

上网行为管理

技术规范



深圳市科创通信科技有限公司

SHENZHEN DIAL-LINK TECHNOLOGY CO., LTD.

Tel : 86-755-33118799 Fax : 86-755-33118798

<http://www.dial-link.net>

产品概述

随着互联网的发展兴起，电子政务、电子商务、视频、语音和多媒体信息在网络中应用日益广泛，网络的拓扑结构越来越复杂，应用环境多种多样，使用网络的人员和需求也千变万化，因此带来了很多的问题，例如：网络服务阻塞变慢、公司核心资料被泄漏、核心数据被破坏、员工大量时间花在与工作无关的网络冲浪上、网络链路失效、内网被入侵、网络病毒、ARP 攻击、DOS 攻击等问题，以及网络使用权限制管理、网络使用监控统计等管理问题都日益严重，这些问题都将直接影响数据业务的服务质量和网络的正常运营，给企业提出了严峻的问题与挑战。

网络面对的各种各样问题，越来越多的管理者希望有一个简单而又稳定可靠的方法来实现对员工的上网行为进行管理，目前国内的 UTM 产品、安全审计类产品、URL 库网页过滤类产品等众多产品均只涉及了部分上网行为管理功能，但这并不是完全实现专业上网行为管理解决方案。完整的上网管理需要包括用户管理、行为审计、行为过滤等多项模块功能，科创通信为推出全面的上网行为管理产品，在独创的核心分析引擎基础上，为用户提供了一个简单易用、高扩展性、功能强大的行为管理产品，目的就是帮助用户提升工作效率、提升带宽效率、避免法律和政治风险、防范泄密风险、提升网络可用可靠性等，为用户带来更大的价值。产品以性能稳定、功能全面、完整等优点，在政府、金融、企业、学校、能源、军队、公安、IT 产业、电信等行业得到了广泛的应用，深受用户好评。

行业需求

★ 全面保护企业信息安全

网络使用面临的外部风险，内部风险不断加大，需要一个整合的产品统一管理，同时对网络攻击，内网异常数据进行管理和过滤，定位攻击源与异常行为，保护企业信息安全，使用高效特征分析引擎来分析攻击特性，关键字特征，文件传输特征等，可以以一种最优化的方式来安全管理网络的各种需求。

★ 防止带宽资源滥用

通过基于应用类型、网站类别、文件类型、用户/用户组、时间段等的细致带宽分配策略来限制 P2P、在线视频、大文件下载等不良应用所占用的带宽，有效地保障 OA、ERP 等办公应用获得足够的带宽支持，提升上网速度和网络办公应用的使用效率。

★ 外发信息过滤、防范泄密

缺少对网络外发信息的管理，企事业单位容易遭遇泄密风险，如单位组织人事调整、市场计划、研发代码等机密泄漏，这将给单位造成严重的损失。凭借对上网应用、行为和内容的精准识别能力，从主动防范外发信息泄密、防范用户被动泄密、以及详细记录上网日志三方面全面防御单位组织信息资产的泄漏风险，最大化的保护信息安全。

★ 快速的找到内部网络问题根源

当出口拥塞，网络访问异常时，只能通过网络层面的设备来分析原因，简单的插拔网线，复位设备，以试图问题解决。但事实上，内在的源头无法定位。产品能让企业拥有更快更准的洞察网络问题应用源头的的能力，能够分析问题的普遍性、严重性、共通性。

★ 网页访问，应用程序管理

在企业中，很多员工喜欢上交友网站、在线炒股、游戏网站、观看视频等，导致员工工作效率低与工作不认真，从而引发各式各样的问题，因此中小企业对无关网站非常需要进和上网行为的管理。产品通过网址分类管理、应用过滤等实现上网管理，从而有效提高员工工作效率，增强企业核心竞争力。

★ 记录上网行为，让管理员有证可依

大部分企业内部员工上网并不受限制，但是他们在网上做了什么？对外发了什么信息？企业完全不知情，也无记录可查询，这就给企业埋下了巨大的法律风险。当企业被公安局网络监察处执行严厉处罚，原因是查出该企业内有员工在网上发布了违反法律的信息，但是无

法查出是哪位员工所为，最后企业只得为这名“幕后英雄”背黑锅。那么在这种情况下，产品将为您提供依据。

★ 让 IT 的管理制度执行难、检查难成为过去

没有对上网行为进行管理，给公司带来了威胁上网安全、泄露机密信息、影响工作效率等风险。为了让网络资源充分地得到利用，公司通常出台了各种 IT 规章制度，不仅悬挂在办公室内，甚至单位组织员工学习讨论。但 IT 制度并没有得到有效的贯彻与执行，执行难和检查难一直困扰着管理人员。产品以用户身份精准识别、上网行为全面识别、上网终端及桌面环境识别为基础，通过上网权限划分、上网流量控制、上网行为审计和记录等手段，帮助单位组织 IT 制度的贯彻和执行，同时规范用户上网行为，以提高效率，保障安全。

★ 让上网速度不会再变慢

在办公室里经常会听到有人抱怨“网速为什么这么慢？”那么企业花钱租用的 10M 甚至 100M 带宽都被用在哪里了？根据联通公司发布的一份调查显示：以迅雷、BT、eDonkey、KaZaA 等为代表的 P2P 应用，消耗了 40% 以上的有效网络带宽。而在企业租用的有限带宽里，充满着大量 P2P 下载、网络电视等应用流量，导致大量带宽被非工作应用所占用。而且，由于 P2P 的应用特征，使得企业高额投资的带宽成了互联网的公共服务，针对 P2P 应用做限制，保障网速带宽。

★ 为网络管理与优化提供决策依据

提供了丰富的网络可视化报表，能够提供详细报告让管理者清晰掌握互联网流量的使用情况，找到造成网络故障的原因和网络瓶颈所在，从而对精细化管理网络，并持续加以优化提供了有效依据。

★ 掌握网络动态、优化网络管理

通过智能报表来自动发现存在有工作效率的问题，并通过关键字报表、热贴报表来反映行为动态。有助于防范问题的出现，并以此为基础实施单位组织文化建设、制度改进等针对性措施，从而提高网络管理水平。

★ 人性化管理，让企业更具凝聚力

产品从员工角度出发，切实做到以人为本的管理模式。在保证员工利益的基础上，倡导员工上网行为管理理念，结合必要的安全技术支持，才能做到切实维护网络资源的同时也兼顾员工自身价值，保证企业整体的发展，从而保证互联网的安全使用，推动整个企业的稳定发展。

技术优势

【强大的内核内容分析引擎技术】

功能强大的内容分析引擎和高效的索引算法，使处理速度得到极大的提高。随着互联网的发展，网络流量和用户数量也随着大幅增加，高效性更能凸显其应用价值和竞争力，产品有足够的处理能力处理各种特大流量或特大用户环境。

【智能识别网络行为】

产品有针对性地识别行为特征、数据流特征、关联特征等，并融合逻辑学、统计学等实现泛滥的网络应用识别的自动化、智能化、流程化。有效的降低对传统 URL 地址库的依赖，让爆炸式发展趋势的网络应用软件、应用协议，更快更智能的识别管理分析。

【灵活的客户端登录控制机制】

产品的客户端登录控制包括 WEB、PPPOE、客户端程序、域用户等，支持自动 MAC 绑定、自动用户识别、默认用户等，可以避免用户繁琐的输入用户密码，以管理终端在线状态，使安全策略更有效地同整体安全防御体系结为一体。

【提供最完整的互联网访问记录】

用户上网信息真实显示，可以根据组、用户、规则和协议进行多向查询，使内网日志一目了然。

【领先的智能流量控制技术】

支持对每台电脑的速度进行准确控制，也可以设置一个时间段，根据当前的带宽使用情况自动设置流量。同时可以分别对每个用户的应用程序的速度进行智能管理，用户还能通过对带宽流量的控制管理和报警信息来了解网络流量状况和防范病毒对网络的进一步损害。

【最新的 P2P 智能识别技术】

产品采用流量识别监测机制，对 P2P 流量进行有效的识别和监测，对用户带宽进行有效管理。

【全面内容过滤，实时页面监控】

大胆创新，新添内容过滤功能，增加了对各类协议具体内容进行实时分析处理，通过预先设置需要过滤的关键词、聊天号码或 ID 号，从而能对网上论坛发言、聊天室、QQ 聊天、MSN 聊天、YAHOO! 聊天、ICQ 聊天等进行实时过滤和监控，报警或阻挡，做到了对论坛发言及聊天从事后安全审计到事前预防监控的飞跃，率先成功实行了在局域网环境的互联网内容过滤。

【智能的负载均衡并行运算技术】

应用智能多核流量均衡技术，提升了系统性能。为满足不断增大的网络流量需求提供了妥善的解决方案。

【全面地防止数据泄密】

由于认知程度的限制和侥幸心理的存在，在过去，数据防泄密管理方案的普及十分有限。随着近几年各种数据泄密事件频频曝光，给个人或单位组织造成了声誉和财产上的损失，上网行为管理在数据防泄密方面的优势逐渐被重视起来：事前预防（过滤与控制技术、异常行为预警）、事发拦截（异常流量拦截、敏感内容过滤）、事后追踪（日志记录）。数据防泄密功能帮助用户有效减少泄密风险。

【强有力的安全防护能力】

作为管理产品，特别具有对网络威胁的识别和防御技术，一方面对网络威胁的防御（如防止 DOS 攻击、防 ARP 欺骗）能保护产品本身的稳定安全，进而保障网络可靠性；另一方面识别并拦截网络中的异常流量，可以避免威胁扩散而给单位组织造成不良影响。

【更智能、更简单的管理】

“设备”应该是“人”的工具！倘若“设备”需要“人”投入大量管理工作、操作，显然倒置。产品准确的统计信息，只对有意义的数据进行统计，生成一目了然的报表，最大化转化上网行为管理日志，降低网络管理员工作量的同时让网络、资源、行为更可控。

【支持旁路侦听、防火墙、网桥三种工作模式】

内置防火墙模式、网桥模式、旁路侦听模式三种工作模式，保证了产品可以适合任何网络结构进行网络监控，还可以基于 IP 地址跨网段、跨 VLAN、跨平台、跨路由、跨交换机对互联网信息进行全面控制管理，彻底解决了同类软件不能对 ICMP 协议和 UDP 协议进行监控的难题。

【优秀的构架设计及模块化设计保证高扩展性和高品质】

优秀的设计构架及高度的模块化设计保证了可移植性和稳定性，其先进的设计思想被融入整个产品的设计研发中，该软件从核心层到应用层与同类相比都具有明显的优势，特别是在带宽控制、邮件审计、聊天审计、页面审计、内容过滤等功能上表现出卓越的性能和优秀的品质，这一切均源于专业的技术底蕴和领先的技术优势，同时其强大实用的功能和简洁易用的界面保障了高效使用。

功能特点



完整的用户认证体系，认证/权限管理，用户/用户组分类管理

认证管理	<ul style="list-style-type: none"> ◆支持 WEB 认证、USBKEY 认证、IP/MAC 认证、PPPOE、L2TP 认证； ◆支持批量导入用户，支持系统自动搜索局域网用户并按组归类； ◆支持 WINDOWS 域用户登录、POP3 用户登录、WEB 页面用户登录等自动与设备连接，创建用户并管理，比如用户登录指定的邮箱就可以完成在设备上的认证； ◆拨号用户支持 RADIUS 认证，如 PPPOE、L2TP 用户账号通过 RADIUS 管理，上网权限通过设备进行管理。
权限管理	<ul style="list-style-type: none"> ◆可配置实名用户登录方式，可配置所属组，可配置过滤策略、审计策略、提醒策略，可配置流控策略，支持 TCP、UDP 会话数管理，指定外网口。
用户组管理	<ul style="list-style-type: none"> ◆根据组管理的用户网段，自动产生用户归属组、继承组、过滤策略、审计策略、应用流量策略、提醒策略等； ◆自动创建本地用户功能，自动创建的用户可以进行编辑、分配权限、修改名称等。



精准识别 URL 网址，各种应用程序，有效控制 IP、端口、关键字、网页过滤、文件下传下载能多项类别

控制类别	<ul style="list-style-type: none"> ◆IP/PORT 控制，关键字控制，对 HTTP 上传数据进行关键字过滤，上传下载文件类别过滤，聊天软件账号过滤（QQ、MSN、飞信）。
URL 类别控制	<ul style="list-style-type: none"> ◆只允许访问包含关键字的 URL； ◆过滤含有关键字的 URL；是否允许通过 IP 访问网页； ◆基于 URL 过滤库进行分类过滤。
应用程序控制	<ul style="list-style-type: none"> ◆应用程序控制支持 20 多种分类，700 余种应用程序，包括常见的网络聊天软件（QQ、MSN、YAHOO MESSAGE、UC、网易泡泡），各种主流网络游戏如 CS、星际争霸、征途、联众、浩方、QQ 游戏、大话西游、盛大、迅雷游戏等 100 余款游戏，BT、迅雷、电驴等下载工具、PPLIVE、PPS、QQLIVE、风行等 P2P 视频、大智慧系列（国泰君安大智慧、江南证券大智慧）、联合证券、银河证券（同花顺，双子星）分析家、大参考、钱龙等炒股软件、IPHONE、安卓等大量的应用程序； ◆支持 P2P 智能识别，比如对加密 P2P，新的 P2P 程序的自动适应； ◆支持对不可识别程序的管理，比如可以禁止所有不可识别的程序，做到严格控制用户网络使用。



智能策略模板，有效地进行过滤、审计、流量、配额提醒等多项控制

策略模板管理	<ul style="list-style-type: none"> ◆支持过滤策略，审计策略，应用流量策略，配额和提醒策略，每个模板含有多条策略，用户只需选择模板就可以分配属性，每个模板都支持时间段的管理，如控制策略在星期几，每天的什么时间段生效。
--------	--



最领先的流量控制技术，人性化的提醒机制，方便全面管理

用户流控	<ul style="list-style-type: none"> ◆用户的上下行带宽控制； ◆支持智能流控，即根据外网带宽和本地用户数自动分配用户带宽； ◆支持连接数限制。
应用流控	<ul style="list-style-type: none"> ◆可以对用户的各种类别的应用程序进行流控，如限制 BT 下载只能占到用户分配流量的 50%。
流量提醒	<ul style="list-style-type: none"> ◆可以对应用流量，使用时长进行控制，如用户当月看网络视频超出 5 小时或大于 1000M，就发送提醒页面，或者拒绝再使用网络视频； ◆支持每月、每天、本次上线多种时间段；支持多种应用类别组合。



实时跟踪记录网络行为，方便有效审计上网行为

行为审计	<ul style="list-style-type: none"> ◆能够全面详实的记录网络内流经监听出口的网络行为，根据国家有关法规规定保存至少 60 天，以便进行事后的审计和分析。
审计类别	<ul style="list-style-type: none"> ◆可以对 HTTP (GET/POST)、SMTP、POP3、TELNET、FTP、QQ、MSN、SQL SERVER、ORACLE、MYSQL) 等常用协议进行内容记录。如网址及对应的网址分类、FTP 命令/文件目录/文件名以及文件内容，聊天工具帐号及对应的聊天内容、网络游戏的游戏名称、TELNET 命令及端口、P2P 工具等； ◆包括能详细记录电子邮件 (SMTP、POP3、WEBMAIL) 的正文和附件内容，还可记录 WEB 形式的 BBS、新闻评论、微博等论坛发帖、聊天等各种 POST 文字和附件 (明文情况下)； ◆对常用搜索引擎的搜索行为进行记录； ◆记录 QQ、MSN、飞信等聊天工具聊天内容，账号登陆情况； ◆详细记录上传文件的信息，包括完整的文件，可以下载到本地。记录下载文件的文件名，连接地址等信息； ◆可完整记录被过滤策略产生的日志，如被允许或拒绝的应用程序名称、上传的文件名、URL 类别、关键字类别、账号信息等、包括完整的数据包的记录； ◆用户上下线行为日志； ◆能够审计数据库访问行为 (SQL SERVER、ORCAL、MYSQL) 等； ◆对不能识别的网络访问协议，能够记录基本的源和目的、IP、端口、MAC 等信息。



精准的告警提醒机制，多样化的告警方式

行为告警	<ul style="list-style-type: none"> ◆ URL 拒绝时弹出页面告警； ◆ 超出流量可弹出提醒页面； ◆ 支持公告页面。
内容告警	◆ 可以对 HTTP (GET/POST)、SMTP、POP3、TELNET、FTP、MSN、数据库等常用协议和应用进行内容关键字告警。
告警方式	◆ 弹出页面、发送邮件、SNMTRAP、中心平台告警。



智能全面分析统计数据，形成报表，方便管理查询

数据统计报表	<ul style="list-style-type: none"> ◆ 可根据自定义时间，对所有协议的上网情况进行统计，统计类型包括排名，趋势，应用程序，访问资源等，可生成列表，饼状图，以及各种上网情况的分布图。统计条件包括时间类型，报表类型，开始时间，结束时间等； ◆ 对每个用户的网络使用情况进行统计产生报表。
--------	--



强大的企业级 VPN 功能，分别支持 IPSEC、SSLVPN、PPTP 和 L2TP 制式

IPSEC	<ul style="list-style-type: none"> ◆ 支持网关对网关模式； ◆ 支持客户端对网关模式； ◆ 支持 USBKEY 认证； ◆ 支持多路负载均衡； ◆ VPNUSBKEY 认证。
SSLVPN	◆ SSLVPN 通过虚拟桌面可以支持各种应用。
PPTP	◆ 用户支持用户管理，支持 RADIUS 认证。
L2TP	◆ 用户支持用户管理，支持 RADIUS 认证。



强大的防火墙功能，特别具有对网络威胁的识别和防御技术

防攻击	◆ 有效抵御各种 DoS/DDoS 攻击，可识别和防御 syn flood、icmp flood、udp flood、tcp scan、udp scan、ping sweep、teardrop、land、ping of death、smurf、winnuke、圣诞树、tcp 无标记、syn fin、无确认 fin、松散源路由、严格源路由、ip 安全选项、ip 记录路由、ip 流攻击、ip 时间戳等攻击。
入侵检测	◆ 具备独立蠕虫过滤功能，对 sobig、ramen、welchia、agobot、opaserv、blaster、sadmin、slapper、novarg、slammer、zafi、bofra、dipnet 等主流蠕虫病毒的识别、过滤和拦截。



集中端管理，极大地方便管理员集中管理设备

中心集中管理	◆支持多个设备接入一个中心平台进行集中统一管理，中心能够对设备镜像状态的监管，实时查询各种日志，和统计数据，实时进行控制策略的下发，实时进行报警条件的设置下发等功能；
	◆设备能够统一告警到中心平台；
	◆审计数据能够自动备份到中心平台。



人性化的管理界面，通俗易懂的菜单设计，方便进行设备管理配置

系统资源监控	◆监控 CPU、内存、磁盘占用率；
	◆外网口流速信息；
	◆应用类别的总流量分布，最近 10 分钟流量分布；
	◆当天邮件数、聊天数量、发帖数量、外发文件数量等；
用户状态监控	◆支持通过 SNMP、SNMPTRAP 方式向外部提供接口状态，CPU、内存、存储状态等信息。
	◆在线用户列表，包括登录方式、在线时间、所属组；
	◆用户流速排名，包括上下行流速，TCP、UDP 连接数；
	◆总应用流量，各种应用类别的流量，流速；
登录安全	◆用户的每种应用类别的流量、流速、占用时长；
	◆用户当前连接信息包括 IP、端口、应用类别。
审计信息管理	◆支持多管理员，管理员权限可设置，管理员登录系统时只显示他具有权限的页面，不具有权限的页面不显示；
	◆支持特定 IP 管理，限制非法登录次数。
	◆支持远程 FTP 备份；
	◆支持远程 SYSLOG；
弹出页面管理	◆支持数据库自动清空早期数据；
	◆支持数据库占用比例过大时邮件提醒。
加密登录	◆自定义公告页面；
	◆自定义拒绝页面。

技术参数

功能特性:

输入电压范围: AC160V-230V/50-60Hz
管理用户数: 150 (可增加)
VPN 用户数量: 200 (可增加)
最大并发会话数: 50000
接入方式: 网关、路由、网桥、旁路接入

体积:

体积: 430×301×44.4mm
重量: 3Kg
外壳封装: 标准 1U 机箱设计 19 寸机柜的安装方式


接口:

LAN 口: 3 个 1000M (RJ45)
WAN 口: 2 个 1000M (RJ45) WAN2 也可做 DMZ 口, 与 DMZ 口是相同口
DMZ 口: 1 个 1000M (RJ45) 也可做 WAN2 口, 与 WAN 口是相同口
RESET 键: 按住 5 秒密码和网关 IP 回复出厂值
(注意: 不同型号对应的接口数量也不同, 这里依 DLK-S850 和 DLK-R8100 列写)

环境:

工作温度: -30℃~70℃
存储温度: -40℃~80℃。
湿度: ≤90%

型号规格

序号	型号	最大用户	接口
1	DLK-S850	支持 50 个内网用户	3 个千兆 LAN, 2 个千兆 WAN 口, 1U 机箱
			
2	DLK-S8100	支持 100 个内网用户	3 个千兆 LAN, 2 个千兆 WAN 口, 1U 机箱
			
3	DLK-S8300	支持 300 个内网用户	1 个千兆 LAN, 3 个千兆 WAN 口, 1U 机箱
			
4	DLK-S8500	支持 500 个内网用户	1 个千兆 LAN, 3 个千兆 WAN 口, 1U 机箱
			
<p>注：大于 500 用户数量设备也可提供，详细信息欢迎前来咨询，谢谢！</p>			