600 光单向安全隔离数据自动导入系统采用高可靠性设计,支持电源冗余、端口冗余等机制，保证设备可靠运行。

3.10 地址绑定

提供 IP 与 MAC 地址绑定功能，可对指定接口所连接的网络中的主机的 IP 和 MAC 地址进行绑定，防止内部用户盗用 IP 和内网地址资源分配的混乱，方便网络 IP 资源管理。

3.11 轻松的管理

网神 SecSIS 3600 光单向安全隔离数据自动导入系统配备专门的管理端口，通过数字证书认证与管理信息的加密传输实现网闸设备的集中管理。系统采用全中文的 Web 方式进行远程网络管理，界面友好，操作方便。系统管理员和审计员实现分权管理，使得对网闸的管理更加安全可控，避免人为因素带来的安全风险。

3.12 传输方向控制

网神 SecSIS 3600 光单向安全隔离数据自动导入系统通过光传输技术通信机制，实现从低安全区域到高安全区域的单向数据传输，能够保证高安全区域数据绝对不会流失到低安全区域。

3.13 完善的安全审计

网神 SecSIS 3600 光单向安全隔离数据自动导入系统提供管理员多种手段了解网络运行状况及可疑事件的发生。用户可根据特定的需要进行日志审计（包括系统日志、访问控制策略日志、应用层协议分析日志、应用层内容检查日志等）。系统支持本地日志缓存，可实现本地日志的浏览查询等操作。日志依据事件的重要程度分为错误/警告/通知三级，支持 Syslog 日志存储，可实现日志的分级发送。

3.14 强大的抗攻击能力

网神 SecSIS 3600 光单向安全隔离数据自动导入系统具备强大的抗攻击能力，内外网主机模块采用专用的安全多核并行安全加固操作系统，内核经过特殊定制，实现强制性访问控制，保护自身进程及文件不被非法篡改和破坏。同时系统实现了针对多种 DoS 和 DDoS 攻击的防范，可阻挡 SynFlood、UdpFlood、PingFlood、TearDrop、Ping of Death、Smurf、Land 等多种类型的 DoS 和 DDoS 攻击，保护可信网络的安全。

3.15 多样化的身份认证

网神 SecSIS 3600 光单向安全隔离数据自动导入系统支持多样灵活的身份认证方式，包

括：本地用户名及口令认证、基于数字证书的认证等等。

- **数字证书认证**

网闸支持数字证书认证，网闸可导入根证书，通过检查用户证书格式、证书的过期时间、签发者等信息以确认访问者身份的合法性，还可依据用户身份属性判断其是否具有适当的访问权限。

- **本地用户名及口令认证**

网闸向第三方认证服务器发送用户名和口令，一旦认证服务器认证成功，则网闸允许用户访问。

- **第三方认证**

支持与第三方认证服务器进行认证。

3.16 易用使用的特色功能

网神 SecSIS 3600 光单向安全隔离数据自动导入系统具有多种易用使用的特色功能。包括：液晶面板功能、SNMP 功能、SISLOG 功能、配置导入导出功能、设备运行状态检测功能、系统资源查看功能、网络命令调试功能、补丁管理功能等多种使用功能，方便用户使用。

4 .技术优势

在网络中部署网神 SecSIS 3600 光单向安全隔离数据自动导入系统既能够符合政府、军队、企事业单位等的强制性安全策略－－既在不同安全等级的网络间实现安全隔离，又能够保证可靠、安全的信息交换，提供文件交换服务，在网络应用的安全性及可用性间取得完美的平衡。

4.1 采用光为传输介质，误码率低

A、B 网主机间通过光为传输介质，具有信号强度高，频率集中等特点，不会有任何光信号衰减，所有误码率低。

4.2 高效传输

SFP（Small Form-factor Pluggables）是千兆位电信号转换为光信号的接口器件，理

论速度为双向 2.5Gbps/s，通过 8b/10b 编码方式，实际上能够达到的最高速度为 2 Gbps/s，四个 SFP 口也就是 8 Gbps/s 。因此不存在性能瓶颈。

PCIE（PCI Express）是新一代的总线接口，x1 的理论速度是 2.5 Gbps/s，也要经过编码处理实际上能够达到的最高速度为 2 Gbps/s，x4 也就是 8 Gbps/s；

4.3 私有协议传输，保证高安全性

FPGA 设定了一个私有协议，可以在两个交换卡之间传递数据，从而实现主板之间的数据传输；

4.4 “协议落地“等多种机制最大化保证数据传输完整性

网神 SecSIS 3600 光单向安全隔离数据自动导入系统，在内外网各有一块硬盘，保证服务器到网闸单侧的数据的绝对完整性。

系统会对每个传输完成的文件计算 MD5，当目的端接收到的文件 MD5 校验不一致，则会主动删除目的端的文件。

系统任务配置中可以配置“优先级”和“冗余”，对于重要文件，可以设定文件优先发送和单向发送的次数，保证目的端接收文件的完整性。

从系统 B 网主机中手动导出本端同步的文件目录，导入 A 网主机，可以在 A 网主机系统上发现接收错误的文件。

4.5 安全高效的硬件交换系统

网神 SecSIS 3600 光单向安全隔离数据自动导入系统具有自主研发的 A、B 主机系统间的安全检测与控制处理单元，采用专有电路设计的单通道、单方向高速数据光交换卡，实现了独立的硬件交换控制逻辑，无操作系统及任何“软”控制，自主完成数据的交换，系统只负责把数据写到隔离交换卡中的缓冲区，由隔离交换卡根据硬件控制逻辑自动完成数据交换，自动同步两侧控制逻辑，进行互斥的读写操作。在保证安全性的同时，提供更好的处理性能，能够适应各种复杂网络环境对隔离应用的需求。

网神 SecSIS 3600 光单向安全隔离数据自动导入系统在内外主机系统间采用专有协议，阻断网络连接，不仅使得信息网络的抗攻击能力大大增强，而且有效地防范了信息外泄事件的发生。

4.6 提供无反馈信号的单向数据通道

网神SecSIS 3600光单向安全隔离数据自动导入系统在具体的实现技术中采用了先进的数据二极管技术。数据只是单向的“盲发”，没有反向的控制协议，也就是一方只管发送，另一方只管接收，反向没有数据通道也没有控制通道，完全处于盲状态。也可以理解为在传统的全双工通讯中只选择一个方向的线路，所以也称为信息流的单向技术。SFP 光模块作为传输接口，可以实现彻底的单向安全数据通路，即从硬件上彻底保证了单向性，保证涉密网数据不能外流。

4.7 核心应用的安全最大化

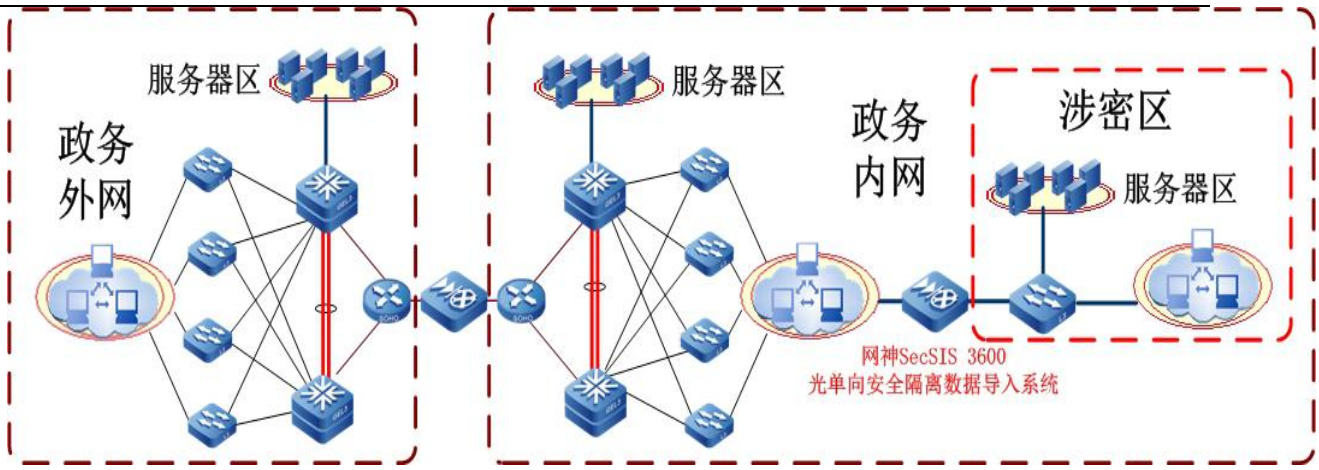
从安全实现的角度来讲，越接近应用层，则安全问题越复杂，解决问题也越困难。光单向安全隔离数据自动导入系统将应用层的数据转换成专有的数据格式进行处理，只允许安全的、可靠的信息在网络中传递。信息的格式、内容、交流对象等因素可依据企业安全策略指定，简化了核心应用面临的安全问题，确保了核心应用的安全最大化。

传统的安全检测产品只能发现利用已知安全漏洞发起的攻击。如果一种攻击手法还没有公布，则凭借现有的技术无法了解其攻击特征，也就无法识别攻击行为。网神 SecSIS 3600 对数据的交换不依赖于任何通用协议，没有数据包的处理及连接会话的建立，而是以静态的专有格式化数据块的形式在内/外网间传递，因此不会受到任何已知或未知漏洞的威胁。

5 .典型应用

5.1 政府行业

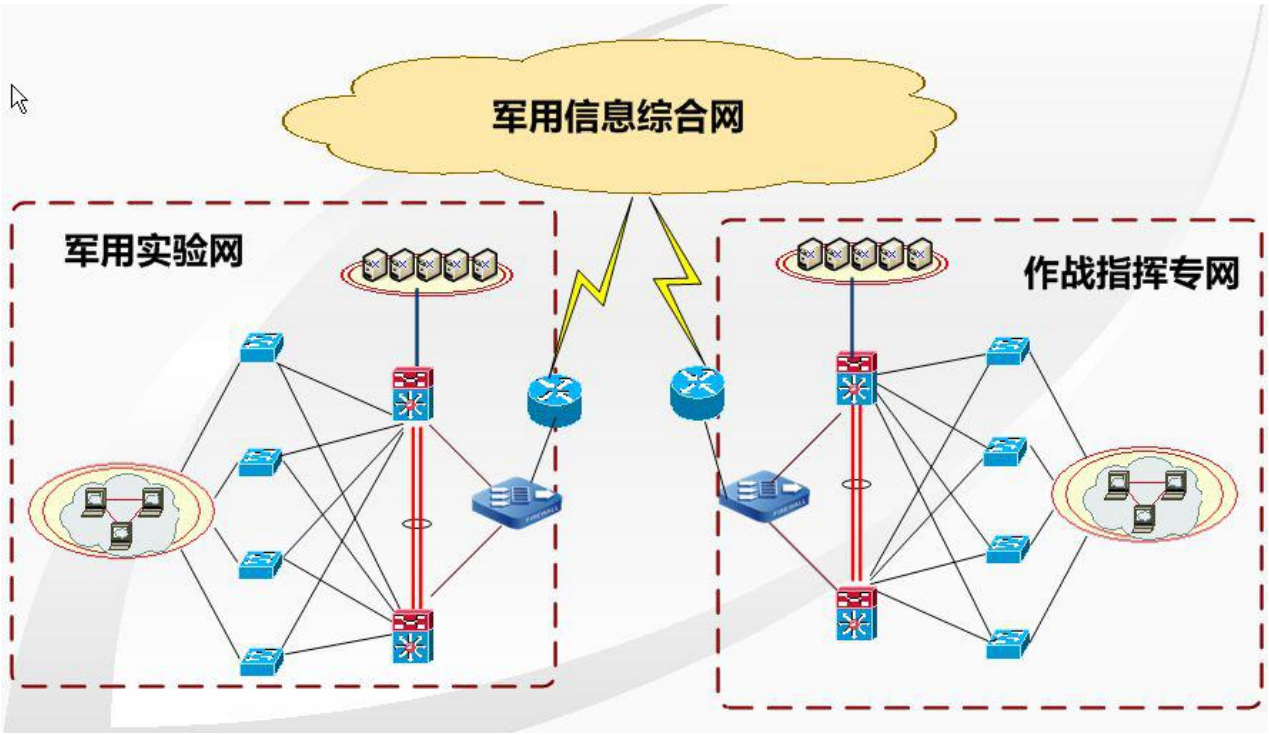
某政府部门开展网上审批业务，允许公众通过互联网提交服务申请并提交相关审核资料。如果允许访问者通过 Web 服务器直接向核心服务器发起数据访问请求和文件提交，则黑客可能穿透防火墙的保护直接侵入服务器，修改审批数据，甚至入侵涉密区服务器，窃取机密文件及信息，从而严重威胁到政府机密信息。如何正常提供电子政务应用的同时，保障政府部门涉密信息的安全成为不可忽视的安全问题。针对以上需求政府行业涉密网络与政务内网间部署网神 SecSIS 3600 光单向安全隔离数据自动导入系统，如下图所示：



此方案将政务网络划分为三个不同的安全级别区域，由低到高分别为政务外网、政务内网和涉密区域。方案中在政务内网和涉密区网络间部署网神 SecSIS 3600 光单向安全隔离数据导入系统，实现安全隔离，并达到数据文件只能进行低密区向高密区单向传输方式。此方案既满足保密局相关政策要求，同时又为电子政务的有效开展提供了可靠的保证。

5.2 军工行业

随着军工网络信息化的建设，如何保证数据单向获取，同时保证涉密网中的涉密数据或敏感数据不会外流，成为军工网络信息化建设的烦恼！军工行业网络包含三部分，分别为军用信息综合网、军用作战指挥专网、军用实验网。军用信息综合网安全级别要求最低，军用作战指挥专网及军用实验网中含有大量的涉密数据，此数据绝对不能外流的同时，需要从军用信息综合网中获取相关数据。针对以上需求，网神通过单向安全隔离数据自动导入系统部署在军用信息综合网与军用作战指挥专网之间、军用信息综合网与军用实验网之间，实现军用信息综合网数据单向自动导入至军用作战指挥专网中及军用实验网中，网络拓扑结构如下图所示：



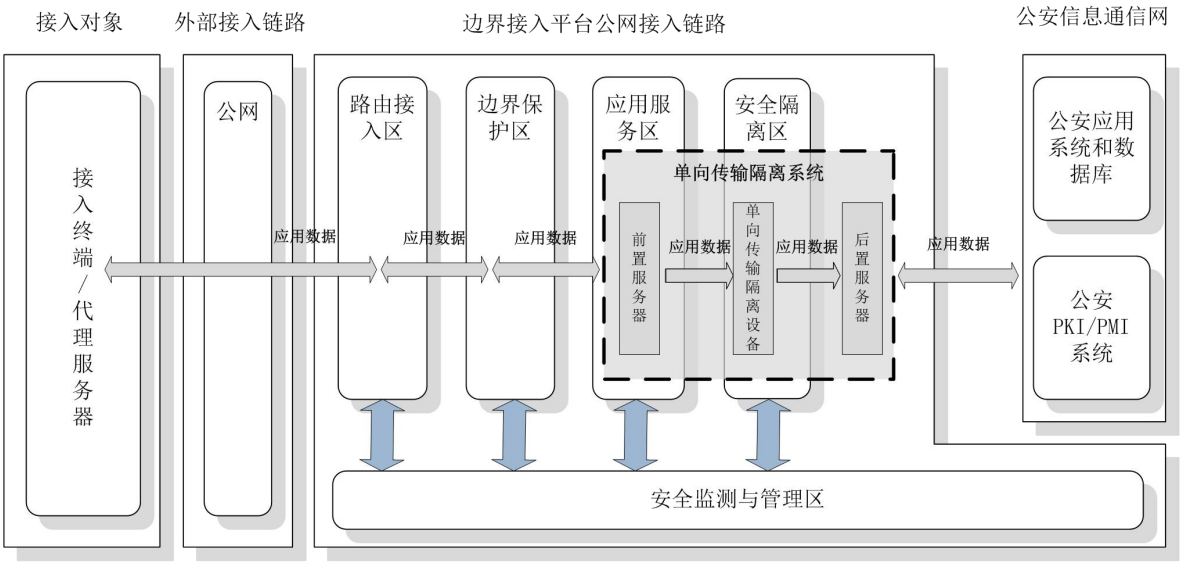
通过网神 SecSIS 3600 光单向安全隔离数据自动导入系统实现如下功能：

- 实现军用信息综合网数据单向导入至军用试验网及作战指挥专网，满足军工行业业务需求；
- 确保军用实验网及作战指挥专网中数据不会外泄，绝对不会泄密；
- 确保军用实验网及作战指挥专网中数据不会被攻击、破坏及窃取；
- 通过文件防病毒模块，防止军用实验网及作战指挥专网的病毒入侵；
- 满足涉密网建设的相关标准及要求；

5.3 公安行业

随着公安行业信息化建设的开展，公安信息通信网需要向公共网络、社会企事业单位、党政机关单位进行信息采集。如何保证数据单向获取，同时保证公安信息通信网中的涉密数据或敏感数据不会外流，成为公安信息化建设的关键。

在单向链路中，社会各行业的数据采集应用终止于应用服务区。在应用服务区与公安信息通信网之间，通过单向传输隔离系统进行单向传输。单向传输隔离设备的主要安全功能为：实现前置服务器与后置服务器的安全隔离；根据安全策略，对从前置服务器到后置服务器的数据进行格式检查和内容过滤，从而保证数据由应用服务区安全地传输到公安信息通信网。如下图所示：



通过网神 SecSIS 3600 光单向安全隔离数据自动导入系统实现如下功能：

- 实现公共网络、社会企事业单位、党政机关单位网数据单向导入至公安信息通讯网，满足公安行业业务需求；
- 确保军用公安信息通讯网中数据不会外泄，绝对不会泄密；
- 确保军用公安信息通讯网中数据不会被攻击、破坏及窃取；
- 满足涉密网建设的相关标准及要求；