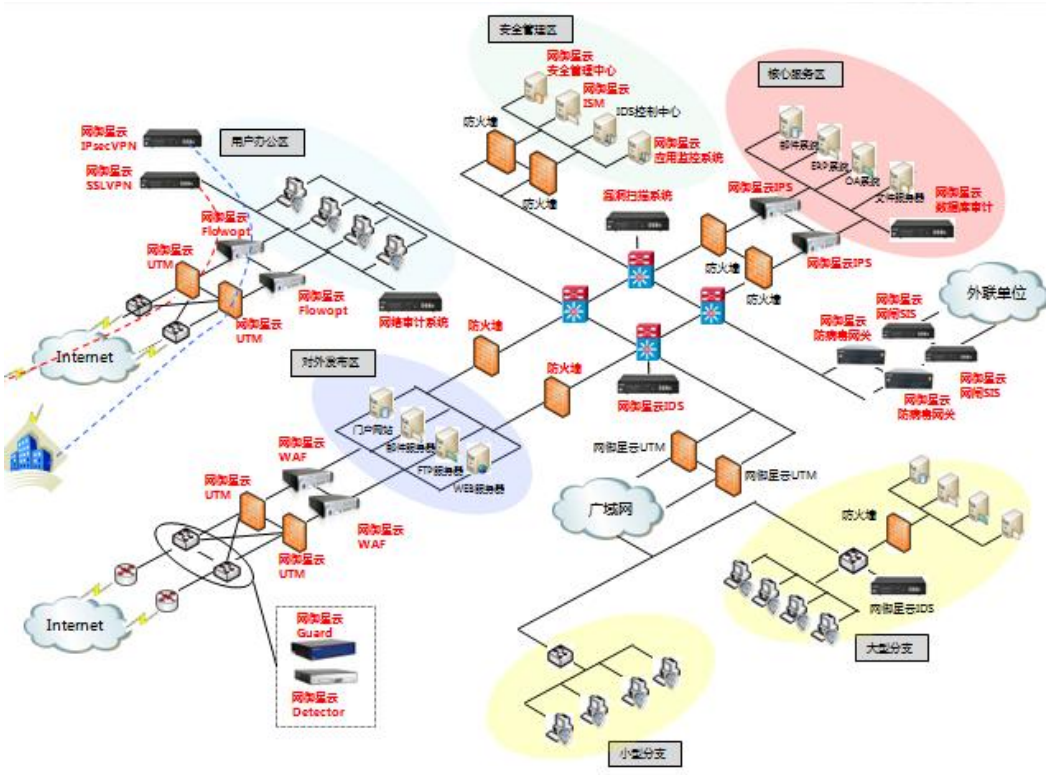
网络安全产品介绍



金钻芯公司销售安全产品全景图：

销售产品有：防火墙 、加固安全网关、 IPSec VPN 网关、 SJW87 网络密码机、 防病毒安全网关、 入侵防护系统、 SSL VPN 应用安全网关、 Web 应用安全防护系统、 安全隔离与信息交换系统、 入侵检测系统、 网御 ATM 异常流量管理系统、 网络优化与流量控制系统 、网络审计系统（数据库审计型）、应用监控管理系统、 安全管理系统等

网御防火墙：

- 多威胁统一管理的多功能防火墙
- 基于应用识别的绿色上网控制模块

◆ 部署了 3 万多台套的高可用防火墙

网御安全隔离与信息交换系统：

网御安全隔离与信息交换系统（以下简称"安全隔离网闸"）基于"2+1"系统架构、Leadsec 专用芯片、USE 统一安全引擎、MRP 多重冗余协议，将安全性、高效性、智能性、可靠性完美结合。对数据在应用层细粒度安全过滤后，以自有协议方式在安全隔离网闸内摆渡，彻底切断了不同安全级别网络间的任何连接，实现了高安全的隔离和实时的信息交换。

网御安全隔离网闸，按照军标级设计要求，采用机箱加固结构、电磁屏蔽机箱、设备健康监测指示灯、低噪低耗 SmartFan 等多项技术，保障产品的高可靠性，为用户提供高品质产品。

网御 IPS 产品发展历程：

2007 年 第一季度网御 IPS 产品成功上市；

2007 年 网御推出业内首款“内外兼修”的 IPS 产品；

2008 年 网御 IPS 产品 IDC 市场排名第一；

2009 年 网御推出基于 MIPS 多核架构的万兆 IPS 产品；

2010 年 网御推出基于主动云防御的 IPS 产品；

2011 年 网御 IPS 产品全面支持 IPV6；

2012 年 网御推出面向下一代全业务融合 IPS 产品；

入侵检测系统

产品概述

网御凭借在防火墙、入侵检测、应用分析等方面的深厚积累，倾力打造出了业内首款“内外兼修”的入侵防护系统（以下简称“IPS”）。网御 IPS 基于 VSP 通用安全平台和 USE 统一安全引擎，综合采用会话状态检测、应用层完全分析、误用检测、异常检测、网络审计、主动云防御等分析与检测技术，实现了“基于 IPV4/IPV6 双栈协议下的入侵检测与实时阻断、应用层访问控制、上网行为管控、带宽管理”等核心功能，配合实时更新的入侵攻击特征库，做到了对网络数据流从高效阻止非法行为（净化）到按需限制合法行为（优化）的全面管理。

网络审计

产品概述

网御网络审计系统是基于嵌入式硬件和 VSP 安全平台的高性能、高稳定性的上网行为监控和内容安全审计设备，安装于网络出口的交换机或共享 HUB 上。系统主要以旁路监听的方式工作，可以根据实际环境的规模选择单机、分布式及其他多种部署方式，在完全不影响原有网络运行的情况下详实记录人员的各种网络行为和内容。

网御 **Web** 安全防护系统

多核架构：多核 SoC 硬件平台实际功耗仅为同档次 X86 平台的 1/3 左右

Web 应 用 防 护：防护基于 HTTP/HTTPS/FTP 协议的蠕虫攻击、木马后门、间谍软件、灰色软件、网络钓鱼等基本攻击；CGI 扫 描、漏洞扫描等扫描攻击；SQL 注入攻击、XSS 攻击等 Web 攻击。

安全事件统计分析：包括安全事件 TOP5、服务器攻击次数 TOP5、最近服务器访问量 TOP5 统计、事件级别与类别统计、源 IP 统计、 URL 统计等统计类型

网御入侵检测系统

网御入侵检测系统（以下简称：网御 IDS）基于分布式入侵检测系统构架的网络入侵检测系统（NIDS），采用网御 USE（Uniform Secure Engine）安全引擎，综合使用会话状态检测、应用层协议完全解析、误用检测、异常检测、内容恢复、网络审计等入侵分析与检测技术，全面监视和分析网络的通信状况。在入侵监控的基础上，遵循 CSC 关联安全标准，可主动发包或与多种第三方设备联动来自动切断入侵会话，实现实时有效的防护，为网络创建了全面纵深的安全防御体系。

网御安全管理系统

网御安全管理系统（以下简称 LEADSEC-SOC）是立足于公司十多年信息安全积累的基础之上，基于客户最新需求推出的全新一代安全管理平台。

LEADSEC-SOC 以 IT 资产为基础，以业务信息系统为核心，以用户体验为指引，从监控、审计、风险、运维四个维度建立一套可度量的统一业务支撑平台，使得各种用户能够对业务信息系统进行可用性、性能与服务水平监控，事件分析、审计、预警与响应、风险及态势的度量与评估，标准化、例行化、常态化的安全流程管控，从而最终实现业务信息系统的持续安全运营。

LEADSEC-SOC 采用新一代的基于超微内核的技术架构，融合多种信息安全技术和管理理念，充分实现组织、管理、技术三个体系的合理调配，帮助用户从监控、审计、风险、运维四个维度实现对业务信息系统的统一安全保障。

LEADSEC-SOC 采用开放平台架构设计，遵循业界通行的应用接口和管理接口，功能部件都实现了模块化装配，客户可以自由选择，并能够与客户的应用和管理环境实现良好的对接与整合。

LEADSEC-SOC 采用 B/S 架构设计，支持 WEB 管理方式，方便用户管理。

异常流量管理系统

网御根据多年对网络攻击和防护的深刻理解，倾力打造了异常流量管理系统 TAM。系统包括异常流量检测（TAM-Detector）、异常流量清洗（TAM-Guard）和管理中心（TAM-Manager）三个独立模块产品。Detector 可对不同网络节点的流量进行检测分析，Guard 对异常流量完成牵引和过滤，Manager 对 Detector 和 Guard 进行统一的策略管理、日志收集、报表呈现。

系统通过 Detector 、Guard 和 Manager 的协同防护，由 Detector 将流量检测分析结果上报 Manager，Manager 下发清洗策略给 Guard，Guard 完成异常流量牵引和过滤。最终 TAM 整个系统协同完成全网流量分析、异常流量牵引、DDoS 攻击流量清洗、可视化监控等功能，实现了检测-清洗-管理"三位一体"的解决方案,帮助用户实时了解网络运行状况，及时发现网络中出现的问题并自动对异常行为作出响应，从而快速清除异常流量造成的危害。

深信服上网行为管理：

- ◆ 上网缺乏管控
- ◆ 带宽被滥用
- ◆ 访问行为无法溯源
- ◆ 上网安全风险

深信服流控

深信服网络流量管理设备，采用基于队列的流量处理机制和分层三色令牌桶技术，并结合 DPI（数据包深度内容检测）、DFI（动态流状态检测）及智能识别等网络应用及数据识别技术，通过高性能硬件平台为客户提供业界性能卓越的流量管理方案。深信服流量控制产品凭借强大的应用识别能力、以及丰富的流量管理策略，可以实现对网络流量的全面透析与管控，优化网络带宽，为网络管理者提供了前所未有的网络可见性，真正意义上帮助用户构建可视、可控、可优化的高效网络。