



SURF-SA

网络安全审计系统

通过对网络应用内容审计和行为控制来达到保护内网信息安全的目的，同时提供极快的日志查询体验。内置丰富、多元化的统计报表，使管理者能更有针对性地加强网络管理，为其规范网络管理、制定正确的管理决策提供有效依据。

CORE TECHNOLOGIES

核心技术

高性能数据分析处理

通过专业的数据分析处理引擎以及专门硬件加速模块，可实现单台审计设备处理10G流量。



并行协议栈

采用并行协议栈取代传统协议栈，给多路CPU、多内核CPU、超线程CPU足够的施展空间。保证在大流量的情况下处理线程之间工作量均等，有效避免过载线程的出现。



海量数据全文检索

通过对数据存储，数据检索及业务挖掘进行全面优化，运用了先进的全文检索引擎，实现了高带宽下审计数据检索的高效率。



基于FPGA的专用网卡

基于FPGA的专用网卡采用零拷贝技术，网卡收到的报文不再经过操作系统协议栈的层层拷贝，而是直接DMA到应用的缓冲区中，避免了数据拷贝的开销。

PRODUCT FUNCTIONS

8大功能



行为审计 1

标准协议及其衍生应用，即时通讯(IM)/网络电话应用，流媒体/网络视频直播，P2P下载应用，娱乐/游戏应用，财经证券类，数据库访问；



内容审计 2

标准电子邮件，网页浏览，远程登录，文件传输，即时聊天，Web邮箱，论坛，微博、博客，数据库访问；



查询与检索 3

查询条件包括源IP/MAC，目的IP，协议类型，开始时间，结束时间等，海量日志快速检索；



业务报警 4

网络行为报警，应用关键字报警，异常流量报警，设备自身资源阈值报警，多种报警方式；



应用控制 5

应用封堵策略，流量限制，基于IP与应用协议的流量控制，IP/MAC绑定，黑白名单；



用户管理 6

透明识别上网用户，认证识别上网用户，企业组织架构划分，组织管理自动分组。与PPPOE，RADIUS，城市热点，AD域等第三方系统联动；



实时监控 7

设备CPU，内存，磁盘占有率，在线用户数，系统时间，网络接口等信息监控，用户流量排名，应用流量排名；



数据报表 8

统计报表，用户分析，行为分析，流量分析，上机分析，搜索分析，趋势分析，外发文件分析，智能报表，报表订阅。

PRODUCT ADVANTAGES

产品优势



TYPICAL DEPLOYMENT

典型部署（旁路 | 网桥 | 网关）

