

网神SecFox-NBA 网络行为审计系统（上网审计型）M系列

SecFox-NBA（Network Behavior Analysis for Internet Audit）网络行为审计系统（上网审计型）M系列通过串联或者旁路部署的方式对内部网络连接到互联网（Internet）的数据流进行采集、分析和识别，监视并控制用户访问互联网的行为，管理网络带宽，发现对互联网的滥用，过滤不良信息，并对用户上网过程中发送和接收的相关内容进行搜索、存储、查询和分析。

需求分析

随着人们对互联网的使用越来越普及，互联网给我们带来许多方便的同时，也带来了许多风险和挑战，内部人员通过网络泄漏敏感资料的事件时有发生，员工因私上网影响工作的问题日益明显，网管对限制员工私自下载危险文档的需求越来越迫切。

与此同时，国家出台的相关法律法规也越来越强调针对用户的上网行为进行审计，并颁布了强制性规定。例如，2005年底，公安部颁布《互联网安全保护技术措施规定》，明文规定了使用网络的单位要有一定的管理制度。

产品介绍

精准的上网行为管理和带宽管理

SecFox-NBA（上网审计型）M系列具备先进的软硬件体系架构，通过串联或者旁路的方式接入网络，配以先进的行为分析、流量控制、灵活多样的管理控制策略，实时分析网络活动，匹配管控策略，对用户上网行为和带宽进行精准的控制，并生成丰富的统计报表。系统还具备流量管理、认证/授权/计费（AAA）功能。

产品亮点

● 多样的部署方式：

旁路接入：对现有网络应用和网络拓扑不产生任何影响，不占用网络带宽。隐藏IP地址，用户无法发现系统，更无法攻击系统。

网桥/路由：网桥模式不改变网络拓扑结构，路由模式节约网络设备部署费用。同时，产品具备ByPass功能，确保对网络影响最小化。

● DPI与DFI相结合的数据分析技术：

产品采用了以DPI技术为主，辅以传统报文分析技术和DFI技术对加密应用协议进行分析。产品通过综合分析应用层协议特征值和行为、UDP/TCP端口信息、IP地址信息、MAC信息、VLAN标签、MPLS标签、传输方向等数据，达到精确分析应用和协议的目的。

● 定期更新URL库及应用库：

为保证URL分类库的准确性及实时性，产品会定期更新URL分类库和应用协议库，以保证对所有网络应用的准确识别。



功能列表

功能点	说明
型号配置	根据被审计用户的规模大小，每种类型的硬件配置都有不同。单台审计用户规模从100到50000用户。
网络审计	能够对邮件信息、IM信息、网络炒股、网络游戏、网络电话、网络电视、网页提交、网站访问、下载、信息、Telnet、代理软件、自定义应用等进行网络行为审计及管理。
网络管理	支持网桥模式、路由模式和旁路模式部署，支持802.1Q、802.1d。可配置静态路由，支持策略路由。支持IP/MAC绑定、NAT、ACL、DHCP等网络配置功能。
策略管理	可定制控制策略、系统策略等，支持当前互联网流行的大多数应用以及协议分析，包括HTTP、网络层协议、文件访问协议、邮件、FTP等多种协议，还可以对QQ、MSN、ICQ、Yahoo Messenger等应用进行封堵。
带宽管理	可设置外网网卡流入、流出的流量以及配置控制功能和统计功能的开启、关闭。能够分别制定组内或者全局的上传带宽控制/保障策略和下载带宽控制/保障策略/连接速率/连接数。可以输入指定条件查询已添加的带宽策略。
报警管理	具有多种报警方式，支持邮件报警、定制化的提示页面报警，还具有即时阻断功能。
地址分类库管理	内置URL分类过滤库，包含百万个站点以上的记录，含有超过千万的网址，支持用户根据企业内部的网络应用特点自行定义网站分类和网站站点，系统可以对自定义的网站进行按管理策略进行封堵或放行等监控。
报表管理	提供丰富的报表管理功能；根据时间、数据类型等生成报表；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。
认证计费管理	在不改变用户网络结构的情况下，系统以机器IP管理或账号管理方式管理监控范围内的机器，可以对机器或账号实施各种不同的策略。账号控制模式实现了网络实名制管理，同时支持多种第三方认证方式，比如本地认证、Window域服务器、LDAP等。
权限管理	采用基于角色的权限管理机制，通过角色定义支持多用户访问。角色能够从设备和功能两个维度进行定义，从而达到控制谁可以对什么设备进行什么操作的控制粒度。
系统配置	完成对系统自身的各项配置工作。
系统安全性	用户登录时，采用了加密的通讯协议，确保了登陆账号、密码及审计数据的保密性；审计数据加密存储。
性能	吞吐量: 50M-10G
	事件存储性能: 事件存储量仅取决于系统所用存储空间大小
	平均无故障运行时间 (MBTF): 不少于60000小时



欲获取更多信息，请即联系网神信息技术（北京）股份有限公司
 全国统一热线服务电话：400-610-8220（7×24小时）
 E-mail: service@legendsec.com
 网站地址: www.legendsec.com

传真: 010-62972896
 通信地址: 北京市海淀区上地信息产业基地开拓路7号
 先锋大厦2段1层 (100085)

版权所有 网神信息技术（北京）股份有限公司 保留所有权利