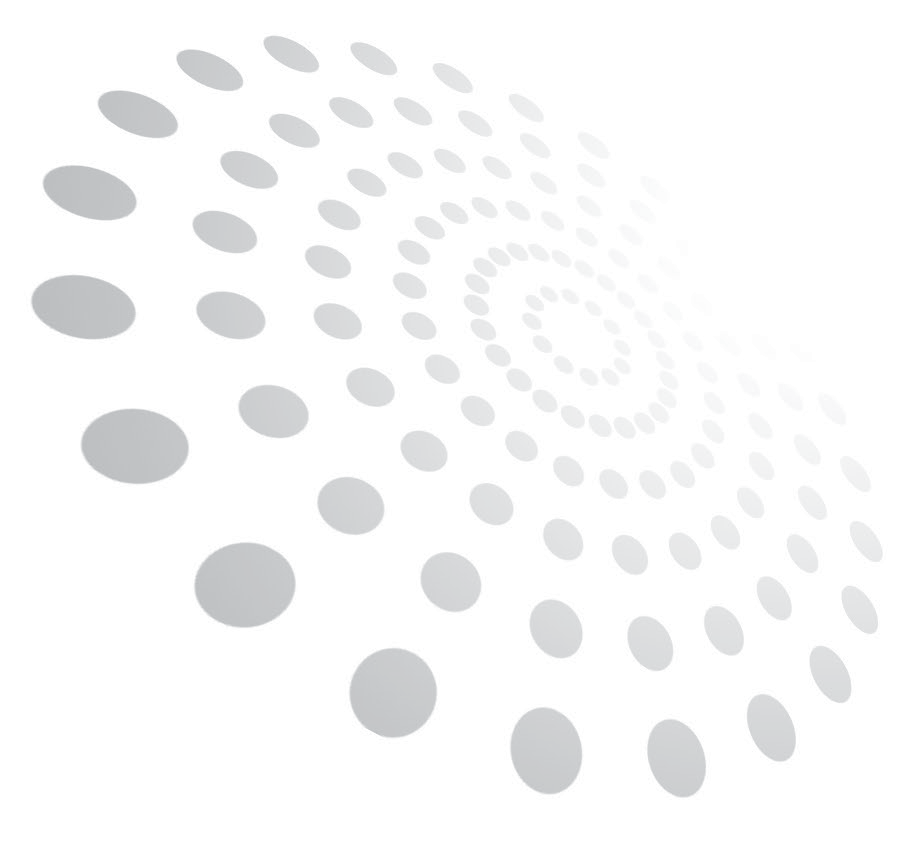




1607-V1





## 网络边界安全防护系列产品

## 应用与数据安全防护系列产品

## 全网安全管理系列产品

[第二代防火墙 02](#_TOC_250030)

[防火墙 04](#_TOC_250029)

[加固安全网关 08](#_TOC_250028)

[UTM安全网关 09](#_TOC_250027)

[新一代VPN安全网关 13](#_TOC_250026)

[SJW87及SJJ0805网络加密机 15](#_TOC_250025)

[网御防病毒网关 17](#_TOC_250024)

[入侵防护系统 20](#_TOC_250023)

[工业防火墙IFW-3000 23](#_TOC_250022)

[Web应用安全防护系统 26](#_TOC_250021)

[安全隔离与信息交换系统 29](#_TOC_250020)

[安全隔离与信息单向导入系统 31](#_TOC_250019)

[上网行为管理系统 33](#_TOC_250018)

[TAM异常流量清洗系统TAM-Guard 36](#_TOC_250017)

[TAM异常流量管理系统TAM-Detector 39](#_TOC_250016)

[应用交付控制系统Leadsec-ADC 41](#_TOC_250015)

[入侵检测系统 43](#_TOC_250014)

[网络审计系统（互联网审计型） 45](#_TOC_250013)

[网络审计系统（数据库审计型） 48](#_TOC_250012)

[网络审计系统（防统方专用版） 51](#_TOC_250011)

[内网安全管理系统Leadsec-ISM 54](#_TOC_250010)

[安全管理系统Leadsec-SOC 58](#_TOC_250009)

[安全管理系统 60](#_TOC_250008)

[日志审计系统Leadsec-RS 62](#_TOC_250007)

[网络行为分析系统Leadsec-NBA 64](#_TOC_250006)

[业务安全管理系统Leadsec-BSM 67](#_TOC_250005)

[安全配置核查管理系统Leadsec-CVS 69](#_TOC_250004)

[漏洞扫描系统 71](#_TOC_250003)

[APT检测 74](#_TOC_250002)

[入侵检测系统——虚拟威胁检测系统 76](#_TOC_250001)

[网络审计系统——FLowEye安全域流监控产品 80](#_TOC_250000)

# 第二代防火墙

## Web应用防护

网御星云

产品简介

### 网御第二代防火墙是基于自主操作系统开发的符合国内第二代防火墙标准的全新产品，该系统具备高性能、高安全性、高可靠性，提高了自身安全性的同时，加速了多线程的内容处理，为运行在其上层的防火墙、VPN、防病毒等安全引擎提供了强

第二代防火墙

第二代目前针对HTTP、FTP等Web服务的攻击呈愈演愈烈的趋势，尤其针对HTTP的攻击更是成为了各黑客组织出于政治目的发泄的重要手段。网御第二代防火墙基于快速识别的应用层威胁发现技术，可侦测超过500种 的针对HTTP、FTP的攻击行为。

## 灵活的数据审计，实现网络行为可追溯

网御第二代防火墙产品可以内置或外接USB硬盘，实现对上网行为、攻击、病毒及防火墙日志的全方位记录、统计、分析。通过设备内置数据中心对用户的访问过的URL、邮件收发、论坛发帖、文件传输、流量及数 据库访问等行为进行全面统计分析、个性分析、各种排行；支持定义报表模板，订阅关注的报表到指定的邮箱；对AV、IPS安全事件进行统计汇总以地图形式直观呈现。

产品优势

## 智能的VSP通用安全平台

采用创新的VSP（Versatile Security Platform）通用安全平台，将实时操作系统、网络处理、安全应用等

### 大而安全的性能支持。网御第二代防火墙在各个安全引擎中运用了新的算法和技术，针对病毒检测，内容分析等海量扫描活动使用了高效的启发式扫描；针对传统包过滤无法检测的威胁，采用了完全内容检测技术；针对未知的攻击行为，使用了实时动态保护技术。网御第二代防火墙除了具备基本Gartner所定义的下一代防火墙集成深度包检测入侵测试、应用识别与精细控制等标准特性外，还具备终端管理与内网安全，私有安全云有效防御APT攻击等。

02

### 网御第二代防火墙产品可广泛应用政府、教育、金融、媒体、能源、运营商、卫生医疗、大型企业、中小企业等行业。

产品荣誉

### 《GA/T 1177-2014 信息安全技术第二代防火墙安全技术要求》标准的制定参与单位

产品特点

技术完美地结合在一起，使产品具备了高智能、高性能、高安全性、高健壮性、高扩展性等特点。

## 高效的USE统一安全引擎

03

采用自主创新设计的USE（Uniform Security Engine）统一安全引擎，实现了多种安全功能独立安全策略的统一配置，可以方便用户构建可管理的等级化安全体系。

## 高可靠的MRP多重冗余协议

基于网御拥有的高可靠设计专利技术，利用电信骨干网可靠性运营维护专业经验，网御UTM安全网关通过自有的MRP多重冗余协议，在物理层、链路层、网络层、实体层等多个层面实现多元化冗余设计，有效地保障 网御UTM安全网关在用户网络应用中的高可用性。

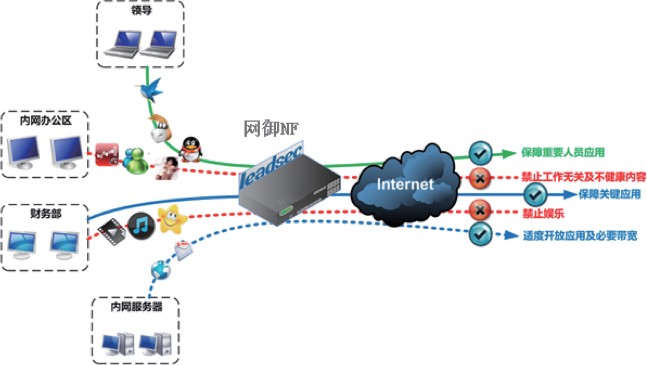
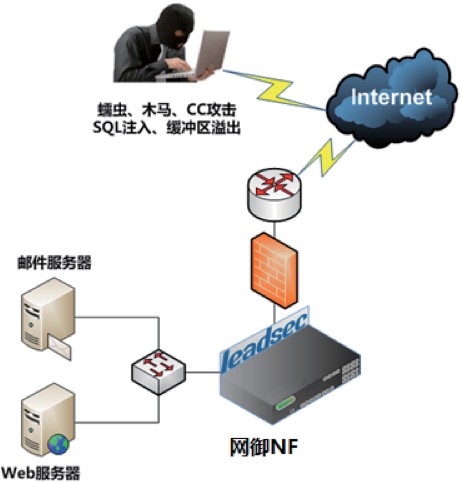
典型部署/应用

## 细粒度的高性能网络访问控制

### 在网御第二代防火墙中，通过深度防护规则实现网络访问控制，深度防护规则包含源地址、目的地址、源端口、源MAC、流入网口、流出网口、访问控制、时间调度、服务、是否为长连接、深度防护策略等多个控制子选项，对于不符合规则的访问，系统可以拦截并发出日志告警。

## 完善的应用控制

### 网御第二代防火墙对应用的识别基于应用行为和数据特征，而不是基于端口号，有效地提升了应用的识别率，避免了误判。尤其对P2P应用中的加密传输，网御第二代防火墙基于应用行为识别与主动探测相结合的方式，有效地克服了加密后无法识别的业内难题。通过精确的识别，网御第二代防火墙对IM软件实现了细粒度的控制，不但可以控制登陆，而且对文字聊天，文件传输，音频、视频都可以实现分类控制。



网络入侵防御解决方案示意图 应用监控解决方案示意图

# 防火墙

网御星云

产品简介

防火墙

* 《通信世界》：网御千兆线速防火墙“2003年200种优秀通信产品”
* 赛迪评测：网御2000防火墙“2002年度精品奖”
* 《网络世界》：网御2000防火墙“编辑推荐奖”
* 《中国计算机报》：网御2000防火墙“编辑选择奖”
* 技术监督情报协会：网御防火墙/VPN网关“3.15质量无投诉、服务无投诉诚信企业”
* 中国保护消费者基金会：网御防火墙“质量、服务、信誉”消费者可信产品
* 中国技术监督情报协会：网御防火墙“全国用户产品质量、售后服务满意十佳企业”
* 赛迪评测：网御2000防火墙“2001年度精品奖”

网御防火墙是网御自主研发的核心产品。目前已广泛应用在税务、公安、政府、部委、能源、交通、军队、电信、金融、企业等各行业， 并为其网络和应用提供安全保障。

网御防火墙分为超万兆、高端万兆、低端万兆、高端千兆、中端千兆、低端千兆以及百兆的高中低系列，共计80余款。网御防火墙是集防火墙、IPSEC VPN、SSL VPN、漏洞扫描、主动防御、入侵检测与防护系统、防网络病毒、内容检测与过滤、上网行为管理、带宽管理、高可用性等众多功能于一身的多威胁统一管理的综合防火墙。

04

产品荣誉

产品特点

## 基于应用的内容识别控制

（1）智能匹配技

网御防火墙按照所有上网行为的特点进行了分类，当经过防火墙的数据包根据用户定制策略匹配到其对应的特征库管道，再由相应搜索引擎对流量进行扫描。这样既大大减少了搜索引擎检索的时间，又提高了过滤引擎的性能。

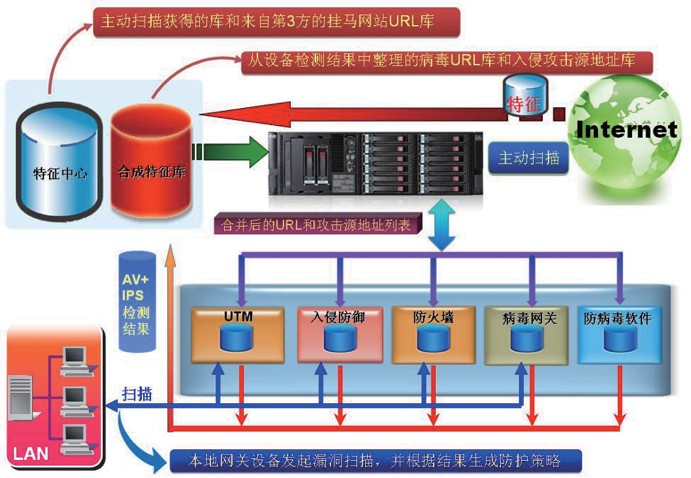
05

（2）多线程扫描技术

网御防火墙采用多线程扫描技术，提高了引擎扫描的效率。

（3）应用感控技术

网御新一代防火墙具有与传统的基于端口和IP协议不同的方式进行应用识别的能力，并执行访问控制策略。



* + 2010年中国信息安全最佳多核万兆防火墙系列产品
  + 2007年中国IT产品最具竞争力奖（PowerV-4812）
  + 中计报：2007年度技术之星奖（PowerV-4000）
  + 《计算机世界》：2006中国信息安全防火墙值得信赖品牌奖
  + 电脑商报：最佳渠道支持到位性奖
  + 2005年度中国网络安全防火墙用户大会：“用户推荐的防火墙产品奖”
  + 2005中国网络主管调查：防火墙企业信赖品牌奖
  + 中国电子信息产业发展研究院：2004中国IT用户“防火墙卓越产品奖”
  + 《计算机世界》：2004年度产品奖
  + IDC：2004年上半年联想集团防火墙市场占有率国内品牌第一
  + 2004中国网络技术与产品调查“网管员最喜爱的防火墙产品奖”
  + IDC：2003年上半年防火墙领域国有品牌销售额排名第一证明
  + 2003年中国IT服务用户满意度调查：防火墙产品“最佳服务承诺兑现奖”
  + 2003年中国网络安全系统防火墙用户大会：“用户推荐的防火墙产品”
  + “网管员之夜大型系列活动”：网御系列防火墙－“专家推荐的防火墙产品奖”
  + 赛迪评测：网御2000 千兆防火墙“技术创新奖”
  + 《中国计算机报》：网御千兆线速防火墙“编辑选择奖”
  + 《计算机世界》：网御千兆线速防火墙“2003年度产品奖”

## 精确细致的Web过滤技术

网御防火墙系列在内容过滤库的处理上力求收集齐全、分类准确、更新及时。通过采用网站全智能搜索引擎技术收集互联网站点，并进行智能分类、人工核验的处理手段。

## 可信架构主动云防御技术

网御防火墙通过与已部署的防病毒网关、IPS、UTM等设备联合抓取病毒源、攻击检测源和挂马网站URL等特征，汇集至云防御服务器定时收纳合并，共同形成整体可信架构云防御体系。

防火墙

## IPv6包状态过滤技术

网御星云支持IPv6功能包括：IPv6环境下的状态包过滤、静态路由、OSPF动态路由、FTP、ALG等基本安全控制，以及IPv6/v4双协议栈功能。

## BYOD用户与企业网络内网管理技术

网御防火墙针对用户接入设备网络采用三维一体的方式进行管理控制，即终端接入控制、远程接入控制、移动接入控制、虚拟桌面统一派送、云端服务集中存取。

## 高性能

网御具有行业内少见的高性能防火墙产品，小包吞吐最大可达80G，PPU等于40G，最大程度上满足企业安 全和性能、性能和体积、体积和功耗、投入和产出的双赢概念。

## 虚拟化

针对部分需要对设备进行物理合并的需求，网御防火墙支持将物理设备逻辑虚拟化的功能，可以虚拟出多台逻辑相互隔离、互不干扰的虚拟防火墙。多台虚拟防火墙之间，可以保持不同配置、更新不同补丁、防火墙重启互不干扰。最大程度上减少了虚拟防火墙之间的影响。具有统一的管理界面，每一台虚拟防火墙都支持资

06 源自定义，设备利用率统一查看。

产品优势

## 高可靠的MRP多重冗余协议

基于网御拥有的高可靠设计专利技术，网御防火墙通过自有的MRP多重冗余协议，在物理层、链路层、网络层、实体层等多个层面实现多元化冗余设计，有效地保障网御防火墙在用户网络应用中的高可用性。

* 基于多出口负载均衡的链路备份。链路层支持多WAN口出口，实现多出口间的负载均衡和备份。
* 基于802.3ad标准的端口聚合。物理端口支持802.3ad标准，可实现多物理端口聚合。
* 基于状态自动探测的双机热备。当主系统发生故障或对应线路的网络故障时，切换时间小于1秒钟。
* 基于状态增量同步的多机集群。支持主动负载均衡、会话保护和接管以及主动配置同步等功能，最多可以支持高达8台的防火墙集群。

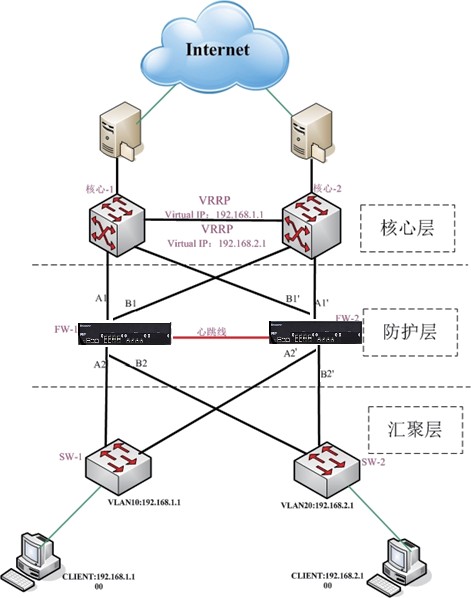
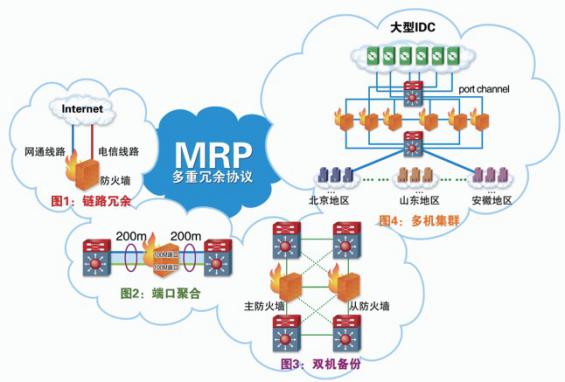
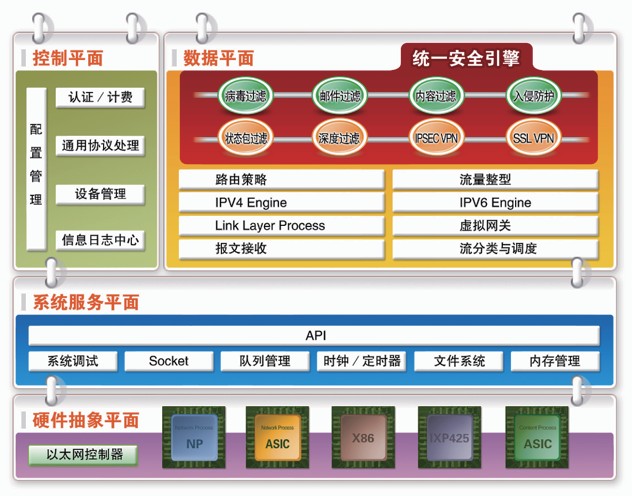
## 日志审计与报表功能

* 系统日志审计提供对设备系统日志的操作功能，并可以进行查询和导出。
* 上网行为日志审计对上网行为进行记录和审计，并可以进行查询和生成相应的报表。
* 日志审计和报表强大的日志审计功能。用户可根据需要从任意角度定制审计查询条件。内置日报，月报

等预设报表，用户可根据需要从任意角度定制报表。 07

* 日志维护提供审计中心管理功能，可以对日志信息进行同步，备份，恢复，删除等操作。
* 面向安全结论的报表，网御防火墙的报表系统分为历史报表、风险智能报表、趋势报表、统计报表、对比报表等，并且可以根据报表模板自定义报表类型，让使用者可以通过分析报表清楚地看到当前是否存在安全风险以及不合规操作等。

## 智能的VSP通用安全平台



网御防火墙采用创新的VSP（Versatile Security Platform）通用安全平台，将实时操作系统、网络处理、安全应用等技术完美地结合在一起，使防火墙产品具备了高智能、高性能、高安全性、高健壮性、高扩展性等特点。

## 高效的USE统一安全引擎

网御防火墙具有高效的USE（Uniform Security Engine）统一安全引擎。它将状态包过滤、VPN、IDS、内容过滤、用户认证等多个子系统集成于单一平台，实现统一的安全引擎处理机制。

典型部署/应用

许多骨干网络的可靠性要求很高，不允许出现因为设备的故障造成网络的不可用，因此在电信网络和骨干网络中加入防火墙的时候也必须考虑到这个问题。正常情况下两台防火墙均处于工作状态，可以分别承担相应链路的网络通讯。当其中一台防火墙发生意外宕机、网络故障、硬件故障等情况时，该防火墙的网络通讯自动切换到另外一台防火墙，从而保证了网络的正常使用。下图为网御防火墙在骨干网络中应用的例子。

加固安全网关/UTM安全网关

网御星云

加固安全网关

网御星云

UTM安全网关

产品简介 产品简介

网御加固安全网关产品系列适用于车载、舰载、机载移动网络的安全威胁防护，可应用于卫星接入、3G/4G、高速以太网等通信网络，具有良好的抗电磁干扰、防振动、抗冲击、防淋雨等抗恶劣环境特性。网御加固安全网关支持防火墙、VPN等方面的安全防御功能，并可根据用户的个性化需求定制开发与生产。

08 产品特点

## 高低温与全封闭防潮设计 高强度抗电磁干扰能力

网御UTM（Unified Threat Management）安全网关采用先进的多核多线程并行运算技术、USE统一安全引擎技术、智能业务处理引擎BPE 技术保证功能全开状态下的高吞吐量运行，通过高效的模版式配置管理、远程URL特征库、灵活嵌入式防病毒和持续的安全服务，配合基于行为分析而优化的配置流程，构成一个先进的

全业务融合安全架构。网御UTM集成了状态检测防火墙、VPN、网关防病毒、入侵防护（IPS）、上网行为管理、反垃圾邮件等安全防护功能，还全面支持策略管理、IM/P2P管理、负载均衡、高可用性（HA）和带宽管理等功能。可以阻挡未授权的访问、网络入侵、病毒、蠕虫、木马、间谍软件、钓鱼诈骗、垃圾邮件，以及其他类型的安全威胁。

09

* 基于智能温控芯片的宽温设计
* 基于低功耗器件的无风扇设计
* 基于合金舱门的密封防潮设计
* 基于内核低扰和分级屏蔽的高可信设计
* 基于功能单元和分阈隔离的模块化设计
* 符合GJB151A-97电磁发射和敏感度要求

产品荣誉

* 中国安全网关产品市场领导奖
* 中国区统一威胁管理产品市场领导奖

## 抗跌落抗冲击及防振设计 立体化数据保护体系设计

* + 2013年中国信息安全年度网关产品金奖
* 基于高可靠连接的零线缆设计
* 基于框架式保护的强缓冲设计
* 符合GJB322A-98通用规范要求

产品优势

* 基于双系统引导的冗余保护技术设计
* 基于程序环境与数据环境的分离设计
* 基于多重冗余协议的多链路复用设计

产品特点

## 细粒度的高性能网络访问控制

通过深度防护规则实现网络访问控制，深度防护规则包含源地址、目的地址、源端口、源MAC、流入网

网御加固安全网关采用一系列领先的抗恶劣环境设计，通过了严酷的第三方测试，能够从容应对各种复杂苛刻的开放式使用环境。



* + 车载应用：适用于颠簸振动、强电磁干扰、沙土飞扬、高温严寒等野外环境；
  + 舰载应用：适用于潮湿封闭、盐雾霉菌、高压振动等水上水下作业环境；
  + 机载应用：适用于高频振动、高温严寒、高压急速，强电磁干扰等环境。

口、流出网口、访问控制、时间调度、服务、是否为长连接、深度防护策略等多个控制子选项，对于不符合规则的访问，系统可以拦截并发出日志告警。

UTM安全网关

## 精准高效的入侵防御

网御UTM安全网关具备3000种以上攻击特征库规则列表，并可自定义特征库，在蠕虫、后门、木马、间谍软件、Web攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计报警等防御手段，完全满足用户的各种应用需要。

典型部署/应用

## 性能和功能完美匹配的病毒防御

网御UTM安全网关采用自有知识产权的病毒防御引擎，针对非缓存流检测模式进行了全面结构调整和优化，不少于600万种病毒特征做为病毒规则库，使安全网关的病毒检测率和处理性能获得质的突破：在保持高病毒检测率的同时，系统性能下降不超过20 ，是业界第一个建议用户把网络访问控制、病毒防御、入侵防御等全部功能同时开启使用的安全网关产品。

产品优势

## 智能的VSP通用安全平台

11

网御UTM安全网关采用网御自主研发的专用安全操作系统VSP（Versatile Security Platform），将实时操作系统、网络处理、安全应用等技术完美地结合在一起，使产品具备了高智能、高性能、高安全性、高健壮性、高扩展性等特点。

10

网络访问控制兼顾病毒防御解决方案示意图

## 高效的USE统一安全引擎

采用自主创新设计的USE（Uniform Security Engine）统一安全引擎。实现了多种安全功能独立安全策略的统一配置，可以方便用户构建可管理的等级化安全体系。

## 高可靠的MRP多重冗余协议

基于网御拥有的高可靠设计专利技术，利用电信骨干网可靠性运营维护专业经验，网御UTM安全网关通过自有的MRP多重冗余协议，在物理层、链路层、网络层、实体层等多个层面实现多元化冗余设计，有效地保障网御UTM安全网关在用户网络应用中的高可用性。

## 无缓存的协议重组和跨数据包连续匹配技术

网御UTM安全网关针对协议重组模块为保存会话信息、应用层协议分析和解码、特征匹配等工作而带来的大量内存拷贝动作，采取了无缓存的协议重组和跨数据包连续匹配技术，减少了数据的延迟，此技术已申请相关的专利。

网络入侵防御解决方案示意图

UTM安全网关/新一代VPN安全网关

网御星云

新一代VPN安全网关

产品简介

上网行为管理解决方案示意图

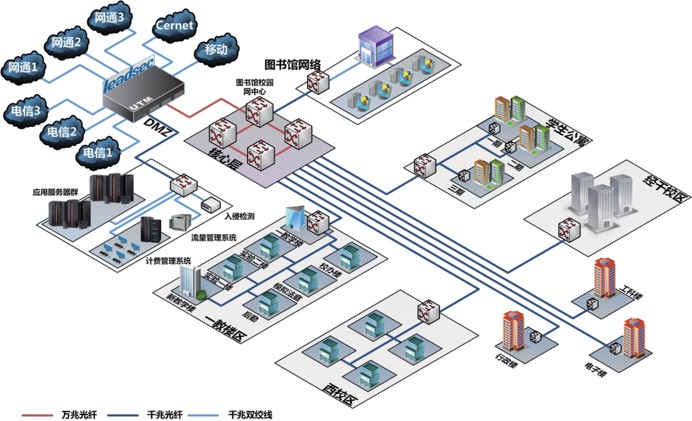
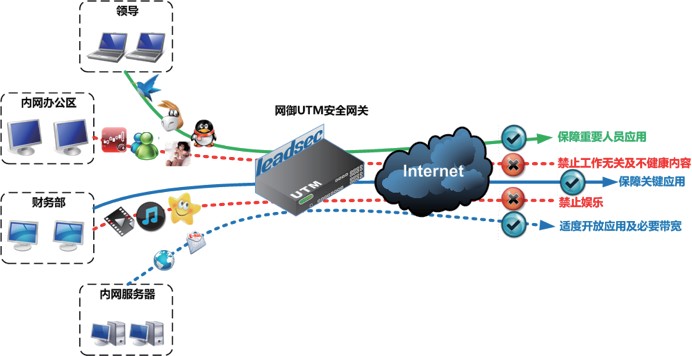
网御新一代VPN安全网关是集VPDN、IPSEC、SSL VPN于一身，兼具用户认证、访问控制、NAT、SAML众多功能的综合性VPN安全网关，具有稳定强、易用强、网络环境适应性强，性能高的特点。常年为军队、公安、政府、党务等多种国家重要行业、团体提供网络数据加解密服务，最大限度的保护用户网络数据传输安全。

12 产品特点及优势

13

中小型企业及分支机构解决方案示意图

## 集成多种VPN接入技术，适应各种应用场景



网御新一代VPN产品综合了多种VPN接入技术，适应任意VPN接入应用场景。无论部署是VPDN、IPSEC VPN或者SSL VPN的单独部署，还是多种VPN同时使用的综合性VPN环境，网御新一代VPN都能稳定的满足。

## 多种移动设备接入技术

近年随着移动设备办公的迅猛发展，网御VPN产品也全面支持IOS及Android系统移动设备接入。支持接入方式包括移动设备自带VPN、远程应用发布、SDK封装APP三种方式。移动设备自带VPN功能为客户提供完全免安装的VPN接入解决方案；远程应用发布方式，为客户提供移动设备快速访问传统PC业务系统的解决方案；SDK封装方式，为用户提供独立APP无痕接入VPN解决方案。

## 二合一傻瓜式客户端，一站式接入技术

网御新一代VPN产品创造性的将不同类型VPN的客户端进行整合，一个客户端同时支持VPDN、IPSEC和SSL。在此基础上，客户端革命性的采用中心服务端主动推送配置的方式，实现VPN客户端的100 免配置使用。中心节点也采用简洁式配置设计，简单几步就快速可以完成传统客户端的复杂配置。

高校大数据化安全解决方案示意图

新一代VPN安全网关/SJW87及SJJ0805网络加密机

## 动态多点配置同步的灵活组网技术

网御新一代VPN产品支持动态多点VPN技术（DYNAMIC MUTLI-VPN ，缩写为DMVPN）。该技术主要用于复杂的IPSEC星形网络中。

在传统的星形拓扑中，每接入一个分支节点，都需要修改中心节点的配置，而DMVPN技术可以大量减少扩展节点的配置工作，每接入一个节点，只需要修改接入节点的配置，仅需对中心及新接入节点做简单配置，即可实现全网通讯。DMVPN技术，能够增加产品组网的灵活性，极大程度的降低网络拓扑更改的成本。

典型部署/应用

二合一VPN产品适用于任何IPSec或SSL独立部署及联合部署环境。下图为典型的IPSec结合SSL的三级VPN应用。分总部间使用网关到网关模式的IPSec VPN进行对接，解决公司间数据传输安全问题；出差人员使用SSL VPN 接入内网结合隧道接力技术实现对中心内网资源的访问。

网御星云

SJW87及SJJ0805网络加密机

产品简介

网御SJW87及SJJ0805网络密码机是国家密码管理局批准生产和销售的商用密码产品，可为各种规模的企业和政府机构提供相应的网络数据加解密服务。SJW87及SJJ0805网络密码机是集传输数据加密、防火墙等众多功能于一身的多功能安全保密网关。

网御SJW87及SJJ0805网络密码机采用专业设计的高可靠性硬件平台和创新的VSP通用安全平台，在保障产品自身安全性的同时，也使得产品网络处理能力比普通网络密码机高20％～30％。SJW87及SJJ0805网络密码机采用贴片式陶瓷电容和固态电容替代部分传统工艺上采用的电解电容，使得硬件平台的转换效率和耐高温能力得到提升，改善了产品硬件稳定性。

SSL隧道

14 内网 IPSec隧道

产品荣誉

### 网御星云具有国家密码局颁发的《商用密码产品定点生产单位》证书及《商用密码产品销售许可证》，同时密码机产品也具备《商用密码产品型号证书》，是具有密码机产品销售完整资质的厂商。

15

互联网

VPN网关

VPN网关

VPN网关

互联网

产品特点

## 符合2014年最新的国家规范及技术标准

### 根据我国密码管理政策的要求，国家密码在2014年7月管理局发布了《IPSec VPN技术规范》、《IPSec VPN 网关产品规范》、《SSL VPN技术规范》、《SSL VPN网关产品规范》以及《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》等一系列关于密码产品的规范。网御在第一时间进行响应，成为首家送测二合一VPN 加密机的厂商。2014年新规范较原有国密算法相比进行了较大的修改，提高了密码机产品在技术方面的安全性、规范性、兼容性，新标准在未来将成为国内网络密码机实现IPSec/SSL VPN必须遵循的标准。

## 遵循国家IPSec规范要求

SSL与IPSEC结合使用拓扑图

### 网御密码机产品严格遵从国家密码管理局最新发布的《IPSec VPN技术规范》及《IPSec VPN网关产品规范》， 使用硬件模块实现数据加解密、签名验证和随机数生成等功能。同时，密钥的协商和管理过程严格遵从规范要求， 具有更高的安全性。

## 遵循国家SSL VPN规范要求

### 网御密码机产品严格遵从国家密码管理局最新发布的《SSL VPN技术规范》及《SSL VPN网关产品规范》， 使用硬件模块实现数据加解密、签名验证和随机数生成等功能。同时，密钥的协商和管理过程严格遵从规范要求，具有更高的安全性。

SJW87及SJJ0805网络加密机/防病毒网关

## 高可靠性硬件架构

### 网御网络密码机是以专用硬件加密卡插卡形式对数据进行加/解密的特殊设计硬件设备，采用安全牢固的硬件架构，并在整机安全性设计方案上通过国家主管部门审查批准，能在同一硬件平台上实现对各种安全应用的支持，为网络信息提供安全保密服务，可防止来自内/外的安全威胁和攻击，硬件整体性能达到国内领先水平。

## 专用硬件加密卡

网御星云

产品简介

防病毒网关

### 在硬件加密卡上，网御网络密码机提供完善的密码卡自检功能，具有物理防撬措施，提供敏感数据自毁功能，在加密算法上，网络密码机完全支持国家密码管理局指定的商用密码算法，同时支持完善的密码算法保护体制，且密钥不以明文方式出现在密码卡之外的任何地方，还具有完善的密钥管理体制，保障用户数据传输中的高度机密性。

产品优势

## 支持最新的NAT穿越（NATT）协议

### NAT技术是目前国内企业共享上网、小区和智能大厦宽带接入、城域网宽带接入所使用的主流技术，所以在应用IPSec技术组建密码机网络时，一定要考虑选用的密码机是否具备“NAT穿越”功能。网御SJW87及

### 16 SJJ0805全系列密码机均支持最新的NATT协议标准，具有非常好的网络适应性。

## 完善的防火墙功能

### 网御SJW87及SJJ0805网络密码机中集成开发了功能强大的防火墙，并进行了友好易用的用户界面封装，提供专用防火墙产品绝大部分的功能，包括动态包过滤功能、双向NAT功能、MAC地址绑定功能、ARP代理功能、透明应用代理功能、抗攻击等功能。

网御星云早在2001年就开始研发网关防病毒技术，并于2004年取得了网络防病毒专利（专利号： 01109178.9）。新一代的网御防病毒安全网关基于独创的VSP(Versatile Security Platform)通用安全平台， 采用多核多线程并行运算技术、USE统一安全引擎技术、柱面神经元技术和内容加速技术，保证高速的病毒扫描处理能力。

产品荣誉

### 2004年取得了《网关级计算机网络病毒防范的方法》专利（专利号：01109178.9）

17

产品特点

1、采用自主创新设计的USE（Uniform Security Engine）统一安全架构，实现了多种安全功能独立安全策略的统一配置，可以方便用户构建可管理的等级化安全体系；

2、病毒防护引擎采用双引擎架构，扫描强度可控；

3、自有防病毒引擎，内置600万病毒库，20万Web2.0特征库，1300种应用识别特征库，综合应用特征控制力业界第一。可集成第三方知名防病毒引擎，且和自有防病毒引擎完美兼容。

## 提供丰富的冗余备份方案

### 网御SJW87及SJJ0805网络密码机提供两种冗余备份解决方案，为保证企业密码机网络的稳定性提供了强有力的工具，提供双机单线路主从备份、双机双线路镜像备份等方式。

产品优势

典型部署/应用

### 网御密码机产品为客户提供高效、安全、可靠的数据保护完整解决方案。

## 获得专利的病毒扫描技术

### 网御防病毒安全网关以独创的VSP通用安全平台为基础，结合了特征值检测和启发式检测，实时防御多种形式的病毒，可快速对文件进行重组和压缩文件解压还原，从而实现对2-7层全文内容过滤与病毒查杀，具有准确高效拦截网络病毒的能力。

# 网御防病毒网关

## 多样的病毒事件响应

### 基于不同需求，网御防病毒安全网关对病毒事件提供丰富的响应机制，包括病毒隔离、阻断、清除、记录日志，发送电子邮件报警等。其中，对病毒的隔离可以通过U盘导出隔离病毒后，进行分析生成特征库，通过网御的云防御技术从云服务器推送至网御防病毒安全网关。

## 360°网络病毒实时拦截

### 网御防病毒安全网关使用USE统一安全引擎，将多个安全功能有机地整合为一体，实现了状态检测、反病毒、反垃圾邮件、高层协议分析、深度内容检测等引擎并行处理。其防护能力大大超出传统防病毒网关产品。可以对网络病毒、蠕虫、混合攻击、端口扫描、垃圾邮件、网页钓鱼、间谍软件、P2P软件带宽滥用等各种广义病毒进行全面的拦截。同时，独创的VPN Defend技术，为用户VPN网络进行病毒攻击的防护。

校园网络解决方案示意图

## 政府电子政务接入解决方案

### 用户环境：华东某省电子政务内网，网络覆盖省政府，以及13个地级市、23个县级市、25个县的政府。 部署配置：A8340、A5320、A3330分级部署在省、市、县的三级政府网络互联出口上，开启病毒和网络攻

### 击的检测过滤，对整个网络进行区域防护。

### 应用效果：在分级部署了网御防病毒安全网关部署后，彻底解决了病毒通过业务网络传播的问题，极大的

### 18 降低了整个网络爆发病毒和网络攻击的风险。 19

典型部署/应用

## 校园网络解决方案

### 用户环境：西南某重点大学校园网络，2个WAN出口：教育网千兆出口和电信网络百兆出口，PC总计5000台以上，服务器区包括学校Web服务器、远程教育服务器、VOD课件服务器等。

### 部署配置：两台高端防病毒安全网关产品部署在学校网络出口，使用蠕虫控制功能限制内部异常流量，并开启防病毒功能保护内部客户端免受病毒侵害。同时开启双机热备模式，有效保证了网络的可靠性。另一台高端防病毒安全网关产品部署在服务器区，开启防病毒功能，主要用于过滤内网的病毒和外部网络攻击对服务器的侵害。

### 应用效果：在网御防病毒安全网关部署前内网终端因经常感染病毒和蠕虫，在部署网御防病毒安全网关后完全解决了这些问题。

政府电子政务接入解决方案示意图

# 入侵防护系统

网御星云

入侵防护系统

## Ipv6/v4双栈数据处理机制，更具适应性

### 网御入侵防护系统全面兼容IPv6/v4网络环境，基于IPv6/v4双网、双栈的数据处理机制，实现IPv6/v4网络接入、IPv6/v4网络攻击检测、IPv6/v4网络病毒检测、IPv6/v4网络带宽管理等核心防护功能。

产品简介

网御入侵防护系统基于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、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、抗拒绝服务、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。

产品特点

20 多维立体防御，全面高效

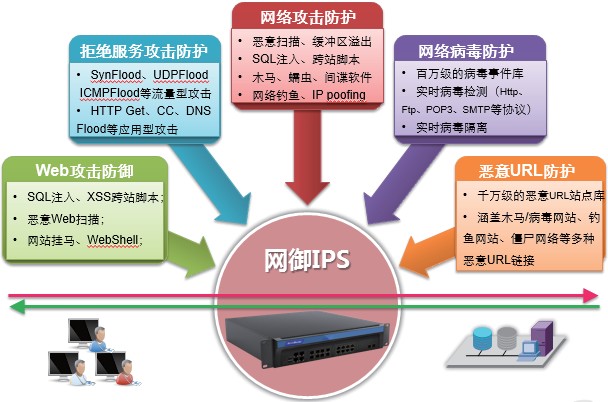
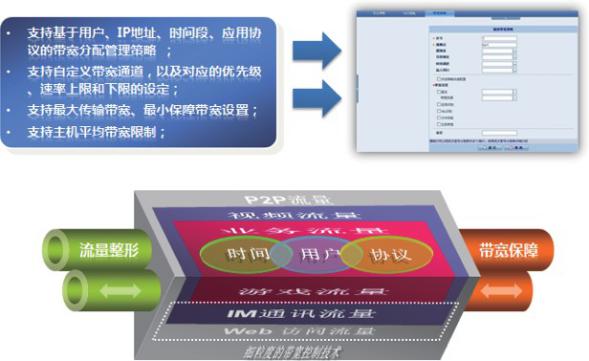
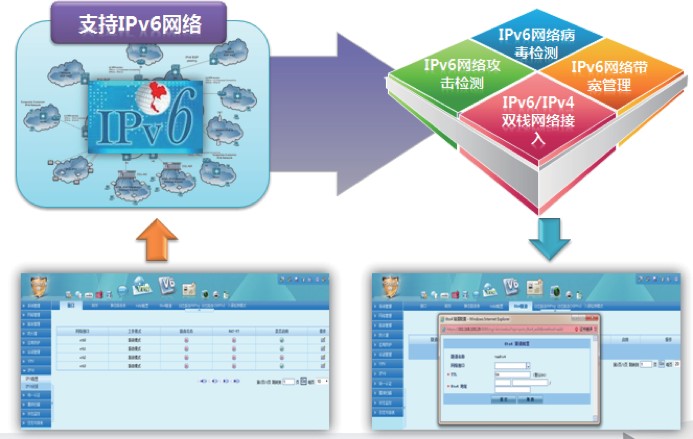
### 网御入侵防护系统具有网络攻击防护、Web攻击防护、拒绝服务攻击防护、网络病毒防护、恶意URL防护五大攻击防御体系，可构建多维立体防御解决方案，达到全面高效的防御效果。

IPv6/v4网络适应性示意图

## 上网行为管理与带宽管理，控管结合

21

### 网御入侵防护系统具有上网行为管理与带宽管理两大增值功能，上网行为管理模块内置支持52类、千万级URL分类库，可识别1300多种网络应用，带宽管理模块可细粒度管控IM、P2P、流媒体、在线游戏、股票、虚拟隧道等网络应用。通过管控结合的管理手段，可提升工作效率，降低安全威胁，同时可有效分配管理带宽，合理优化网络流量。



上网行为管理与带宽管理示意图

多维立体防御示意图

入侵防护系统/工业防火墙IFW－3000

典型部署/应用

## 方案一：全网安全防护解决方案

网御星云

工业防火墙IFW-3000

### 此方案中，网御IPS部署于边界防火墙之前，可解决以下两大安全问题：

### ◎抵御来自于外联网针对防火墙和内部网络的攻击。防火墙往往是攻击的重点对象，一旦防火墙遭到攻击，将会造成网络中断。网御IPS除了对各种暴力攻击能有效阻挡之外，基于对所有数据包进行详细的应用层分析，使黑客利用合法形式进行的非法存取攻击也无所

### 遁形。

### ◎实现局域网对外联网存取应用的有效管理。基于对软件行为的分析，网御IPS可识别IM/P2P/网游/炒股等各种网络应用，并制订各种管理策略，如特定访问对象限制、应用功能选择性禁止、网络带宽限制、流量传输总量限制等等。使企业实现网络弹性管理，从而提高员工工作效率和落实企业管理制度。

产品简介

Figure1IFW-3000-F302D Figure2IFW-3000-F201D

23

## 22 方案二：服务器区安全防护解决方案

### 此方案中，网御IPS部署于服务器安全区域边界，可解决以下两大安全问题：

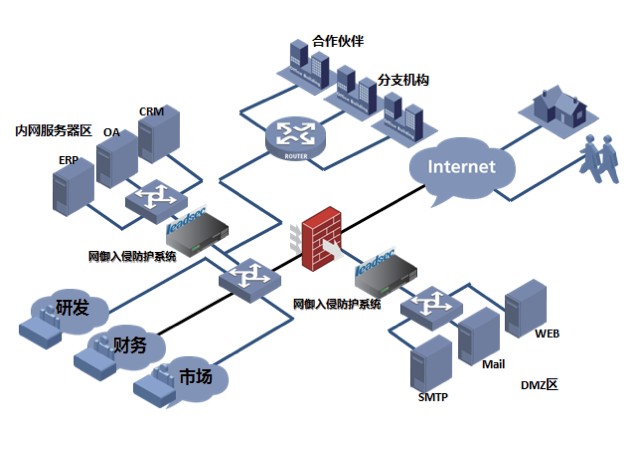
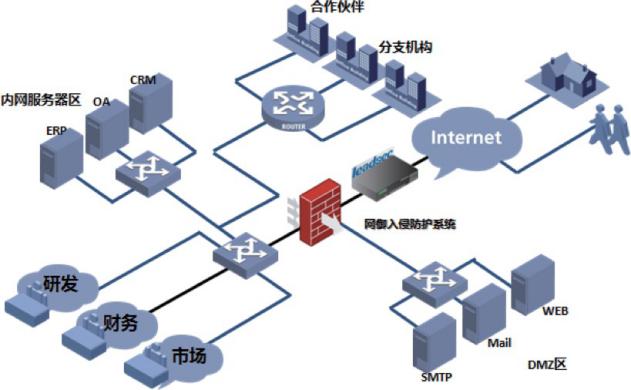
### ◎可抵御DoS/DDoS、蠕虫、端口扫描等针对服务器进行的攻击威胁，并可追踪管理Web服务器对数据库的存取行为，如可禁止外部SQL注入攻击。

### ◎重要服务器的操作系统或应用软件补丁更新之前，均需经历长时间严格的测试。在漏洞发现和修补的时间间隔内，服务器很容易遭受到黑客的攻击。网御对高风险漏洞做到了漏洞发现和攻击特征库发布时间的“零日”间隔，IPS可以实时拦截针对相应漏洞的攻击，为服务器提供“虚拟补丁”。

网御工业防火墙IFW-3000是一款专门为工业控制系统开发的网络安全产品，覆盖工业网络纵深防御的安全需求，可实现SCADA、DCS、PCS和PLC等工业控制系统的边界防护，被广泛的应用到核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关领域的工业控制系统。

产品荣誉

Figure 3 IFW-3000-F1100R



网御工业防火墙IFW-3000经过发改委组织的专家答辩、评审及严格的产品评测，荣获专项支持，正式列入发改委2013年国家信息安全专项名单。

产品特点

## 匠心打造，军工品质，产品适用于工业严苛复杂的生产环境。

◎导轨式和机架式：机架式可以部署在生产车间的机房中；导轨式设备可以直接部署到环境严苛的生产现场。

◎气候保护要求：产品具备超强的耐寒暑环境适应能力。导轨式设备工作温度支持-40~70℃，存储温度支持-40-85℃，湿度支持5％-95％，无凝结。

◎侵入保护要求：产品全金属外壳，无风扇设计，导轨式设备符合IP40的防护等级，可有效的防护直径>1mm 异物进入，完全适应尘土飞扬的工业环境。

◎高可靠性：产品支持冗余电源、ByPass和双机热备。

工业防火墙IFW－3000

## 工业协议深度解析引擎，支持主流工业协议。

## 先控站与工程师站隔离

◎OPC协议：支持OPC DA、HAD、A&E、DX协议的动态端口防护，可实现动态识别跟踪、完整性检查、碎片管理。

◎Modbus/TCP：可实现Modbus/TCP协议应用层深度解析防护，包括功能码、寄存器范围等字段过滤；同时支持基于阻断时的Reset回复、异常回复、合规性检查等。

◎Modbus/RTU：可实现Modbus/RTU应用层深度解析防护。

◎IEC104：可实现IEC104协议应用层深度解析防护，支持对遥控、遥调、遥脉等命令的访问控制。

### 只允许先控站与OPC Server之间通信或工程师站与生产设备通信，避免U盘摆渡等入侵方式。

## 支持网关间基于工业协议的VPN数据加密传输，保证数据安全。

## 国内首款支持串行链路通信防护安全产品：

同时具备以太网口和串行链路通信接口，用以满足不同的生产环境。以太网口支持设备部署在工业以太网的环境中。串行链路通信接口支持设备部署在RS232\485标准的基于串行通信链路生产线上。

## 基于自然语言规则的可扩展安全匹配引擎：

安全能力取决于使用它的人，思维有多深，防护能力就有多强。

## 关键PLC防护

Figure 5 先控站与工程师站隔离

24

产品优势

### 对关键PLC进行隔离防护，对工业协议如Modbus/TCP、IEC104协议进行指令级过滤，避免非法指令下发， 提供工业网络的核心生产的安全。

已经包含在产品特点中。

25

典型部署/应用

## 数控隔离

### 通过对OPC协议的深度防护，避免数采和控制网之间的病毒感染。可广泛的应用在各个工业领域。

Figure 6 关键PLC防护

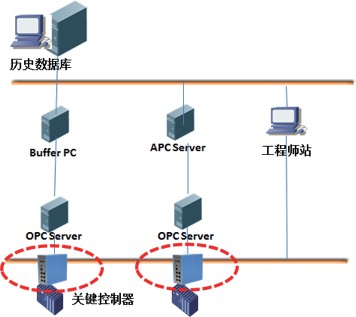
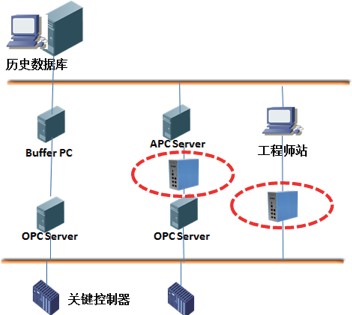
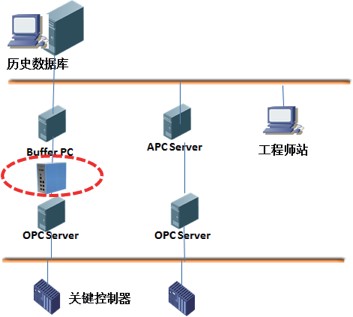


Figure 4 数控隔离

# Web应用安全防护系统

网御星云

Web应用安全防护系统

## Web的虚拟服务

产品简介

网御Web应用安全防护系统（以下简称：网御WAF），是网御星云公司所研制开发的基于Web安全防护与应 用交付类应用层安全产品。产品主要针对Web服务器进行HTTP/HTTPS协议分析，防护以各类Web应用漏洞为目标的网络攻击行为，并针对Web应用访问行为进行全方位的合规管控及优化，从而提高Web应用的安全性、合规性

及可用性，确保各类Web业务应用能够安全、可靠、快速地交付。 通过部署一台网御WAF管理多个独立的Web应用，各Web应用可采用不同的安全策略，可以在不修改用户网络架构的情况下增加新的应用，为多元化的Web业务运营机构提供显著的运营优势与便利条件，可以实时配置

产品特点

26 Web应用防护

修改多个后台Web系统，而无需让Web系统下线。

应用层DOS防护 27

网御WAF能够精确识别并防护常见的Web攻击：

◎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。

网御WAF可防护带宽及资源耗尽型拒绝服务攻击，如对SYN FLOOD等常见攻击行为进行有效识别。

Web应用安全防护系统/安全隔离与信息交换系统

典型部署/应用

## 透明模式

网御星云

安全隔离与信息交换系统

产品简介

网御WAF透明模式部署模式

◎以透明模式接入，无需调整和更改用户网络的拓扑结构，无需更改用户原有网络配置，实现对Web服务器的保护。

◎透明模式是部署最为简便的方式。透明模式下，网御WAF可实时阻断第7层的Web攻击，让其它的流量通过。

28

## 代理模式

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、低嗓低耗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。

29

网御现已成为国内安全隔离网闸业内技术最优、产品线最全、市场占有率最高的领导厂商，已为政府、金融、交通、能源、教育等各大行业提供了许多成熟的安全隔离解决方案。

产品荣誉

◎ 2012-2015连续四年荣获Frost&Sullivan市场领导奖；

◎ Frost&Sullivan报告：连续四年市场占有率第一；

◎ 中国自主创新产品；

◎ 荣获2012年中国质量评价协会科技创新奖。

产品特点

网御WAF代理模式部署模式

◎在代理部署模式下，对访问用户能够完全隐藏Web服务器的真实IP地址，有效保障Web服务器安全。

## 业内领先的安全模型

◎独创闭环“安全链”模型，将隔离、应用数据白名单、内容过滤、审计融为一体，模拟高级别政府部门“门岗管理制度”，防范未知安全风险；

◎基于“GPIC”自主芯片的“2+1”硬件架构，彻底阻断内网间的TCP/IP通信，安全隔离内外网；

◎基于自主化“VSP”安全系统，从系统层、网络层、应用进行安全加固，并经业内领先的ADLabe实验室检测， 自身安全性达到最高级别。

安全隔离与信息交换系统/安全隔离与信息单向导入系统

## 全新光隔离交换模块，高达万兆线速性能

基于光传输介质，采用双路电子开关设计，在保证内外网任何时刻处于“物理断开”的同时，最高性能可达万兆线速。

## 广泛的业务适用性

网御星云

安全隔离与信息单向导入系统

具有数据库同步、文件同步、视频传输、消息传输、应用代理等10多个成熟模块，满足用户通用需求，并对多个行业深入研究，提供用户专业化定制需求。

## 业内领先高可靠性

采用军品级硬件平台，基于MRP（Multi-Layers Redundant Protocol）多重冗余协议实现多重冗余方案，支持自身端口冗余、双机热备、多台安全隔离网闸负载均衡，保障用户网络和应用的高可靠运行。

产品优势

◎ 中国网闸第一品牌；

◎ 业务领先的万兆线速性能；

30

◎ 产品易维护和高可靠性；

◎ 产品资质全级别高。

典型部署/应用

产品简介

为保证数据安全，高密级网络与低密级网络之间，往往要求数据仅且只能由低密级网络流向高密级网络。为解决高密级网络通过连接环境泄密问题，网御推出安全隔离与信息单向导入系统产品， 在提供物理绝对单向无反馈传输环境同时，采用“多级前向纠错编码”专利技术，保证数据传输的高可靠、高效率。

网御安全隔离与信息单向导入系统由于其物理单向无反馈传输环境、基于数据的单向导入，使黑客无法通过该套系统进行入侵和探测，同时行为得不到任何信息反馈，在为用户提供绝对单向无反馈传输功能的同时， 为用户提供最高级别的网络攻击安全防护解决方案。

31

网御安全隔离与信息单向导入系统特别适合下述应用场景：

◎ 非涉密网络到涉密网络的数据传输；

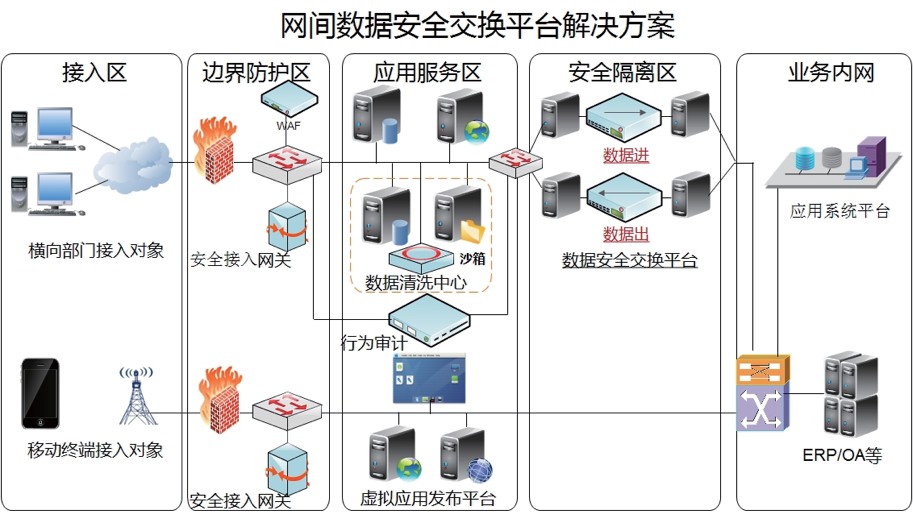
◎ 低密级网络（安全域）向高密级网络（安全域）的数据传输。

产品荣誉

◎ 荣获公安部网络单向导入产品《计算机信息系统安全专用产品销售许可证》三级

◎《军用信息安全产品认证证书》

◎ 具有“一种在单向网络中传输数据的方法及装置”发明专利



产品特点

## 基于光传输技术绝对单向无反馈设计，单向传输可见、可验证

网御安全隔离与信息单向导入系统采用“2+1”架构设计，即外网主机、内网主机和单向导入隔离部件， 内外主机通过单向导入隔离部件连接。

其中单向导入隔离部件采用独特单向无反馈电路设计，并采用单根光纤通信，外网端仅且只能发送数据， 内网端仅且只能接收数据，网御的硬件设计从物理上保证了数据的绝对单向无反馈传输，且单向传输环境可见可验证。

安全隔离域与信息单向导入系统/上网行为管理系统

## 高可靠多级前向纠错编解码解决方案

数据传输的可靠性直接决定了单向导入系统在实际环境中的可用性，网御安全隔离与信息单向导入系统采用拥有专利技术的多级前向纠错编码、解码技术，通过外编码解决内编码未能纠错的数据，增强了数据传输端到端的重构能力，提高了单向无反馈环境数据传输的可靠性。

网御星云

上网行为管理系统

## 智能流控及数据完整性自动校验技术

在无反馈环境下接收端状态无法反馈给发送端，为了平衡接收端与发送端的数据发送、接收速度，网御开发独特的调速功能，快速平衡发送、接收速度。

由于单向导入系统理论上的不可靠，为了让用户第一时间了解数据接收状态，网御在接收端自动校验数据，实时报告正常和未正常接收数据状态信息。

## 全面的数据安全控制

以 USE（Uniform Security Engine）统一安全引擎为基础，对单向传输的内容进行全文数据还原，对数据内容实施全文深度检测，并采用自主知识产权病毒引擎、专业病毒特征库进行病毒查杀，为单向数据传输提供了“绿色通道”。

32 典型部署/应用

产品简介

网御上网行为管理系统可协助用户实现对互联网访问行为的全面管理。包括流量管理、网页分类过滤、网络应用封堵、内容监控审计、企业级路由等功能。能够满足企事业单位、政府机关、金融电信、石油能源、学校教育行业等各种Internet互联网使用单位的网络行为监控需求。

产品核心价值

33

## 智能流量管理 防止带宽资源滥用

对OA、ERP、视频会议、邮件等办公应用进行带宽保障；对在线视频、迅雷等与工作无关的软件进行带宽 限制；同时单独保证重要人员的网络速度，防止网络带宽拥堵，提升网络使用体验。

## 掌控网络行为 提高员工工作效率

提供员工详细的网络使用记录，例如网页浏览、在线影视、迅雷下载、炒股、网络游戏、偷菜等；并根据企业要求，对工作无关的应用进行封堵，规范员工上网行为，提高工作效率。

## 过滤外发信息 降低机密泄漏风险

对微博、邮件、QQ、BBS发帖等外发信息进行过滤，帮助企业过滤敏感的内容，防止企业内部机密外泄， 保护企业信息资产安全。

## 超大存储空间 90天记录规避法律风险

超大容量存储空间，全面保存员工上网信息，提供QQ、MSN、飞信等聊天工具的聊天内容，做到有据可查，避免企业承担不必要的法律风险。

上网行为管理系统

## 网络统计报表

## 方便企业管理

典型部署/应用

提供了丰富的网络可视化报表，能够让您清晰掌握互联网的使用情况，以便找到造成网络瓶颈的原因所在，为网络优化提供依据，便于您更好的管理网络。

## 路由模式

产品特点

## 统一安全引擎（USE：Uniform Secure Engine）

网御上网行为管理系统工作在路由模式时可开启设备的全部功能，包括路由（NAT）、流量控制、应用阻断、内容过滤和审计等，并可取代传统路由器或防火墙作为出口网关，节省网络总体投资。

网御上网行为管理系统采用高效的统一防御引擎USE。它将应用协议分析、行为管理、应用过滤等多个子系统集成于单一平台，构造统一架构，综合并优化各子系统，去除冗余，简化数据处理流程，实现统一的安全引擎处理机制。

路由模式部署示意图

## 专家会诊系统（Expert Consultation System）

数据通讯平台采用了专家会诊系统，对多个安全处理单元一次并行处理，可以使得数据包分析处理时间大幅度缩减。

## 34 DPI与DFI相结合的数据分析技术

以DPI( Deep Packet Inspect，深度包检测)和DFI( Deep/Dynamic Flow Inspection，深度流行为检测)技术为核心，结合带宽自动分配算法、令牌桶算法、随机公平队列等技术，对网络应用进行深入检测和识别，能够全面识别和控制包括P2P、VoIP、视频/流媒体、HTTP、网络游戏、数据库及中间件等在内的多种应用，以及各种使用动态端口、仿冒端口及经加密或代理（支持Http及Sockes代理）后的网络应用及协议。

## 桥接模式

网御上网行为管理系统工作在桥接模式时，无需改变用户的网络拓扑结构。桥接模式下设备不具备NAT功能，可对网络应用进行控制、对流量进行管理、对内容进行过滤和审计等。

35

桥接模式部署示意图

## 零拷贝技术（ZERO-COPY技术）

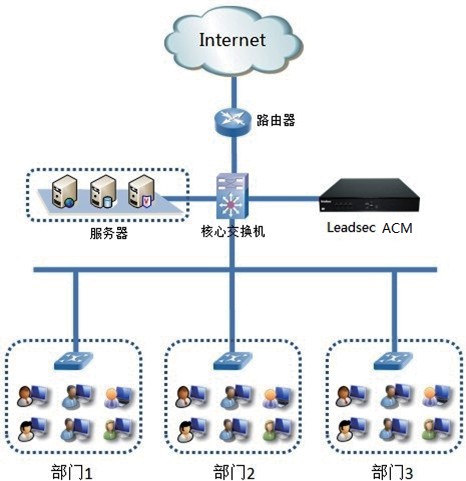
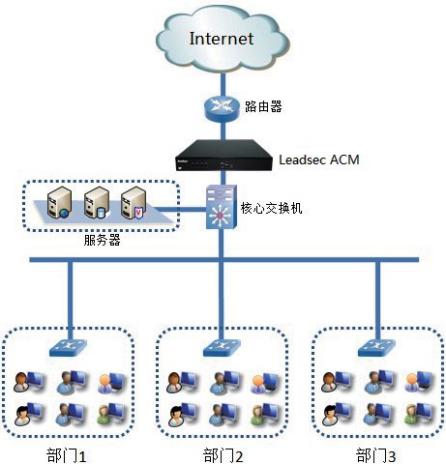
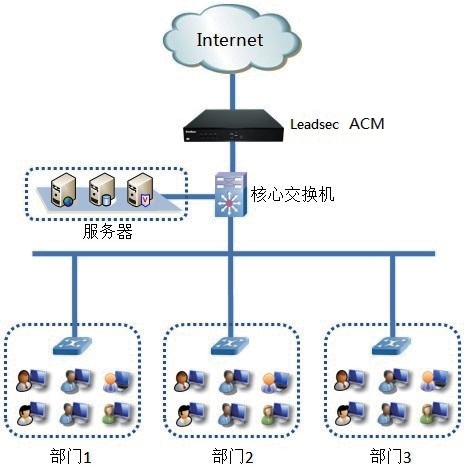
利用DMA技术将网络数据报直接传递到系统内核预先分配的地址空间，避免CPU参与，将系统内核中存储数据报的内存区域映射到检测程序的应用程序空间，检测程序直接对这块内存进行访问，从而减少系统调用的开销，减少数据复制过程，降低CPU负载，提高系统效率。

## 分布式集中管理体系结构

网御星云提供智能安全集中管理平台，满足用户对网御上网行为管理系统设备分布部署、统一集中管理的需求。集中管理平台支持业界标准的SNMP v1/v2c/v3协议，并具备独到技术提供NAT穿越能力，提供对网御上网行为管理系统的单独或批量远程升级、配置策略下发及数据导入导出等操作。同时可自动记录设备运行日志及网管操作日志，便于问题定位及处理，极大地降低运维成本。

## 旁路模式

网御上网行为管理系统支持旁路方式部署在网络核心交换机上，通过交换机端口镜像功能，对用户的上网行为进行实时检测。旁路模式下支持上网行为审计功能，但不具备上网行为控制和过滤功能。



旁路模式部署示意图

# TAM异常流量清洗系统TAM－Guard

网御星云

产品简介

TAM异常流量清洗系统TAM-Guard

## 快速高效的异常流量过滤器

网御Guard通过独创的智能防护算法，对攻击行为进行分析和学习，可有效区分攻击流量和正常流量，防护SYN flood、UDP flood、ICMP flood、DNS flood等二十多种攻击，保证正常流量不受影响。网御Guard异常流量过滤器采用了以下几种技术：

◎特征识别：网御攻防实验室长期积累攻击和攻击工具的特征，形成攻击特征库，可直接过滤网络上流行

的多种攻击。

◎身份鉴别：在通信过程中，加入验证的过程，验证源地址和连接的有效性，防止伪造源地址和连接的攻击，并支持黑白名单。

◎动态过滤：支持简单包过滤、状态包过滤和动态包过滤，可以根据源地址、目的地址、源端口、目的端口、协议进行访问控制，禁止不必要的访问。

◎智能防护：网御独创的智能防护算法，区别于传统的统计丢包算法，通过对一段时间内的通信进行分析，以及对多个上下文数据包的分析，区分正常流量和攻击流量，然后过滤绝大部分的攻击流量，正常流量不

网御星云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（Detector）、异常流量清洗（Guard）和流量清洗管理中心（Manager）三个组件。其中，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对多台Guard进行统一管 理。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做出动作响应，从而快速消除异常流量造成的危害。

36 产品荣誉

◎ 异常流量管理系统——软件著作权证书

◎ 网御异常流量管理系统（万兆）V3.0-EAL3证书

◎ TAM网御异常流量管理系统V3.0（千兆）——销售许可证（基本级）

◎ TAM网御异常流量管理系统（万兆）V3.0流量清洗产品（合格品）销售许可证

产品特点

## 防范攻击多

可防御二十多种DoS/DDoS攻击，除可防范SYN Flood、UDP Flood、ICMP Flood和Stream Flood等流量型DDoS攻击外，还可有效防范HTTP Get Flood攻击、DNS Query Flood攻击、CC攻击、数据库连接耗尽等应用型Flood攻击，可针对未知类型攻击进行自定义防护。

## 多机集群部署

受影响。对UDP flood和ICMP flood有较好的防护效果，如可有效防护针对聊天服务器和视频的UDP flood攻击。

◎协议分析：检查通信过程是否符合TCP/IP协议的完整性。并对HTTP、DNS等应用层协议进行深度分析， 支持对SYN/SYN ACK/ACK flood攻击、HTTP get flood攻击、DNS query flood攻击、CC攻击的防护。

◎连接限制：支持对IP/子网的并发连接和新建连接限制，可根据源地址、目的地址、源端口、目的端口、协议限制并发连接总数和新建连接速率限制，从连接数的角度对网络资源进行合理配置，可防止大规模攻击的发生，并支持防扫描功能：TCP端口扫描、UDP端口扫描和ping sweep等。

37

产品优势

## 产品安全性

系统可通过局域网连接，客户可配置私网IP对设备进行管理，完全的网络隔离提供了强大的安全保障。在配置广域网IP后，系统须使用专用登陆器远程控制，所有网络传输数据均使用加密报文，任何数据被截取均无法破译。同时，系统具备日志功能，对所有登录操作均保存存档。

## 产品灵活性

系统支持旁路挂载模式，不需要对其它网络设备进行新的配置，在加入和撤离网络时不改变网络的拓扑结构。

## 产品可扩展性

TAM-Guard默认开启等同模式，完美且友善的接口可以在设备支持的前提下轻松扩展群集。



网御异常流量管理系统TAM多机集群解决方案，具有配置简便、可扩展性强的特点。方案支持2～64台设备的多机集群，支持集群设备间的状态同步，通过独创的二级负载分担技术，可以满足运营商骨干网处理海量攻击流量的需求。

TAM异常流量清洗系统TAM－Guard /TAM异常流量管理系统TAM－Detector

## 应用层防护能力

TAM-Guard具备专用于WEB服务器和DNS服务器防护的抗攻击功能，内置的各种专门的防护插件提供了诸如：高速缓存、宕机保护、防CC攻击等专属功能，彻底解决针对此类应用的攻击行为。

## 灵活的部署模式 全面支持各种组网需求

网御星云

TAM异常流量管理系统TAM-Detector

TAM-Guard支持串联部署和旁路部署模式。旁路部署中有多种流量牵引和回注方式，可以充分满足各种网 络结构下的部署要求，例如：支持BGP牵引、OSPF牵引、策略路由回注、二层回注功能等，为客户提供足够的 部署选择方案，实现产品部署无障碍。

典型部署/应用

产品简介

面对网络流量的复杂性给网络运营维护带来的巨大挑战，异常流量检测系统（TAM-Detector）可以帮助用户解决流量可视化、回溯分析、异常流量检测与响应联动等问题，系统采用DFI技术，通过基于动态基线的行为建模，检测网络中的已知和未知异常，如DDoS、蠕虫病毒等攻击行为。

产品特点

## 异常检测

产品采用基于行为建模的基线技术和特征检测技术相结合的方式，发现流量的异常，如DDos攻击、蠕虫事

38 件、流量超常、协议比例异常、流量分布异常、网络滥用、DNS攻击等异常。 39

## 流量分析

产品可以通过对网络流量的精细化统计分析，让网络流量可度量、可评估。利用测量的结果，可以应用于网络优化、网络规划、网络异常监控、广域网流量监控、流量计费等。包括基于区域的流量分析、基于时序流量分析、基于技术特征流量分析等。

## 设备检测

产品基于网络拓扑对路由设备和服务器设备的网络分布、流量详情、设备状态等进行可视化展现。通过设备监控用户可以直观的了解整个网络和各个设备的流量和运行情况。

## 路由分析

产品可以通过分析路由消息和路由表信息，得到关于路由稳定性和合理性的结论。包括路由前缀数目分析、路由稳定性分析、路由数目分析、BGP包分析、路由震荡分析等。

产品优势

## 独创加强型vFlow技术

在旁路镜像获取到网络数据包后，对数据包内容进行基于扩展NetFlow的流量分析技术的处理，转换成网 御星云独有的vFlow。对于基本参数字段采用了标准NETFLOWV5的统计字段；对于TCP层和应用层的扩展参数， 则扩展插件框架，来支持了更多的应用协议识别。

TAM异常流量管理系统TAM－Detector/应用交付控制系统Leadsec-ADC

## 探针式流量检测

采用网络探针的部署方式，通过收集Netflow流量信息，并结合SNMP、镜像流分析等方式，既不会影响用 户原有的网络拓扑，又能够靠近发生异常流量的网络节点，同时具有检测延迟小，检测精确高的特点。

## 多层次应用防护

网御星云

应用交付控制系统Leadsec-ADC

应用层DDoS攻击正在成为攻击的主流，尤其是HTTP攻击、DNS攻击和VOIP攻击，产品能够针对主流应用层DDoS攻击进行有效检测。

## 动态的分析呈现

系统能够通过对一个时间窗内历史数据的自动学习，获取包括总体网络流量水平、流量波动、流量跳变等在内的多种网络流量测度，并自动建立当前流量的置信度区间作为流量异常监测的基础。在此基础之上，可以将监控节点的流量分布、异常攻击、Top地址、Top协议、安全总体态势等信息动态、实时得显示给管理员，帮助管理员准确掌握所管辖网络的安全态势。

典型部署/应用

40 产品采用旁路的部署方式，只相当于增加一个网络节点。产品的部署，不改变用户的拓扑结构。支持光纤接入方式。

产品简介

网御星云应用交付系统产品具备安全，高性能，稳定，功能领先，配置灵活，部署简单的特点，产品型号覆盖全应用场景，最高性能可达600G，支持IP6-IPv4网络混合部署，具备完善的虚拟化云计算中心流量管理解决方案，完全可以满足从中小企业业务系统，到运营商网络及新型数据中心的部署需要，实现关键业务的快速，安全， 可靠的交付需求。

产品荣誉 41

◎ 网御星云应用交付控制系统覆盖行业包括国家级部委、省级政府单位、金融数据中心、运营商、电力、高校、公安、能源、税务等众多行业，各种案例超过300个。

◎ 网御星云应用交付系统全系列产品均通过IPv6 Ready认证。

flow

产品特点

## 软件弹性扩展

**!**

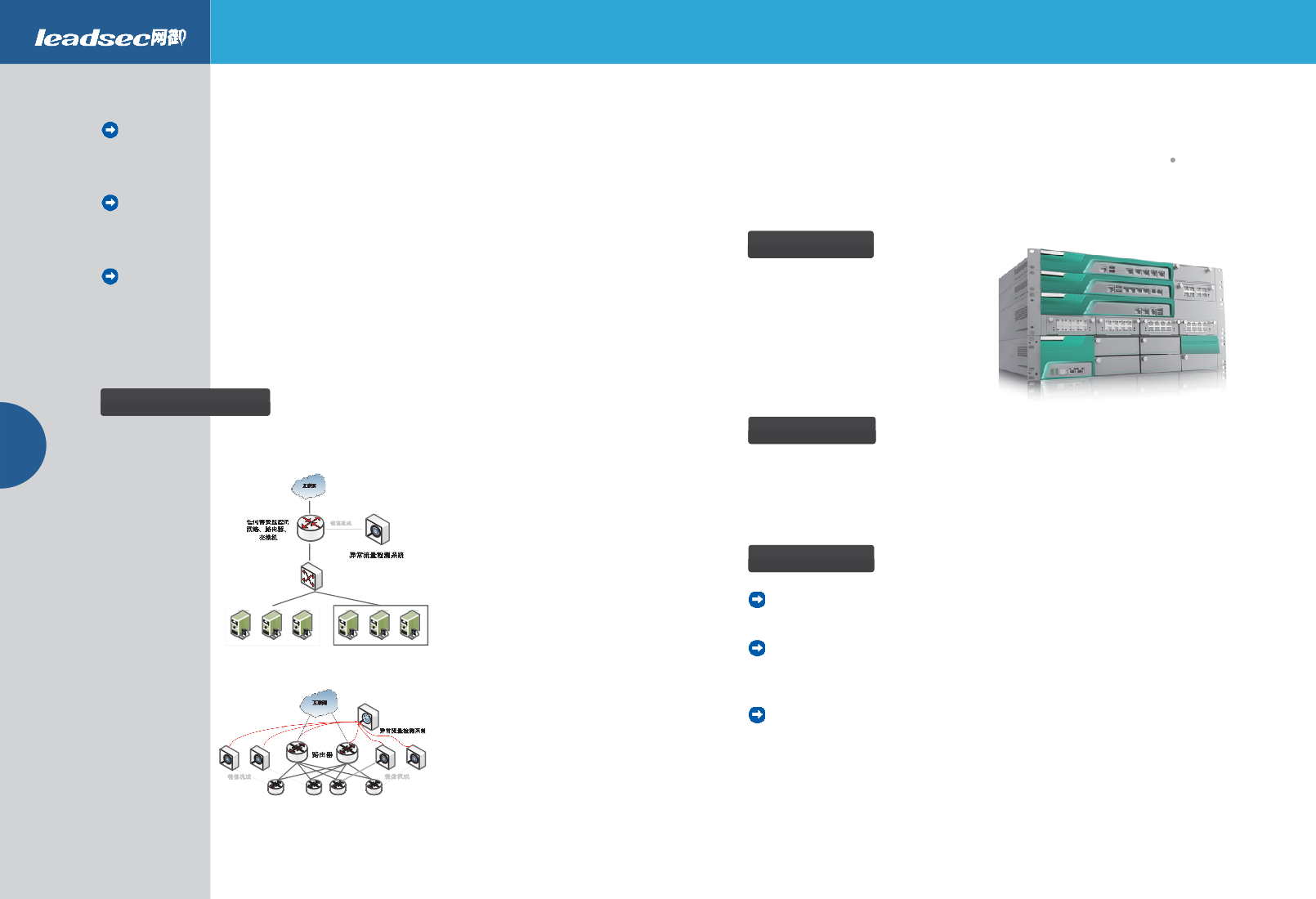
全系列产品均支持按需负载，根据用户实际需求弹性扩展性能，节省采购成本。

同时产品也支持级联部署。

## 硬件弹性扩展

全系列产品均支持接口扩展，包括千兆电口、千兆光口、万兆接口等，根据用户实际环境灵活配置。且全系列都支持SSL加速卡扩展。

## 应用路由



内置应用协议检测引擎，根据协议类型、特性等把相关应用引导至指定的链路出口。

flow flow

应用交付控制系统Leadsec-ADC/入侵检测系统

## 灵活部署

支持HA部署，最高支持32台设备集群，支持IPv4-IPv6的混合部署。

网御星云

入侵检测系统

产品优势

## 高性能

最高可提供600G的数据处理能力，全系支持虚拟化，满足大型云数据中心需求。

## 功能全面

支持服务器负载、链路负载、全局负载、应用优化、应用加速、应用防护等功能。

## 安全防护

支持4~7层防火墙功能，并具备抗DDOS攻击、抗CC攻击、防敏感信息泄露等应用级安全防护。

42 典型部署/应用

政府云数据中心方案：

产品定位

网御入侵检测系统V3.2，即IDS，是国内领先的入侵检测与管理系统。其主要作用是帮助用户量化和定位 来自内外网络的威胁，为用户提供有效的指导处置措施，为用户的网络安全建设提供决策依据的网络安全产品。

网御入侵检测系统融合多种检测方法，搭载经高性能优化的硬件平台，根据用户需求定制策略，准确分析网络中各种异常事件和攻击行为，通过实时报警和多格式用户报告，为用户提供翔实、准确、可操作的安全建议。产品坚持以“全面检测、有效呈现”的核心设计理念，帮助用户对网络安全整体水平进行效果评估。

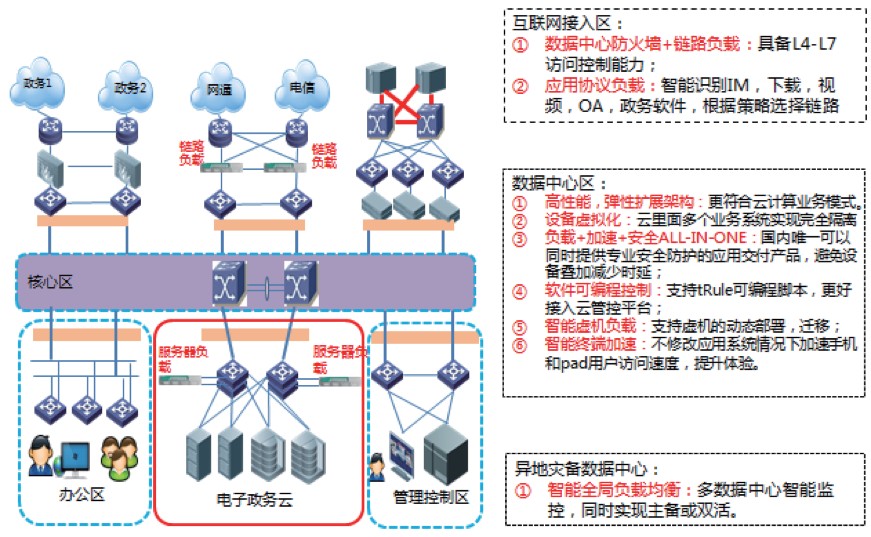
网御IDS系列中的NGIDS系列型号，该系列是在一台检测设备上，实现了网络层的已知威胁入侵检测和未知高级持续性威胁检测（即APT检测）的所有功能，降低用户采购成本、节省用户部署空间，目前属于国内厂商独家具备的产品形态。

产品技术

43

作为新一代智能入侵检测产品，系统的软件架构覆盖了网络已知威胁和未知威胁两大检测技术领域，功能涵盖全面。从已知威胁的检测、发现、预警、报告、展现五个维度进行威胁闭环管理，到动态检测和静态检测结合的未知威胁的全面检测，产品帮助用户全面实现网络威胁精确检测，尤其对网络协议攻击、手机病毒攻击、未知恶意代码威胁、未知漏洞利用攻击、嵌套式攻击、木马蠕虫病毒攻击、外联隐蔽信道等网络威胁。

作为国内自主品牌的入侵检测产品，产品运用了大量创新技术，譬如，采用关注度算法，快速过滤掉海量的低质量报警事件；采用智能调度算法，提升对恶意文件的并行虚拟执行效率；采用资产关联算法，使系统展示出来的事件数量大幅减少；用代码优化技术，提升检测处理性能等等，旨在帮助用户，快速定位网络威胁、聚焦重点事件、降低安全管理难度。



产品亮点

## 全面检测

◎全面检测范围：提供网络入侵事件、网络违规事件、流量异常事件等多种异常检测，具有独立的AV引擎，还具备各种未知威胁检测能力。

◎全面检测机制：支持基于特征和基于行为的两种检测方式，同时融合静态检测和动态检测机制，扩大深度检测范围，实现已知与未知威胁全面检测。

◎全面协议分析：支持协议自识别与协议插件技术，可准确识别非常规端口的协议和新型协议。

◎全面事件分析：提供业界最规范的后继服务支撑体系，确保对新型事件的快速准确响应。

◎全面信息收集：支持多级、分布式部署，实现策略统一下发，信息集中收集。

◎全面检测性能：采用最短时间优先算法，确保了产品在网络数据高负载情况下的检测效率，可满足百兆、千兆、万兆网络环境下的安全检测要求。

入侵检测系统/网络审计系统（互联网审计型）

## 有效呈现

◎精确报警信息：结合环境指纹技术，在发现有攻击行为后，与存储的环境信息进行二次匹配，将那些能够确信为“有用”的报警信息单独呈现，减少用户的分析操作消耗。

◎详尽信息呈现：报警信息除事件的双方地址、协议等信息外，还包括了对事件的具体描述、漏洞信息、修补建议、影响系统等，可以将最细致的事件信息呈现给用户。

◎威胁地址定位：提供与实际地理拓扑相结合的报警显示方式。在大规模部署的情况下，可以将设备拓扑与地理拓扑相结合，使得管理员可以直观而迅速的判断威胁所在。

◎丰富报表展现：提供基于时间、地址、事件等多重参数信息的分析报表，结合历史分析数据，可清晰展现安全建设发展趋势，协助考量网络安全建设水平。

◎威胁细节报告：提供包括漏洞利用分析、行为分析、代码地址、虚拟环境等细节的威胁检测报告，标识威胁级别和威胁信息。

型号配置

网御星云

网络审计系统（互联网审计型）

产品简介

网御网络审计系统(互联网审计型)，能够通过先进的实名上网等技术手段对上网人员进行行为监控和内容合规细粒度审计；能有效监管上网人员利用工作时间娱乐、购物、聊天、进行P2P下载、在线游戏等无序上网行为。在加强机构内外部网络信息控制监管的同时，产品可为避免相关信息外泄及事后的追溯取证提供保障。

产品名称

N系列

44 TD3000-FS系列

TD3000-GS系列TD3000-NGIDS系列TD3000-TS系列

说明

经过裁剪的入侵检测产品，满足用户最基本需求

百兆系列，共分5个子型号，可满足200Mbps到600Mbps网络流量环境的检测需求 千兆系列，共分10个子型号，可满足800Mbps到5.5Gbps网络流量环境的检测需求

具备未知威胁扩展能力的下一代入侵检测，7个扩展插槽，监听接口灵活配置。该系列最大特点 是，在一台设备上，实现了已知威胁检测和未知威胁检测的功能，节省空间节约成本

准万兆、超万兆系列，8插槽，满足20Gbps网络流量环境的检测需求

产品特点

## 实名制上网

45

◎应用独特的三层交换环境下的MAC地址探测技术，即使是在三层交换网络环境中也能够准确获取终端用户的真实MAC地址；

◎通过IP+MAC地址绑定认证、本地Web认证、AD域认证、LDAP认证、USB KEY身份认证、刷卡认证和白名单免监控管理等多种对象识别技术，可以实现对组织机构内部数量庞大的用户身份精准识别。



## 广泛支持各种网络应用

网御网络审计系统支持全面的行为审计、内容审计及行为控制功能，同时支持数据库审计、运维操作审计功能，广泛支持目前常见的各种网络应用：

◎对于常用的HTTP协议，除支持网页浏览（HTTP GET）审计外还全面支持各种网页提交（HTTP POST）类应

用的审计，其中POST应用可细分为WEBMAIL、WEBBBS、WEBCHAT（聊天）、WEB登录等上网行为，对基于HTTPS加密协议的网页浏览行为也将记录除域名地址之外的所有关键数据；

◎除常用的网页浏览和电子邮件应用外全面支持当前常见网络应用的审计包括：文件传输、即时通讯、P2P 下载、流媒体、在线游戏、财经证券等应用；

◎在旁路部署模式下可实现较强的网络行为控制功能，包括对网页浏览、电子邮件服务器、即时通讯、P2P 下载、流媒体、在线游戏等应用的控制。

## 灵活的黑白名单功能

为了使审计策略更加灵活、精准，网御网络审计系统采用了黑白名单的机制，大大降低了审计策略的复杂程度，同时也减轻了管理人员的工作量。

网络审计系统（互联网审计型）

## 丰富直观的报表

系统根据历史审计日志数据进行统计，可产生丰富详细和直观的报表，包括分组上网排名、人员上网排名、网络应用统计、访问资源统计、趋势分析、自定义报表等。能够从上网对象、时间、分类、目标等多个维度对网络活动进行查询分析，并以柱状图、饼图、曲线图、折线图等形式来体现排名、结构、趋势等上网概况，使管理者对所掌握的数据有清晰直观的认识。报表可以以EXCEL、PDF、WORD、HTML等形式导出保存，并支持自定义的周期性报表自动生成和订阅。

## 常规部署

Internet

!

## 46 先进的多路捕包技术，四路同时捕包

网御网络审计系统采用业界领先的多路并行捕包技术，单台设备最多支持高达4路数据的并行捕获与分析，为在复杂环境下的灵活部署，提供先进的技术保障，也提高了审计数据的准确度。

47

## 多级部署

## IPv6协议支持

网御网络审计系统在国内率先实现了对IPV6的支持，并同时能够兼容IPV4，为目前已经应用IPV6的单位和即将应用IPV6的单位提供了及时的应对方案。

典型部署/应用

网御网络审计系统采用旁路部署方式，全面支持电口镜像与分路、光口的镜像与分光等多种线路部署方式，在复杂网络环境下的部署游刃有余，运用自如。对于单台设备无法处理的超大流量环境或含有分支机构的分布式环境，系统支持高扩展性的多台设备分布式部署方案，通过多台设备对超大的流量或各分支机构分而治之，又由统一的管理平台实现对整个网络的透明、统一的管理。

# 网络审计系统（数据库审计型）

网御星云

产品简介

网络审计系统（数据库审计型）

◎多种响应方式

－在网络审计系统（数据库审计型）审计服务器中记录相应的操作过程；

－在日常审计报告中标注；

－向网络审计系统（数据库审计型）管理控制台发出告警信息；

－实时RST阻断会话连接；

－管理人员通过本系统手工RST阻断会话连接；

－通过Syslog方式进行告警

－通过SNMP Trap方式进行告警

－通过邮件方式进行告警

网御网络审计系统V3.0实时监视网络系统的运行状态， 记录网络事件，发现安全隐患，对网络活动信息进行记录， 存储，分析和审计。全面实现管理层对内部网络资源和用户行为的全局监控，建立完善的安全预警和应急响应体系，为信息安全提供保障。系统包括两部分：审计引擎、审计数据中心,引擎负责抓包审计，数据中心用来管理引擎，收集日志，生成报表，展示结果。

48 产品特点

## 人性化的报表展示

◎多种筛选条件自定义

报表自定义报表筛选条件可基于时间、客户端IP、服务端IP、关键字、事件级别、引擎名、业务用户身份等进行组合设置。可根据需要灵活地设置审计报表的各种要素，迅速生成自己希望看到的审计内容。

◎宏观事件到微观事件钻取

提供从宏观报表到微观事件的关联，审计员可以在统计报表、取证报表中查看宏观的审计数据统计信息， 通过点击相应链接即可逐步下探到具体的审计事件。

◎自动任务支持

提供报表任务功能，审计员可根据实际情况定制报表生成任务；系统支持HTML、EXCEL、CSV、PDF、Word 等多种文档格式的报表输出，可以通过邮件方式自动发送给管理员。

49

## 丰富的协议支持



◎数据库协议：Oracle/SQL-Server/DB2/Informix/Sybase/Teradata/Mysql/PostgreSQL/Cache/人大金仓Kingbas /达梦DM/神舟通用(OSCAR)等

◎运维协议：Telnet/Rlogin/XDMCP/X11/NFS/VNC/RDP等

◎网络协议：FTP/ HTTP、HTTPS、POP3、SMTP

◎其他协议：NetBIOS/RADIUS等

## 细颗粒度审计

◎细颗粒度规则

支持制定基于用户、服务、主机、规则集、时间等因子随意组合的策略，规则集支持自定义，自定义粒度可细化到命令行级别。

◎多编码环境支持

适用于多种应用环境，特别是在异构环境中，某些数据库同时采用几种编码与客户端进行通讯，若系统不能识别多种编码，会导致数据出现乱码，对多编码的支持是衡量审计系统环境适应性的重要指标之一，网御网络审计系统（数据库审计型）支持如下编码格式

ASCII、Unicode、UTF-8、UTF-16、GB2312、EBCDIC

产品优势

## 性能最高

◎专业设计的数据库结构，优化审计日志入库方式，入库速度业界最高；

◎数据预处理技术，1T日志检索速度达到秒级；

◎专业状态检测和特征匹配算法相结合，提升数据包解析速度；

◎引擎和数据中心采用独立平台，管理和检测分开进行，提升整体处理性能。

## 功能强大

◎支持对数据库协议、网络协议、运维协议等的审计，审计协议丰富；

◎三层关联，实现前台URL和后台SQL语句的对应；

◎异常行为审计，实现全托管，无需复杂的人工配置，即可发现网络中异常操作、异常账号；

◎数据字典，实现网络设备和具体组织、使用人员的对应。

网络审计系统（数据库审计型）/网络审计系统（防统方专用版）

典型部署

## 旁路部署

网御星云

网络审计系统（防统方专用版）

产品简介

网御网络审计系统（防统方专用版）是一款专门针对医疗行业非法统方行为进行甄别记录的审计产品。系统通过对各种网络行为进行解析、分析、记录、汇报，可以帮助医疗行业用户对统方行为进行监控与审计。从事前规划预防、事中实时监视、事后日志报告、事件追踪溯源等多角度、多方位对统方进行管理，加强医院监管，完善业务系统的安全防范体系，遏制医疗腐败事件的发生。

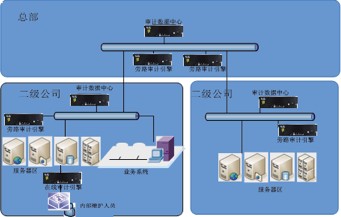
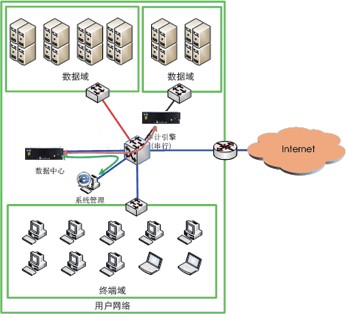
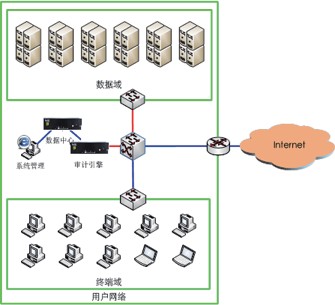
## 在线部署

50

产品特点

## HIS访问人员的定位与管理

51



◎实现数据库访问人员的定位与管理

◎实现HIS系统访问人员的定位与管理

◎实现基于科室和用户名称的审计记录

## 详细的审计报告

统方事件可精确定位到科室、人员、时刻、操作目标等。系统可提供Word、Excel、HTML、PDF等格式报表。系统提供统方事件统计日、周、月、年报表，可自定义报表。可统计疑似统方事件TOP10，并呈现重点疑 似统方事件原始操作。

## 多级部署

网络审计系统（防统方专用版）

## HIS系统访问与数据库操作的全面审计

支持多种数据库访问方式的审计，包括：客户端/数据库访问、浏览器/Web服务器/数据库访问、Telnet远程登录数据库访问、专业数据库工具（如sqlplus等）访问等。

支持对HIS系统访问审计，包括HTTP、FTP、Telnet、网上邻居的访问审计。

产品优势

## 型号丰富

网御对三甲及以上医院、三甲以下医院、社区卫生院等不同医疗单位需求深度调研。设计研发出多款防统方产品。提供千兆高端、千兆标准、百兆标准等多个产品档次，用户可根据实际情况选用。

## 性能强劲

高端产品采用分体式架构设计，分为数据引擎和数据中心。将捕包解析操作与数据写入分机处理。实现1+1>2的性能提升。数据中心采用RAID5磁盘阵列，突破磁盘I/O瓶颈。

数据捕包采用“零拷贝”技术，提高捕包效率100 以上。数据查询中应用中间表技术，减少磁盘I/O。极

52 大的提高了产品性能。查询TB级数据秒出。

## 关联审计

## 分级部署

如下图所示，管理员可以在上级防统方系统中对下级系统进行配置，这样管理员可以通过一级审计系统实现对二级、三级审计系统的审计策略、日志、报表的统一管理。

53

部分HIS系统采用B/S三层结构或基于中间件的三层结构，用户的一个业务操作往往是由两个不同过程来完成，首先客户端访问应用服务器进行业务操作，然后再通过应用服务器访问后台数据库来获取或修改数据。目前国内所有防统方系统及多数审计系统都只能分别审计这两个过程，无法将这两个过程关联起来形成一个完整的业务操作。防统方系统利用独创的先进技术，真正实现了业务操作与数据库操作的关联审计。

典型部署

## 旁路部署方式

采用旁路部署方式对原有网络不造成影响，设备故障不影响现有网络的正常运行。一般部署方式如下： 1、根据不同的审计范围部署一到多台防统方系统；

2、通过IE浏览器进行访问和管理。

# 内网安全管理系统Leadsec-ISM

网御星云

内网安全管理系统Leadsec-ISM

产品荣誉

◎2011年度网管员最喜爱的内网安全产品奖

◎2011年度最佳终端安全产品奖

◎2010年度网管员最喜爱的终端安全管理产品奖

◎2009年度CPW年度盛典应用导向产品奖

◎2007年度中国网络技术与产品调查网管员最喜爱的内网安全产品奖

产品简介

产品特点

网御ISM内网安全管理系统（以下简称ISM），以业界领先的准入控制技术为依托，以内网终端为管理对象，全面解决终端安全管理建设各阶段面临的难题。ISM拥有丰富的各行业解决方案，覆盖了终端桌面及资产管理、主机防火墙、主机监控与审计、非法外联控制、移动存储管理、终端接入管理及准入控制、终端身份认证、安全基线管理、DLP（数据防泄密）等各种需求。

54 其中ISM DLP致力于实现识别机密数据的内容，正确的认识客户的业务流程，梳理出合理的业务流程保证敏感

数据正确的流动为目标。构建完善的终端数据安全管理体系和终端数据风险运营中心，关注数据各个环节的安全，提供统一解决方案，促进核心业务持续安全运行。产品秉承“关注终端数据各个环节的安全，提供统一解决方案”设计理念，为您构筑安全合规的内网环境，帮您实现终端安全管理的跨越式发展。

终端安全管理

## 最全面的准入控制技术

具备业界最完善的终端准入控制技术，从网络准入、应用准入到客户端准入，从有线网络到无线网络，从Windows平台到Linux、Android、iOS平台，从有客户端到无客户端Portal，准入控制条件丰富，彻底解决终端安全接入问题，多层准入控制手段可灵活组合，适用于各种复杂网络环境，确保准入控制无盲点，充分保护用户投资。

## 全过程终端安全管理 55

ISM提供的产品功能覆盖终端安全管理各个方面：准入控制、桌面管理、移动存储管理、DLP（数据防泄密）等。

其中ISM DLP（数据防泄密）致力于为客户带来易于使用并且可以集中控制的数据安全解决方案，从容应对各种最新的、不可预测的泄密威胁，其中包括有意或无意的数据泄密行为。

## 最易部署的终端管理产品

借助独特的CSC体系架构和ISM强大的多层准入控制技术，ISM解决了终端产品部署的难题，使终端部署变 得简单。利用准入控制创造的“客户端用户自助安装”模式，管理员足不出户，轻松完成客户端的安装部署。

## 细粒度强控制

ISM具备真正的安全内核，能够实现对终端和终端用户行为最细粒度的控制，使主机监控与审计、非法外联控制、主机防火墙、移动存储管理、准入控制、终端数据防泄密、单点登录等都具有细致的管理粒度，保证终端用户行为按照预定规范执行，并有效杜绝各种潜在攻击和违规行为所带来的安全风险。

## 广泛的成功案例

经过多年的市场耕耘，ISM已经在包括政府、电力、能源、企业、金融、电信运营商、军工等多行业得到广泛的应用，借助ISM提供的终端安全管理解决方案，帮助用户解决他们遇到的终端安全管理问题，获得用户 的广泛好评。

内网安全管理系统Leadsec-ISM

典型案例

## 广州亚运会

◎依靠网络准入控制解决终端的接入管理，防范非授权人员的终端随意接入导致的病毒传播及网络攻击的

风险

◎终端安全基线管理，监控终端的防病毒软件的运行和升级状态，以及补丁的安装状态

◎移动存储及外设管理，防止病毒通过移动存储或外设感染网络

◎在比赛期间长时间稳定运行，接入认证及授权方便迅速，是包括奥运会在内的大型国际赛事首次采用网络准入进行接入管理，得到了组委会及IT运营商的高度肯定

## 某国有银行广东省分行

◎开启USER-IP绑定的802.1X准入，不安装ISM客户端不能接入网络，合法用户才能入网，并自动设定IP地址，根据用户身份自动设定网络访问权限

◎不安装指定防病毒软件及病毒库没有及时升级不能访问网络

◎禁止运行IM软件，部分区域禁止双网卡，部分区域禁止使用远程桌面

◎ARP防护，阻止内网ARP欺骗

◎自动化的补丁管理、资产管理

56

## 某电信运营商辽宁省分公司

◎DNS准入，不安装ISM客户端不能访问互联网

◎不安装指定杀毒软件不能访问网络

◎分级分部门管理，由各地不同级别的管理员共同管理

◎ARP防护，阻止内网ARP欺骗和嗅探

◎自动化补丁管理，资产管理

◎终端安全加固，终端必须加入AD域方可访问网络

◎网络访问控制，终端只能访问指定的网段或服务器

## 某市地税局

## 某大型国有企业

◎802.1x网络准入控制，实现终端接入管理，非授权终端和用户禁止接入网络

◎网络访问控制，对终端能够访问的企业业务进行规范，杜绝非授权访问

◎安全基线管理，对终端进行安全加固，监控防病毒软件运行及升级状态，监控补丁安装状态

◎移动存储管理，防止敏感信息外泄及防止病毒从移动存储设备感染内网终端

◎资产管理，对企业终端资产进行自动化管理及跟踪

## 某大型全国性商业银行

◎组策略管理功能提高所有办公终端的安全基线。整体完全基线的提升大大增强了办公网络的抵御能力。

◎ISM在线补丁管理功能在空闲时段为内网所有终端及时安装补丁。对未能及时安装补丁的终端要求修复状态后才可以访问网络。

◎软件分发功能不只为用户主动安装各类办公软件，还可以为其他不具有升级功能的应用系统安装补丁文件等。

◎软件中心功能为用户提供了统一的软件下载平台，不依赖于软件分发功能，由用户自主选择需要安装的软件。体现了IT运维部门服务用户的理念。

◎自动关机节电每年为用户节省上百万元的支出。

某市供电局 57

◎敏感文档发现：通过敏感文件扫描功能发现那些包含敏感信息和数据的文档保存在用户终端上，提前发现敏感信息和数据的违规保存和使用的行为。根据发现情况，评估当前涉密状态和涉密程度，对相关的管控策略进行更新，降低由于数据泄密造成的风险。

◎敏感信息外发监控：控制电子邮件、QQ、Web上传、打印、刻录、客户端私自拷贝数据等外泄行为，对通过各种渠道违规外传敏感信息和数据的行为进行拦截，并针对这些违规行为进行记录。

◎敏感信息审计：根据各种违规审计记录，将违规行为追查到当事人，必要时进行通报处理。

◎通过对内网范围的终端数据防泄密建设可以在满足有关监管要求的同时，补齐现有安全防御体系中的薄弱环节，有效封堵常见数据泄密渠道，并且通过该系统有效震慑各种潜在泄密企图，并教育广大内部用户杜绝各种无意识的泄密行为，将敏感信息泄露造成的风险降至最低。



◎主机监控与审计，使终端安全状态及操作行为符合国家保密局的主机审计要求，以通过政府涉密检查

◎安全基线管理，对终端进行安全加固，监控防病毒软件运行及升级状态，监控补丁安装状态

◎非法外联监控，监控并阻止内网终端访问互联网

◎资产管理，对企业终端资产进行自动化管理及跟踪

◎网络访问控制，终端只能访问指定的网段或服务器

# 安全管理系统Leadsec-SOC

网御星云

安全管理系统Leadsec-SOC

## 领先的大数据安全分析技术架构（大数据版）

以分布式并行计算和智能分析方法为基础架构，实现高速数据采集、多源异构数据融合、海量数据存储、智能化安全分析和数据可视化，构建下一代安全管理平台。最大入库性能提升4倍以上，搜索性能提升100倍以上。

产品简介

网御安全管理系统（Leadsec-SOC）是一个以IT资产为基础，以业务信息系统为核心，以客户体验为指引，具有监控、审计、风险和运维的可度量的统一业务支撑平台，满足各种用户对业务信息系统进行可用性与性能的监控、安全数据与事件的分析审计预警、风险与态势的度量与评估、标准化安全运维的需求，最终保护业务信息系统持续安全运营。

产品特点

58

## 面向业务的统一安全管理

系统可以构建业务拓扑，自动构建业务健康指标体系，协助用户从业务的角度去分析业务可用性、业务安全事件和业务告警。

## 强大的安全监控和分析功能

## 安全分析师的工作利器（大数据版）

强大的混合式搜索功能，支持格式化字段查询和全文检索，支持即席在线查询，交互式分析。

产品优势

◎一站式安全运营中心，内置网络管理、安全管理和运维管理功能，灵活选择功能

◎支持超过130种国内外主流设备和系统日志及事件的高速采集、范式化、关联分析、安全存储和响应

◎国内最完善的安全管理知识库，定期维护和更新

◎国内最领先的安全事件关联分析与态势感知能力，实现全网安全风险的量化分析、安全态势评估，并具有态势预测的能力

◎国内第一个采用大数据分析架构的安全管理平台，充分运用并行分布式信息采集、分布式计算和分布式存储技术

59

◎系统开放，可伸缩、可裁剪、可扩展、可集成

◎强大的客户化定制能力，拥有国内最专业的定制开发团队和实施运维团队

典型部署/应用

◎全方位的IT系统性能和可用性监控、多种类型和监控项

◎智能化的基于CEP(Complex Event Process)安全事件关联分析引擎和基于机器学习的行为关联分析

◎智能化的流安全分析，采用独创性的vFlow技术

## 丰富的风险分析和预警管理功能

◎主动的包括漏洞和配置核查在内的全面脆弱性管理

◎创新的基于矩阵的风险评估功能

◎国内首个具备态势宏观分析能力的安全管理平台

◎丰富多样的安全响应管理

## 威胁情报的采集与利用

通过采集威胁情报，结合规则关联和观察列表，使安全管理人员及时发现来自外部攻击源的威胁，实现威胁情报的采集与利用。

# 安全管理系统

网御星云

安全管理系统

## 丰富的报表与呈现

系统通过专业的第三方图表软件，可以生成30多种审计报表，报表支持表格和多种图形表现形式；用户可设定定时生成日志统计报表，并自动保存以备审阅或自动通过邮件发送给指定收件人，实现对安全审计的流程化处理。

产品简介

网御安全管理系统以资产为中心，依据P2DR安全模型，以资产管理、策略管理、设备监控、拓扑管理、补丁下发、日志审计、报表生成等功能集成，能够协助用户实时监控安全设备的正常运行，进行安全设备的事件审计，并为用户解决安全问题提供指导安全管理运行平台。此系统主要对网关本部自研产品进行地集中管理。

网御安全集中管理系统通过SNMP管理协议、SYSLOG以及专用协议等与安全设备通信，以标准平台、基于组件的各类服务为基础构成的安全设备管理系统、安全事件审计系统、安全风险监控三大系统，根据各类实时信息和资产库等基础数据，通过WEB客户端为用户提供了策略配置、设备监控、资产管理、日志管理等服务。

典型部署/应用

在XX企业信息中心网络项目中，部署网御星云安全管理系统一套，实现对防火墙、AV等设备的集中监控、拓扑管理以及设备日志的统一收集、查询和关联分析。

安全管理系统

产品特点

60 直观清晰的拓扑图管理

安全策略远程登陆配置管理

......

61

安全事件告警数据

......

系统支持拓扑图管理方式，用户可以将本单位按照组织结构划分为多个管理域，管理域支持下钻功能，并可直观的显示网络部署和设备情况。

## 智能备份的恢复机制

系统能够周期性地对数据进行备份，并可在数据达到设定阀值时自动对数据进行备份及清除，以确保数据完整性。也可以在需要时将备份的数据重新导入系统中。

## 高效的中间数据压缩

◎通过设备管理功能，形成全局网络拓扑，集中监控各类设备的运行状态、流量状态、告警状态；

◎通过事件管理功能，收集各类设备发出的日志，并进行实时分析，及时发现日志中包含的安全威胁信息；

◎安全管理系统定时统计网络安全事件，形成安全信息审计报告。

为增大备份数据的信息量，系统对备份的数据采用压缩后再保存的方法，压缩率达到90 。在数据重新导入系统时先解压再导入。该方法可极大地增加信息的保存量。

## 海量可靠的日志管理

数量众多的网关安全设备每秒钟都会产生数以万计的事件和日志，它对于系统的处理能力和存储能力都提出了很高的要求，通过数据的压缩、中间分析数据提取以及海量数据存储机制，可以很好的保证数据的完整、系统的稳定和性能。

# 日志审计系统Leadsec-R

网御星云

产品简介

日志审计系统Leadsec-RS

## 安全分析师的工作利器（大数据版）

强大的混合式搜索功能，支持格式化字段查询和全文检索，支持即席在线查询，交互式分析。

产品优势

网御日志审计系统（以下简称Leadsec-RS）是一款用于信息系统日志审计的安全产品。能够通过主被动结合的手段，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。Leadsec-RS具有广泛的应用范围和客户群，在政府、电信、金融、电力、公安、军工、企业等行业均有成功的应用。

产品资质

◎国家版权局《计算机软件著作权登记证书》

◎公安部《计算机信息系统安全专用产品销售许可证》（日志分析三级）

◎保密局《涉密信息系统产品检测证书》

◎中国人民解放军《军用信息安全产品认证证书》

62

◎《中国国家信息安全认证产品证书》增强级——（安全审计产品）

◎中国信息安全测评中心《信息技术产品安全测评证书》EAL3+级

◎《IPv6认证证书》

◎满足等保、合规、内控要求的日志审计系统

◎面向信息系统全面综合审计的基础平台

◎集高性能采集与高性能处理能力于一身的日志审计系统

◎国内拥有各行业用户最多成功案例应用的日志审计系统

◎国内第一个采用大数据分析架构的日志管理平台，充分运用并行分布式信息采集、分布式计算和分布式存储技术

典型部署/应用

63

产品特点

## 详尽的日志范式化和日志分类

系统对收集的各种日志进行范式化处理，将各种不同表达方式的日志转换成统一的描述形式。审计人员不必再去熟悉不同厂商不同的日志信息，从而大大提升审计工作效率。

## 集中化的日志综合审计

系统提供了强大的日志综合审计功能，为不用层级的用户提供了多视角、多层次的审计视图。系统提供超强的日志查询和报表管理功能，支持日志的模糊查询和自定义报表。

## 威胁情报的采集与利用

通过采集威胁情报，结合规则关联和观察列表，使安全管理人员及时发现来自已发现的外部攻击源的威胁，实现威胁情报的采集与利用。

## 融合大数据技术的日志管理技术架构（大数据版）

为了应对海量日志管理带来的挑战，大数据版日志审计采用了国内领先的高性能日志采集范式化、大数据分布式存储与索引、流式集中事件及情境关联分析等技术，从产品技术架构的层面，进行了系统性的设计，真正使得大数据版日志审计产品成为一款能够支撑持续海量日志管理的系统。

订购信息

|  |  |
| --- | --- |
| 标准版本产品型号 | 描述 |
| Leadsec-RS-SW日志审计系统软件 | 软件包。提供主机操作系统、网络设备、安全设备日志收集，查询，告警，审计，报表等功能。 |
| Leadsec-RS-500日志审计硬件 | 日志审计硬件平台。集成日志审计系统，2U标准机架式，冗余电源，专用硬件平台和安全操作系 统。6个千兆电口，1个管理口，存储容量2TB。提供一年免费软件维护升级服务。默认支持30个审 计对象授权。  默认质保期内，硬件免费维修。 |
| Leadsec-RS-1000N日志审计硬件 | 日志审计硬件平台。集成日志审计系统，2U标准机架式，冗余电源，专用千兆硬件平台和安全操 作系统。6个千兆电口，1个管理口，2个USB接口，1个接口板(Leadsec-RS-1000N专用扩展板)，标配 采用Raid5，有效存储容量4TB。提供一年免费软件维护升级服务。默认支持30个审计对象授权。默认质保期内，硬件免费维修。 |
|  |  |
| 大数据版本产品型号 | 描述 |
| Leadsec-RS-CDB日志审计系统软件 | 软件包。提供主机操作系统、网络设备、安全设备日志收集、查询、告警、审计、报表等功能。 单机部署时日志审计性能可达平均15000EPS（事件数每秒），审计中心集群部署后可达到平均5万EPS（事件数每秒）。 |

# 网络行为分析系统Leadsec-NBA

网御星云

网络行为分析系统Leadsec-NBA

## 增强的USM分析深度

对流行为和安全事件进行交叉关联分析，发现更深层次的入侵和违规，可精细化事件优先级，减少误报率。

产品简介

以深度流分析技术为基础，结合DPI、日志分析等技术以一体化融合的威胁识别技术为客户提供资产持续监测、恶意流量发现、违规流量检测、网络行为分析、历史流量回溯取证等功能，协助客户及时发现可疑主机，强化安全法规遵循，快速定位网络故障，优化网络利用效率， 历史异常行为取证，提升网络监管水平，为客户网络的安全、有序运行提供有力的支撑。

产品特点

64

## 行为分析

产品优势

## DFI和DPI技术结合

结合深度流检测技术（DFI）和深度包检测技术（DPI），在有限代价的前提下较好平衡了准确和效率两大难题。

## 加强型VFLOW技术

通过插件框架扩展NetFlow流量分析技术进行增强分析、深度检测。

## 多样化的网络秩序分析手段

业务访问关系自动发现、黑\白\灰名单机制、专用检测算法等多种机制多角度检测异常行为。

65

产品以时间（分钟、小时、天、月、实时、历史等）、空间（全网、IP段、IP组、自定义空间等）和特征

（总流量、进流量、出流量、带宽利用率、数据包分布、协议分布、端口分布等）为基础，对网络流量和网络行为进行多维度、细粒度的分析，并通过形象地的图表曲线帮助客户实现流量和行为的可视化。为用户直观了解网络连接拓扑结构和网络运行状况，并为APT攻击研判和优化网络性能和效率提供有力支撑。

## 异常发现

产品通过灵活的黑白灰策略配置和自学习技术，实现对网络行为和业务操作的合规检测，从而从合规的角度保证客户网络的业务安全。如违规的私自接入和外联、违规的内网非法连接、攻击产生的虚假IP发现、可疑主机发现和异常的网络流量发现等。

## 多维度可视化展现

对全网的流量行为进行多维度透视分析，并可视化展示，轻松掌握全局的安全态势。

## 调查回溯

支持在告警和各种可视化图标中进行下钻，对flow进行追溯，甚至直接对原始pcap报文下载进行人工分析，为事后取证、责任落实提供依据。

## 业务保障

通过持续的设备和网络监控，保障正常业务可连续性。如指定设备的活跃度监控、设备的应用分布、设备的连接请求、历史告警等等。

## 与安全管理中心无缝结合

可以安全管理中心结合进行事件关联分析，形成互动的一个更大、更为健壮的安全生态圈。

网络行为分析系统Leadsec-NBA/业务安全管理系统Leadsec-BSM

典型部署/应用

随着信息化的日益深化，政府、企事业单位对内部网络的合法、合规、合理使用及优化等提出新的要求， Leadsec-NBA可广泛应用于政府、企事业单位内部网络的快速发现、定位、解决流量背后的威胁、违规、故障、效用等问题，降低内外部威胁影响，保障业务正常运转、提升服务质量及用户满意度，满足内部控制、等级保护、分级保护等监管要求。

下图展示了系统的一个典型部署场景。作为Leadsec-NBA部署在一个网络可达的区域，通过旁路实现对全 网流量采集、分析和监控。

网御星云

业务安全管理系统Leadsec-BSM

产品简介

网御安全管理系统——业务安全管理系统（简称Leadsec-BSM）是以IT资产为基础、业务信息系统为核心，集IT综合网管、业务支撑系统监控、虚拟化监控、安全分析等功能为一身的统一业务支撑安全管理平台，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，标准化、例行化、常态化的运维流程管控。

66 产品特点

67

对于大型的政府机构或者企事业单位，系统还支持和SOC的多级级联部署模式，以适合客户分级管理的体制。

## 面向业务的统一运行监控

Leadsec-BSM具备面向业务的运行监控能力，使得管理人员能够对业务进行多视角IT资源监控，一目了然 的洞悉业务当前的运行状况和安全状态。

## 全方位的IT系统性能与可用性监控

Leadsec-BSM采用多种网络协议的数据采集方式，支持对大部分主流IT软硬件资产进行全方位细粒度的监 控。系统能够自动发现并描绘出网络拓扑图，展示IT资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局。Leadsec-BSM支持阈值模版功能，可设定告警阈值及动作后批量下发至各类型监控设备，大大降低了大 规模网络的实施工作量。

## 灵活的自定义监控设备方式

为适应用户网络环境中多种多样的网络设备、安全设备，Leadsec-BSM还提供了图形化的自定义监控对象 及监控指标编辑器，方便用户使用。

## 图形化虚拟拓扑及多层次立体化虚拟环境监控

Leadsec-BSM提供了虚拟化环境的拓扑管理，以及基于Vsphere API方式虚拟化监控功能，通过统一监控云计算环境下的整体安全状态，降低云计算环境的安全风险，为云计算保驾护航。

业务安全管理系统Leadsec-BSM/安全配置检查管理系统Leadsec-CVS

## 自动化数据收集，全面提升巡检效率

Leadsec-BSM支持自动或手工巡检所有网络资源，可自定义巡检指标、巡检模版，确保了巡检工作的质量 以及提高了巡检工作的效率，提升了企业生产管理水平。

网御星云

安全配置核查管理系统Leadsec-CVS

## 实时化的IP地址管理

Leadsec-BSM可以管理企业的IP地址资源，提供了IP分布图像化显示，IP地址查询，IP地址扫描，实时把 握当前IP使用情况，降低未知设备接入风险。

## 智能化的安全事件分析

Leadsec-BSM支持多种管理对象和日志类型，支持多种采集协议，具备详尽的日志范式化与事件分类，能够进行基于策略的安全事件分析和智能化的安全事件分析，并提供了丰富的可视化安全事件分析视图。

产品优势

◎面向业务支撑的监控、虚拟化的监控、IT资源智能化日志分析功能；

68 ◎具备基于情境（Context）的关联分析；

◎采取多种技术手段，对用户网络和业务的影响最小化；

◎多视角的故障诊断分析；

◎支持分布式性能监测、分布式日志采集、分布式事件存储，性能更高，可扩展性更好。

产品简介

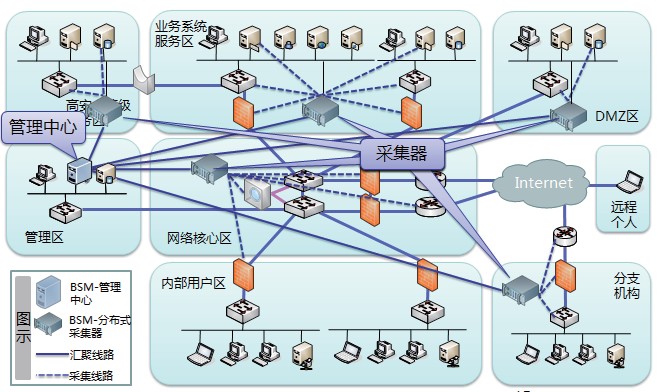
网御安全配置核查管理系统（以下简称Leadsec-CVS）是以自动核查被管设备是否存在配置不合规情况， 并提供详尽的加固方案，提供核查的历史对比，及时准确地掌握设备的整改情况，为设备的自身健壮性提供有力支撑。

产品特点

## 符合等级保护的核查策略

69

安全配置核查系统是专门针对设备配置层面的专业检查设备，而且专门针对等级保护中的条目逐条过滤解读，归类并加以分析，形成专门针对等保的核查策略检查库，协助政企客户去遵从等保的要求。同时，系统通过自动化的检查手段完成自动化的等保核查，形成满足等保要求的核查报告。



典型部署/应用

由上图可见，一个等级保护中的要求项，可以解读分解成多个核查项，例如：采用强化管理的口令鉴别， 解读后会对应多个检查点，包括：口令的复杂度、口令长度限制、口令的生存周期、失效周期、口令失败重试次数等等。总之，配置核查产品通过等级保护的专业核查策略检查库，为运维人员解决了这一难题。

## 复杂网络的多渠道检查支持

安全配置核查管理系统支持在线、离线、分布式采集等多种核查方式，并配备单机代理来解决无登录信息的问题，实现在各类复杂情况下的核查采集，做到全网核查。

单级部署：采集分布式部署示意图

安全配置检查管理系统Leadsec-CVS/漏洞扫描系统

## 开放的自定义功能

可自定义核查标准，核查使用的策略，自定义检查项及脚本，为使用人员提供便利的运维手段。

## 强大的自动探测功能

系统可自动探测被核查的操作系统类型及版本，并自动发现中间件及数据库的安装路径，节约数据采集录入的时间，更智能更准确。

网御星云

漏洞扫描系统

## 智能的错误提醒机制

区别于其它厂商产品，CVS提出全新的错误消息机制，核查失败时准确定位错误，提升产品核查效率。

产品简介

## 高效的多协议支持

提供SSH/Telnet/SMB/RDP/JDBC/Agent/WinRM等协议支持。

## 支持超过1600+ 种检查项的内置知识库储备，不断丰富的CheckList核查知识库与网御安全管理系统（SOC）无缝集成

## 详尽且具有较可读性的配置加固指南

针对每一条不符合规范的配置项，系统都提供了详细的配置安全加固指南。加固指南切合具体的设备类型、系统版本，提出对应的执行命令、参数供加固人员参考，能有效的指导加固操作。

70

产品优势

◎具备等级保护专项策略

◎具备按业务系统分配核查权限

◎具备关键设备核查项告警并转发功能

◎跨设备类型的核查策略自定义，并参数化

◎与网御星云现有安管平台的无缝整合

典型部署/应用

### 网御漏洞扫描系统是网御星云自主研发的基于网络的脆弱性分析、评估与管理系统。

### 网御漏洞扫描系统遵循网御星云在总结多年市场经验和客户需求基础上提出的“发现—扫描—定性— 修复—审核”的安全体系构建法则，综合运用多种国

### 际最新的漏洞扫描与检测技术，能够快速发现网络资产，准确识别资产属性、全面扫描安全漏洞，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而帮助用户在弱点全面评估的基础上实现安全自主掌控。

产品荣誉 71

|  |  |
| --- | --- |
| 资质名称 | 颁发单位 |
| 计算机软件著作权登记证书 | 国家版权局 |
| 计算机信息系统安全专用产品销售许可证（增强级） | 公安部 |
| 涉密信息系统产品检测证书 | 国家保密局涉密信息系统安全保密测评中心 |
| EAL认证（3+级） | 中国信息安全测评中心 |
| 中国国家信息安全产品认证证书 | 中国信息安全认证中心 |
| 军用信息安全产品认证证书（军B） | 中国人民解放军信息安全测评认证中心 |
| 国家信息安全漏洞库兼容性资质证书 | 中国信息安全测评中心 |
| 工业控制系统安全技术测评证书 | 中国信息安全测评中心 |

产品特点

## 全面

### ◎覆盖当前重要、主流的系统漏洞、应用漏洞、配置隐患、弱口令等

### ◎可扫描漏洞数量已超过16000个

### ◎全方位支持网络对象

### ◎全行业中成功应用

漏洞扫描系统

## 快速

◎多任务、多线程、多网口并发扫描

◎每周一次的漏洞库更新

◎遇到紧急、重大的漏洞时即时更新

## 准确

◎准确识别被扫描对象的各种信息

## 业界领先的数据库扫描

### 网御漏扫具备对SQL Server、Oracle、Sybase、DB2、MySQL等多种主流数据库系统的扫描功能，可扫描的数据库系统漏洞总数超过800条，包含了弱口令、用户权限漏洞、访问认证漏洞、系统完整性检查、存储过程漏洞以及与数据库相关的应用程序漏洞等，基本上覆盖了数据库常被用做后门进行攻击的漏洞，并提出相应的修补建议。

### 网御漏洞扫描系统作为国内最早的漏洞扫描产品，已在全行业中成功应用。在政府、金融、电信、军队、教育、企业、能源等各行业获得了最广泛的用户认可。

## 全面的漏洞检查能力

### 网御漏洞扫描系统能够全方位检测网络系统中存在的脆弱性，可发现信息系统存在的系统漏洞、应用漏 洞、web应用安全漏洞、安全配置漏洞，可扫描的漏洞数量已经超过16000个，覆盖了当前网络环境中重要的、流行的漏洞，并且能够根据网络环境的变化及时调整更新，确保漏洞识别的全面性和时效性。

### 网御漏洞扫描系统能够全方位支持网络对象，包括网络主机（如服务器、客户机、网络打印机）、操作系统（如Microsoft Windows 系列、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD等）、网络设备（如Cisco、Alcatel、D-Link等，支持IPv4/IPv6双协议栈）、应用系统（如数据库、Web应用、FTP、电子邮件等）、常用软件（如Office、Symantec、McAfee、Chrome、IE等）、云计算平台（OpenStack、KVM、Vmware、Xen等）、Apple类（如MAC OS，Safari，itunes等）、网站开源架构（如phpmyadmin、WordPress 等）。同时支持Web漏洞检测功能、网站可用性和响应速度监控、网页变更监控、DNS解析监控、关键字监控、ICP备案号检测、暗链挂马监控等诸多监控功能。

典型部署/应用

### 网御漏洞扫描系统的部署非常简单，应用灵活，适合各种规模的企业、单位以及检查测评机构使用。

## 独立扫描

### 中小型企业和单位可以通过部署单个网御漏洞扫描系统扫描单元实现对全网各个区域的自主扫描，部署如下图示。这种独立扫描的情况同时适合监察评测机构，他们可以将网御漏洞扫描系统安装在笔记本电脑上，即可实现对独立网络单元的移动式检查测评。

## 72 快速的任务执行与数据更新能力

73

### 网御漏扫综合运用预探测、渐进式、多线程的扫描技术，能够快速发现目标网络中的存活主机，根据渐进式探测结果选择适合的扫描策略，启动多个任务、多个线程进行并发扫描。对于扫描对象分布在多个互不相通的网段中的扫描任务，网御漏扫提供多网口并发扫描，无需移动扫描器设备或更改网络配置，大大简化用户操作复杂度的同时保证了扫描任务可以迅速完成。

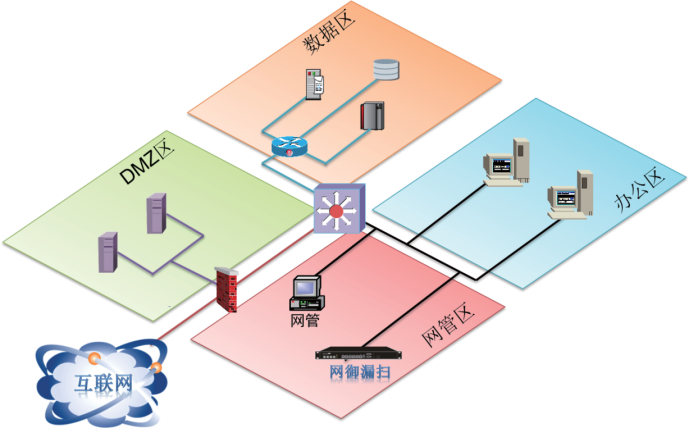
### 通过对漏洞发布信息的实时跟踪和分析，网御漏扫能够及时更新漏洞的补丁信息和修补建议，保持每周一次的漏洞库更新，并在遇到紧急、重大的漏洞时即时更新。

## 准确的信息扫描与发现能力

### 网御漏扫采用渐进式扫描分析方法，融合最新的操作系统指纹识别、智能端口服务识别等技术，能够准确识别被扫描对象的各种信息，如操作系统、网络名、用户信息、非常规端口上开放的服务等。除了使用常规方法扫描外，网御漏扫还可以对于同一漏洞采用多种不同类型的扫描方法进行关联校验，以达到准确判断效果。

## 统一管理

### 统一的脆弱性扫描与管理体系更加适合大型的信息系统，除了能够减少人力资源投入外，还能够对整个网络的脆弱性管理实施统一扫描策略和有效监管，降低了上下级间的沟通成本，提高了脆弱性扫描与管理工作的效率。



## 灵活的部署方案

### 针对不同的客户需求，网御漏扫有丰富的产品型号可供选择，能够实现灵活的应用部署，既可以在独立网络中单独使用，又可以实现分布式多级部署下的统一管理，能够最大限度的满足用户的各种部署要求。同时网御漏扫产品的三大模块系统漏洞扫描、安全配置核查、Web漏洞扫描可单独部署，满足不同用户的不同需求。

## 支持云计算平台漏洞扫描

### 全面支持云计算平台SaaS层、PaaS层、IaaS层的漏洞扫描，包括OpenStack、KVM、Vmware等主流的云计算平台，云平台的SaaS层的扫描主要由Web扫描模块完成；云平台的PaaS层、IaaS层的扫描主要由系统扫描模块完成。

APT检查

网御星云

产品定位

APT检测

产品亮点

### ◎漏洞利用行为检测

### ◎文件威胁行为检测

### ◎外联隐蔽信道检测

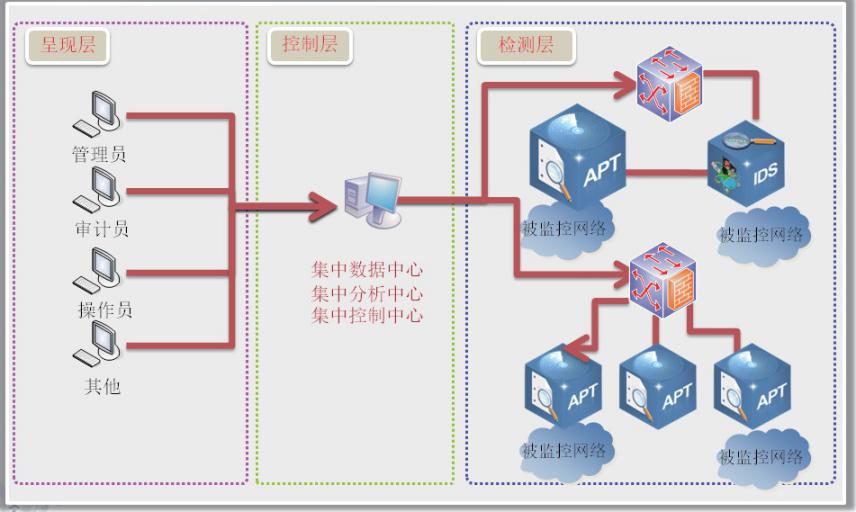
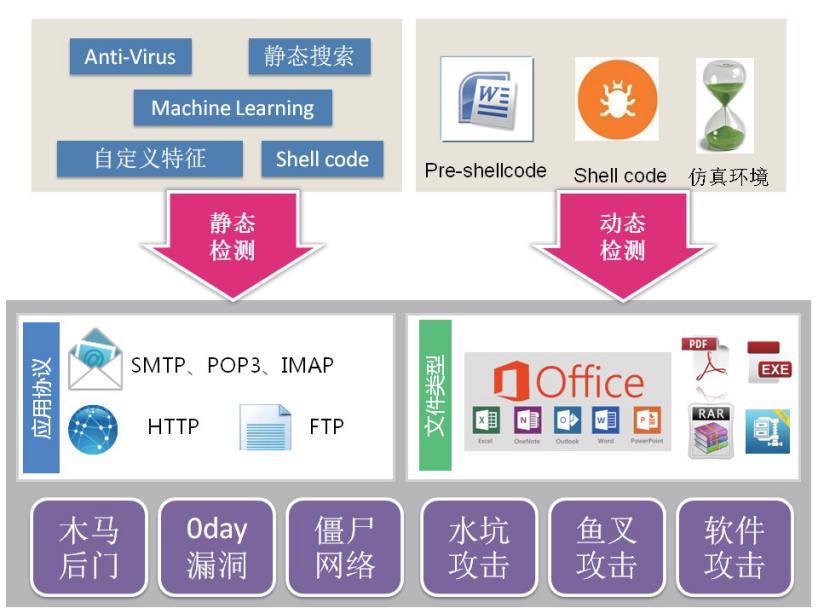
### ◎多环境虚拟机调度

### ◎恶意样本留存机制

### ◎安全产品深度联动

### ◎恶意代码分析服务

### 网御APT检测系列，是一款针对网络中未知威胁深度检测后提供专业分析报告的安全产品，产品可对未知恶意代码威胁、未知漏洞利用攻击、嵌套式攻击、木马蠕虫病毒攻击、外联隐蔽信道等多类型攻击行为的有效检测，由启明星辰集团独立自主研发。



### 网御APT检测系列中的APT3000型号，是在一台检测设备上，实现了网络层已知威胁检测的入侵检测（即IDS）和未知高级持续性威胁检测（APT）的所有功能，降低用户采购成本、节省用户部署空间，目前属于国内厂商独家具备的产品形态。

74

产品技术

### 网御APT检测系列采用专业高配置硬件，整机检测性能优异，系统软件兼容性和稳定性国内领先，系列采用双重检测方法（静态检测和动态检测），多重检测技术手段，包括但不限于：二进制检测、堆喷检测、ROP 利用检测、敏感API检测、堆栈检测、Shell code检测、模拟沙箱检测等，从产品化角度帮助用户应对网络APT 攻击，同时，产品配合人工分析服务，能帮助客户避免APT攻击行为的袭扰。

型号配置

|  |  |
| --- | --- |
| 网御APT（单机APT版本） | |
| 产品 | 型号 |
| 网御APT800 | TD3000-APT800 |
| 网御APT1000 | TD3000-APT1000 |
| 网御APT产品IDS检测引擎模块授权 | APT3000-TD-IDS-E-AT |
| 网御高级持续性威胁检测与管理系统（二合一APT） | |
| 产品 | 型号 |
| 网御APT3000-TD-S | APT3000-TD-S |
| 网御APT3000-TD-A | APT3000-TD-A |

典型部署

75

入侵检测系统－虚拟威胁检测系统

网御星云

入侵检测系统——虚拟威胁检测系统

### 其中，Vetrix虚拟化系统是VTDS的基础平台，负责安全产品的虚机管理、授权管理以及系统的自身管理。VTDS系统提供虚拟安全市场功能，安全市场源服务器负责提供各种虚拟安全产品包映像文件。用户可从安全市场源服务器下载虚拟安全产品包，并安装在Vetrix系统的虚拟机里，由安全虚拟机负责实现具体的安全功能。Vetrix和安全市场两部分相互独立，可以灵活部署。如下图所示：

产品简介

### 网御VTDS虚拟化威胁检测系统是一款集多种虚拟安全产品于一身的强大虚拟安全管理系统，具有集成虚拟IDS、虚拟审计、虚拟WAF、虚拟IPS等多种虚拟安全产品于一身的强大功能。产品具备良好的用户体验与易用性， 能够为用户快速组织各类安全产品，构建面向已知威胁、未知恶意威胁、威胁审计于一体的新一代安全检测与防御体系。是网御星云面向政府、军队、金融、电信、企业、

### 76 制造业、医疗、教育等推出的新一代安全产品。

产品功能

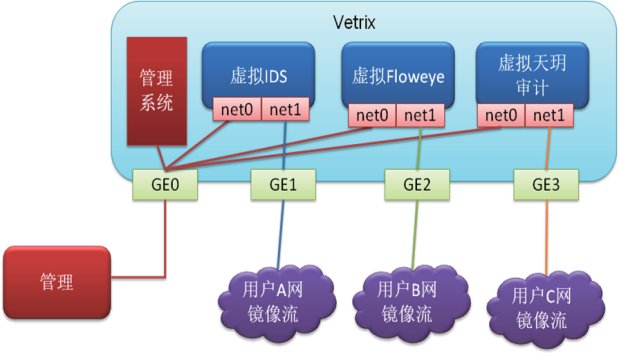
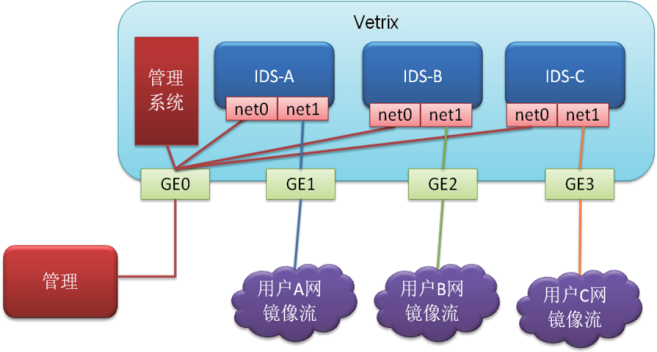
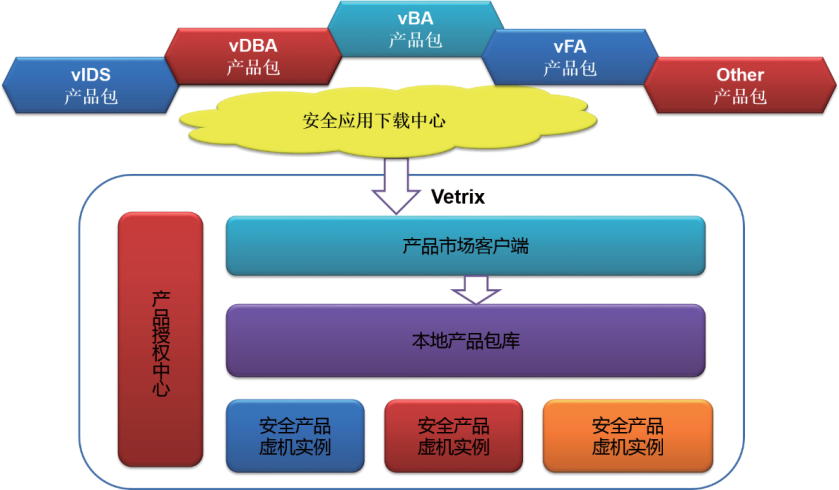
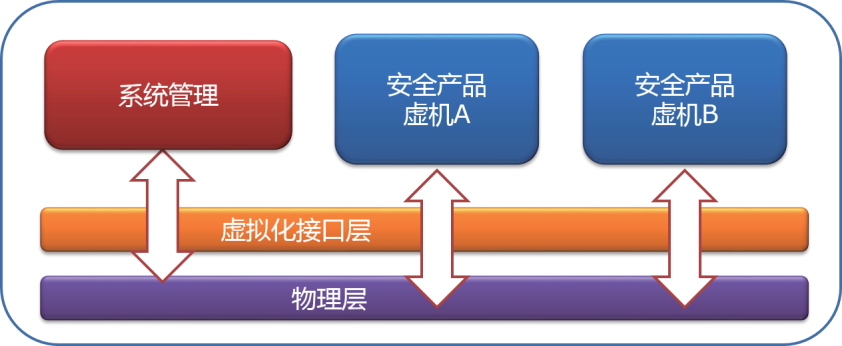
产品规格可能有变化，请以实际产品为准。

### 网御VTDS产品具备良好的用户体验与易用性，能够为用户迅速构建威胁检测、业务审计、安全防护于一体的新一代安全检测与防御体系。不论在部署传统网络的环境，或是搭建私有云的环境，VTDS都具有良好的适应性。产品在政府、军队、金融、电信、交通、医疗、教育、企业、制造业等行业用户中有广阔的市场前景。

77

适应场景

### 网御VTDS虚拟化威胁检测系统，是网御星云自主研发的基于KVM虚拟化技术的可扩展信息安全检测与防护系统。该产品具有可集成多种虚拟安全产品于一身的强大扩展能力。虚拟化的安全产品包括：虚拟IDS (vIDS)、虚拟数据库审计（vDBA）、虚拟FlowEye（vFA）、虚拟业务审计（vBA）等。产品安装后，用户可根据自己的需求动态调整相应的虚拟安全产品，而无需经过复杂的硬件产品上架过程。



### 安全产品虚拟化就是使软件和硬件相互分离，把软件从主要安装硬件中分离出来，使得安全产品的系统可以直接运行在虚拟环境上，可允许多个安全产品同时运行在一个物理硬件之上。如下图所示：

## 传统网络多合一安全一体机

### ◎独享网卡应用方案 Vetirx可将各物理网卡分别与各虚拟机，虚拟机所运行安全功能即可相同，也可不同。各安全虚拟机可分

### 别分析来自所属的网卡的流量。如下图所示：

入侵检测系统－虚拟威胁检测系统

### ◎共享网卡应用方案 Vetirx可将物理网卡共享与各虚拟机，虚拟机所运行安全功能即可相同，也可不同。各虚拟机可分别分析

### 来自不同网段或vlan的流量。如下图所示：

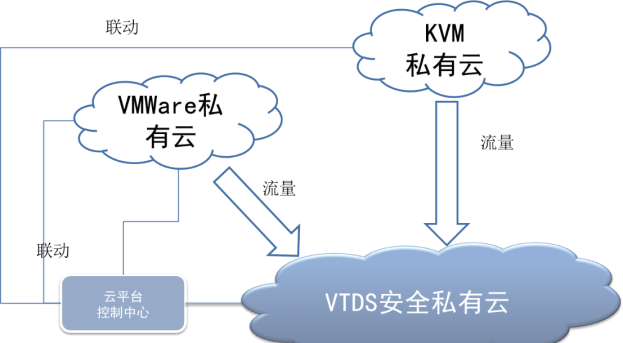
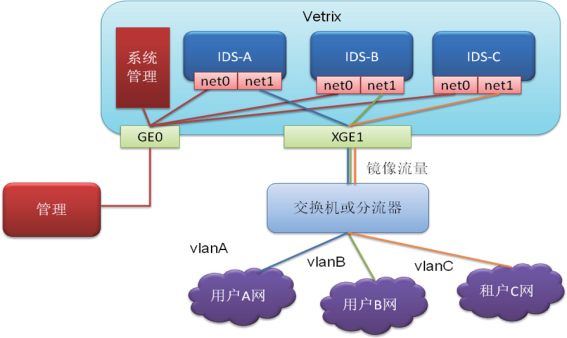
## 减少开销和能耗

### Vetrix通过运用虚拟化、动态迁移和工作负载整合等技术提升运行资源的利用效率；资源的集中共享可以满足多个安全虚拟机不同时间段对资源的峰值要求，避免按峰值需求设计容量和性能而造成的资源浪费。资源利用效率的提高有效降低VTDS的运维成本，减少能耗，实现绿色IT。

## 集中管理

### 基于Vetrix系统创建的安全虚拟机天然具有可被集中管理的特点。利用Vetrix可实现对异构安全产品的状态监视与实时控制。不需要建设专门的信息安全管理系统，缩短业务系统建设周期，使用户能专注于业务的功能和创新，提升业务响应速度和服务质量，实现业务系统的快速部署。

## 私有云的安全资源池



79

|  |  |  |
| --- | --- | --- |
| 一级功能 | 二级功能 | VTDS虚拟化威胁检测系统规格说明书 |
| 主机管理 | 主机资源监控主机基本控制自定义创建虚机虚机的统一配置虚机删除  虚机资源监控虚机配置管理虚机操作管理  产品映像市场  自定义产品映像断点续传  系统授权导入激活  虚拟产品授权导入 | √（可以监视主机当前的CPU、内存、硬盘资源，监控CPU、内存、硬盘使用率情况，支持监控主机运行时间） |
| √（可以重启、关闭主机） |
| 虚机管理  安全市场  授权中心  网络管理  系统管理  日志管理 | √（支持根据产品映像、CPU、内存、硬盘、网口等自定义条件创建安全产品虚拟机） |
| √（支持对虚机管理IP、访问IP、默认路由、DNS、授权服务器、日志服务器、控制中心的统一配置） |
| √（支持删除虚机） |
| √（支持实时或24小时的虚机CPU、内存、硬盘读写监控，支持运行时间统计） |
| √（支持对虚机基于VNC、串口、http/https的配置管理） |
| √（支持对虚机启动、关机、重启、暂停、恢复的操作管理） |
| √（支持局域网下安全产品映像市场，可下载多种安全产品映像和相关文档，用于创建安全产品虚拟机实 |
| 例和日常配置使用） |
| √（支持用户上传第三方产品ISO文件，可用于安装第三方产品，例如windows或linux系统） |
| √（支持产品映像断点续传，显示下载进度） |
| √（支持虚拟机最大数、内存最大值、CPU最大等授权导入和激活） |
| √（支持安全产品的授权导入） |
| 授权详细信息以太接口透明桥  管理访问IP地址  管理员、操作员、审计员权限管理， 具有自身安全审计功能  管理用户资源权限限定  管理员强身份认证功能  系统时间系统启动管理系统配置管理系统升级功能  补丁包的更新和回退串口管理 SSH管理  HTTPS管理 | √（支持授权列表项查看） |
| √（支持协商模式、双工模式、速率、MTU设置） |
| √（支持静态路由、默认路由） |
| √（支持对http、https、vnc、ssh、ping、mysql服务的管理、支持源地址限制） |
| √（支持接口上配置IP地址） |
| √ |
| √ |
| √ (支持静态账号口令、管理员IP地址限制） |
| √（支持从自定义服务器或互联网NTP服务器同步系统时间、支持手工时间同步） |
| √（支持设备双系统启动，支持系统的重启、关机） |
| √（支持系统配置导入导出） |
| √（支持系统升级、历史记录） |
| √ |
| √ |
| √ |
| √ |
| 系统日志  日志查询虚机日志 | √（记录系统运行以及管理员的操作日志） |
| √（根据主机IP、模块、时间、关键字、日志级别查询相关日志） |
| √（支持虚机各种操作日志） |
|  |  | |

### 用户已关注IT资源的使用效率，开始应用虚拟化技术，逐步将原有业务迁移至虚拟化环境之中。虚拟化环境与传统网络环境相比，安全产品的部署受到更多限制，如：旁路型安全设备，因其所需的计算和磁盘I/O更为密集，容易对同物理主机的业务虚拟机造成影响。故旁路型安全产品不宜将安全虚拟机与业务虚拟机同机部署。比较合理的方案是：将租户流量引导到虚拟化环境之外并交付安全设备，实现对流量进行安全检测和分

### 78 析。这样将安全设备独立于承载业务的虚拟化环境部

### 署，可以更清晰的划分职责，并且便于维护。 VTDS可对私有云租户提供个性化的安全能力，用

### 户可以将VTDS作为用户私有云的安全资源池。目前， VTDS已实现同主流云平台的对接：VMware vSphere或Openstack环境均可部署VTDS。部署示意图如右所示：

产品特色

## 安全资源池化

### VTDS可将安全产品以资源池的方式提供给不同用户或云租户使用，这些虚拟的安全资源可根据客户的需求进行动态分配。

## 快速伸缩性

### 客户可以根据需要快速、灵活、方便地配置和释放安全虚拟机资源。对于客户来讲，这种资源是弹性的， 能在任何时候获得所需的安全资源量，以应对随时变化的安全性能需求。

详细功能

网络审计系统－FLowEye安全域流监控产品

网御星云

网络审计系统——FLowEye安全域流监控产品

## 互连关系管理

### 互连关系管理包括互连关系监控、互连关系表和互连关系查询三个功能点。其中，互连关系监控主要展现了业务系统中设备间因一定需求存在的、现实存在的连接情况的总体视图和非法互连关系产生后的告警。对于不在白名单中的互连关系，可由业务系统维护、管理人员和厂商经过分析、判断后进行确认。可帮助用户发现网内设备与境外设备的可疑连接及疑似木马隐蔽通道。

产品简介

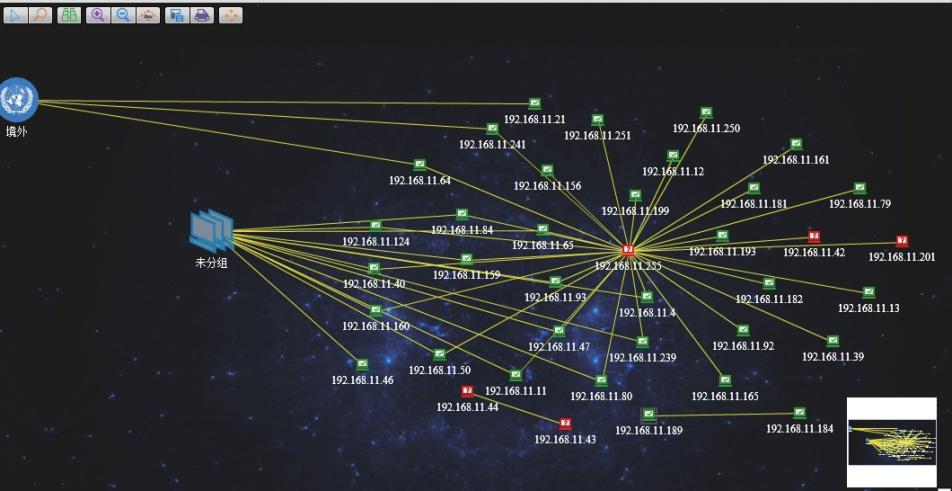
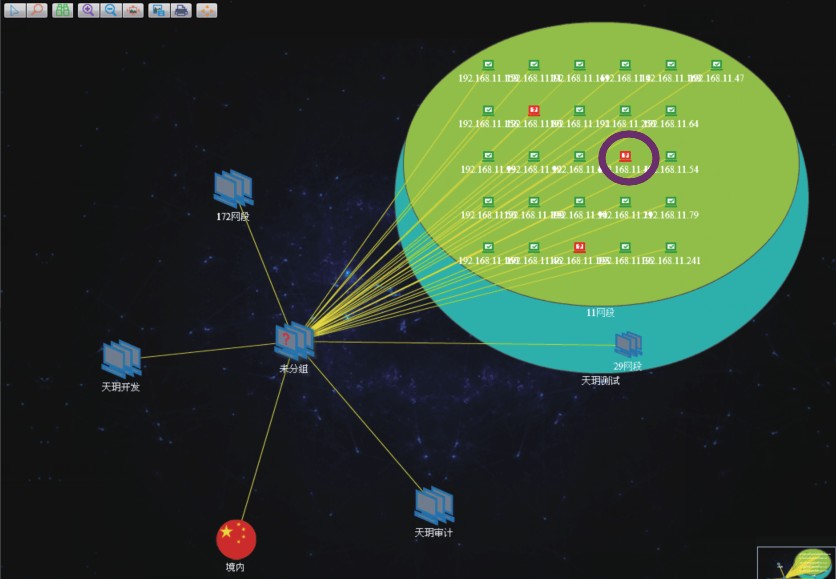
### 网御网络审计系统——安全域流监控（简称FlowEye）产品定位于为用户提供流量监控和分析平台：该平台可帮助用户对网络流量进行分析，梳理出流量中所蕴含的内网主机间、内外网主机间的访问关系。并通过对访问关系数据的挖掘，可发现网内未知设备、来自境内外的可疑连接；确定是否存在异常流量，确定内网是否存在高危IP，确定系统间防火墙安全策略是否合理。同时还能够梳理出安全域间业务访问的黑、白、灰名单。系统依据黑、白名单来精确判断访问关系的正常与异常并协助用户做出适合业务场景的安全管理决策。

81

802

产品功能

## 设备发现



### 产品具备网内设备自动发现功能，对于未在管理范围内的又在网络中存在流量的设备能够自动监测到其存在。能够真实的反映网络设备的存在状况，减少人为手动设置带来的不确定性和复杂性。

## 互连关系监控

### 通过采集不同区域流量，系统能展现出当前监控的所有设备互连关系的连接关系视图。实时显示互连关系视图能够全局的体现当前的多业务系统、安全域、设备、互连关系的存在状况。可全局化和层次化两种直观方式体现这几者之间的关系，并能够体现它们之间的联动关系，给使用者提供便捷逐层定位手段。并可实时的体现网络中多业务系统，安全域，设备，互连关系的变化，并提供有效的信息提示。如下图所示：

网络审计系统－FLowEye安全域流监控产品

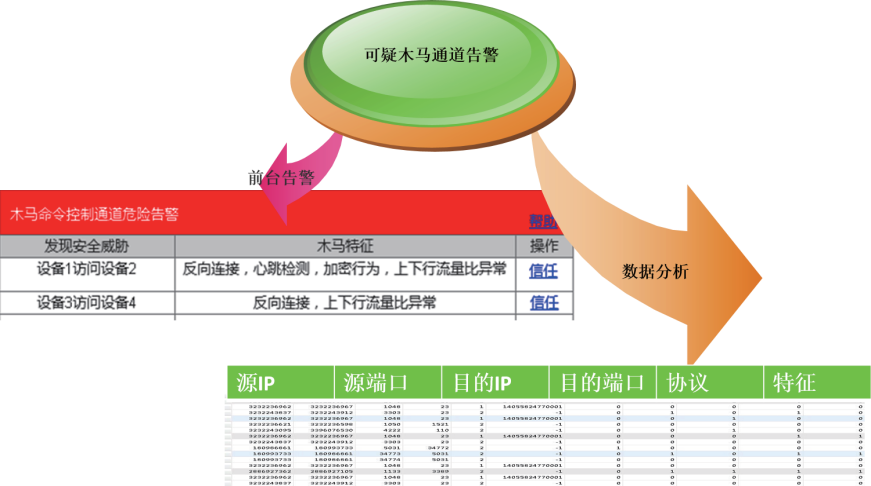
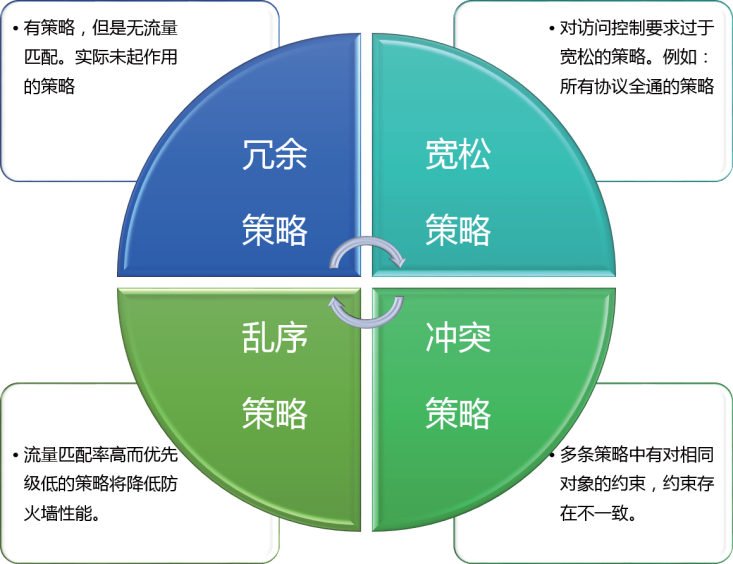
## 省际/国际互连监控

### 针对IP归属地为本地之外的互连，产品提供省际和国际互连监控功能。对于国际互连系统默认提供原始会话数据抓包功能，供用户对可疑国际互连进行事后分析。

境内互连

## 防火墙策略审核

### 产品可根据对实际流量的分析与防火墙策略进行比对。使管理员能了解当前防火墙策略的使用状况，可以查看哪些策略是长期以来没有被使用过，哪些安全策略的使用率最高，可以查看某条安全策略实际的流量状况，分析流量是如何穿过这条策略的。根据这些信息，管理员就可以定位出冗余策略、宽松策略、乱序策略、冲突策略等不合理的防火墙策略。从而使得管理员可对安全策略进行优化，如清理掉一些不必要的策略，并且能够准确了解到当前策略的使用效果等。良好的全图形化界面将提升管理员对安全策略的可视性，这将大大提高管理员针对防火墙的安全管理效率。防火墙的管理将变得简单、容易。



境外互连

83

82

## 木马隐蔽通道发现

### 针对新型木马不断出现，基于特征检测的方法无法有效检测特征库之外的木马的缺点，本产品提供基于木马流量行为特征的木马通道检测方法。其优势在于可以检测新型未知木马的活动，无需依赖木马特征库工作， 间接提高了新型木马检测的时效性。

境外互连

网络审计系统－FLowEye安全域流监控产品

## 高风险IP检测

### FlowEye使用IP资产画像技术，通过勾勒该IP资产的各种特征，例如互连关系、对外提供的服务、各服务的流量和频次等，描绘出该IP资产的整体行为轮廓。当资产的日常行为与其轮廓差异较大时，系统可以基于偏离程度进行不同等级的报警。

产品部署

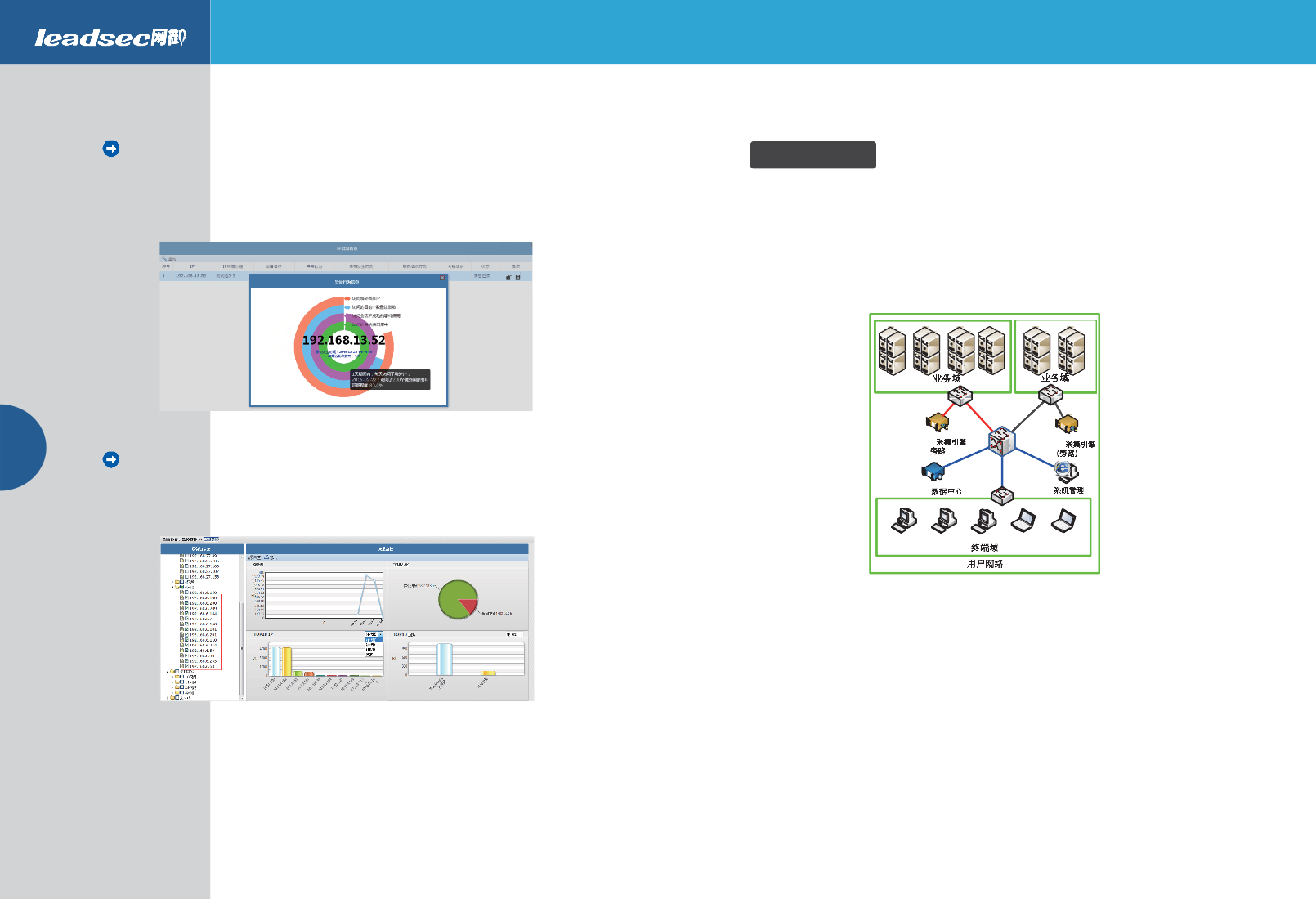
### 安全域流监控产品采用逻辑上两级结构管理方式，即采集和分析控制模式。由采集引擎负责采集网络中的流量并进行协议解析。由数据中心负责收集各引擎的信息，分析网络中的互联关系，并提供管理界面。

### Floweye采集引擎采用旁路部署方式对原有网络不造成影响，设备故障不影响现有网络的正常运行。一般部署方式如下：

### 1、根据不同的监控范围在各交换机上部署一台或多台Floweye采集引擎；

### 2、在管理域部署一台Floweye数据中心，并可与各引擎管理接口路由可达；

### 3、通过IE浏览器访问数据中心进行管理。



84 85

**)**

**Fl owEye**

**Fl owEye**

**(**

## 流量分析

### FlowEye除具有常规的统计分析功能之外，还可根据业务进行流量统计，而非简单得基于IP、协议、时间进行统计。FlowEye可将参与业务的所有主机在一定周期内的流量情况统计分析。其结果更加贴近用户的实际需求。

**Fl owEye**



