擎企上网行为管理应用系统
产品白皮书

北京擎企网络技术有限公司

2017 年 1 月

版权声明

说明：

下面文档中如果没有特别说明，公司指的是北京擎企网络技术有限公司，产品指的是擎企上网行为管理应用系统产品。

免责条款

信息反馈

如果您有任何宝贵意见，请反馈：

地址：北京市海淀区中关村南大街 48 号，九龙商务 C 座 4017,4018 室

邮编：100084

电话：010-58483126

传真：010-62386781

您也可以访问我们的网站 www.qqinet.com：获得最新技术和产品信息

目 录

第1章 产品价值

1.1 阻制与工作无关的流量，防止对带宽的滥用

对那些与企业工作无关且会消耗大量带宽的信息流，如 P2P 下载、网络视频、娱乐信息流、可疑数据流等进行必要的限制 ,减少其对网络资源的占用 ,提高企业员工与办公业务的上网速度。

1.2 保障关键应用的稳定运行，确保重要员工顺畅地使用网络

支持多种智能带宽保障模式，满足关键业务（VPN、ERP、OA、视频会议、邮件等业务）与重要员工的带宽保障需求。动态保障这些业务与员工所需的带宽，在其需要使用网络时得到带宽的保障，优先使用网络；在其空闲的时候，带宽可以被其他业务或者员工使用。在不增加带宽的前提下，提升被保障业务与员工访问互联网的质量与速度。

1.3 管理员工上网行为，提高员工网上办公的效率

禁止员工在上班时间用网络聊天、炒股、玩游戏等，提升员工的工作效率。提供员工上网行为分析报告，方便管理部门了解员工的工作效率和上网行为规律。

1.4 网络实名制，将网络的行为准确定位实际人员

建立网络实名，有效区分用户，是部署差异化授权和审计策略、有效防御身份冒充、权限扩散与滥用等的管理基础。网络实名也是事后对内容追溯，定位问题根源的重要根据。

1.5 依照法规要求记录上网日志，避免违法行为

实施全面的上网行为管理，使网络安全建设符合国家对企业使用互联网的管理规定（《公安部令第 82 号》）。详细记录常见的互联网交互信息、做到发现问题有据可查。禁止员工访问违法网站，防止员工在发帖、网络聊天中包含违法言论，降低企业的法律风险。

1.6 保障内部信息安全，减少泄密风险

实时监控网络外发的信息，发现可能的与商业或研发机密有关的信息外泄，及时阻断并予以警告。详细记录邮件，网页浏览与搜索，微博、博客、论坛发帖，各种聊天消息及 FTP、Telnet 控制命令信息，并可对其审查。实现事先防范、事中警告，事后追查。实现全方位保障内部信息安全，减少机密外泄风险。

1.7 内置企业级路由器与防火墙，降低安全风险

产品开创性的在行为管理产品中采用应用防火墙 ACL（访问控制策略），可以有效的保障企业网络免遭互联网的攻击，增强网络安全防护能力。设备支持 SNAT,DNAT,支持静态路由，策略路由，OSPF 等路由协议，可以完全代替用户的出口路由器和防火墙。

1.8 专业负载均衡 ，提升多线路的使用价值

确保企业网络及应用的可用性，提高上网访问速度，减少服务器负载与管理复杂度，降低企业的带宽成本。可以按照源地址，目标地址，域名，以及应用进行智能选录

1.9 全面透视网络流量，快速发现与定位网络故障

从整体、应用、员工多个角度透视网络流量。通过对出口带宽利用率、应用流量排名、员工流量排名、网络的质量、连接成功率、数据重传率等反映网络真实状况等数据与指标的分析，通过几次鼠标点击操作就可以快速定位到出现异常或故障的主机或应用 ,同时为设置流量管理策略提供依据。

1.10 帮助网络优化与规划，提供决策支持

具有全面的历史趋势分析与决策支持能力，为网络管理、优化与规划提供科学的依据。

1.11 综合多种功能于一身，大大简化网络部署，减少企业成本

产品集流量分析、带宽管理、上网行为管理，路由器，防火墙，IPSEC-VPN，SSL-VPN、负载均衡，服务器流量管理等多种功能于一身，全面满足用户出口设备的需求。

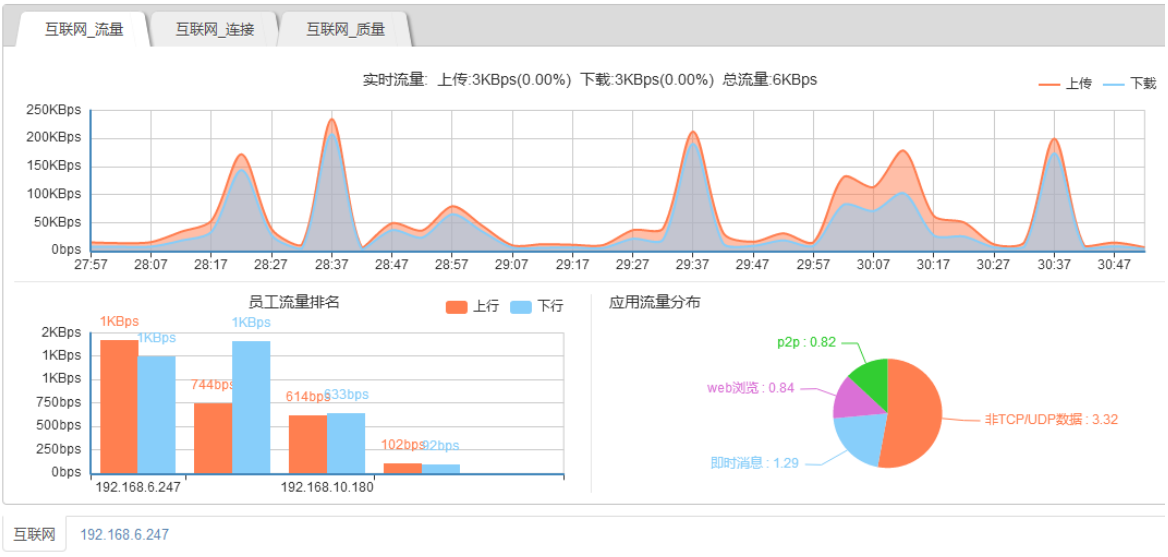
多个功能合成一体，可以大大简化网络部署与能耗；减轻网络管理人员的运维负担；显著减轻企业的拥有成本。

第2章 功能简介

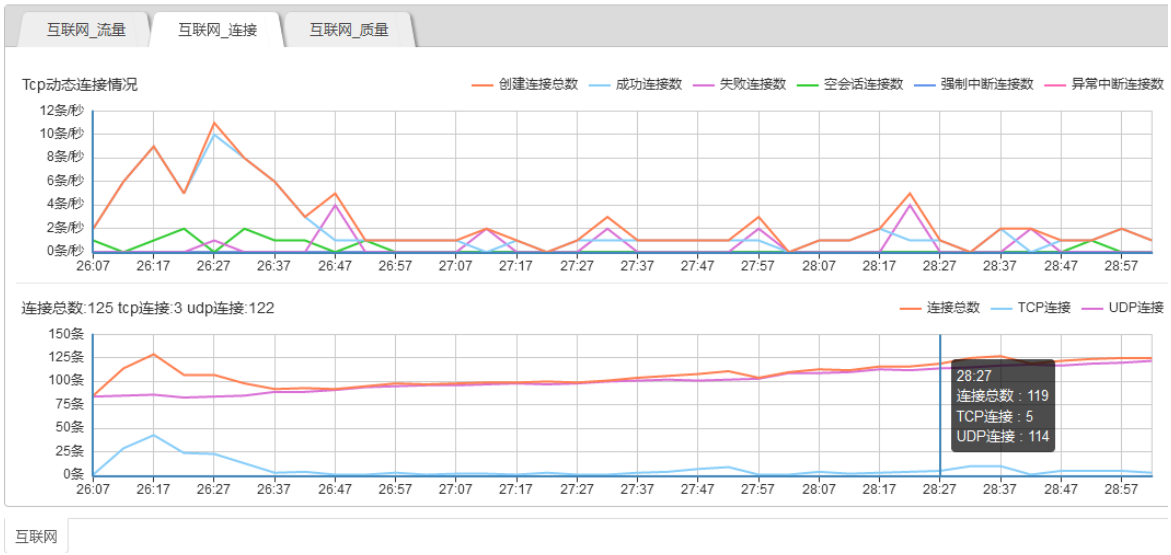
2.1 流量分析

全面透视网络应用，快速发现网络问题，迅速定位网络故障。

- 可以实时了解当前网络流量是多少？占用网络带宽的比例是多少？
- 可以实时知道全网流量最大的是哪些应用？全网流量最大的用户是哪些？
- 可以实时发现网络的主要数据流量流向哪里？主要使用了哪些端口？
- 可以查询应用的访问情况如何？应用网络的质量怎样？连接成功率、数据重传率是多少？
- 可以分析用户、业务应用的运行历史以及预测未来的发展趋势。
- 可以准确、快速定位到异常流量的主机或应用。



图表 2-1 整体流量图



图表 2-2 并发连接数分析图

2.2 带宽管理

保障关键应用和重要人员的上网带宽，限制 P2P 等无关应用的带宽，保障网络通畅。

- **保障重要人员和关键应用的带宽**

对需要一定带宽的重要人员和关键应用，如单位核心成员、视频会议、ERP 系统，分配一定的保障带宽，从而确保这些重要人员顺畅地使用网络，保障关键应用的稳定运行。

- **限制无关应用**

对那些与单位工作性质无关或者会消耗大量带宽的信息流，如 P2P 下载、网络视频、娱乐信息流、可疑数据流等进行必要的限制，减少其对网络资源的占用。

- **公平分配带宽**

通过制定基于应用、个人、部门的网络资源分配策略，可以防止因个人主机中毒而导致整个网络瘫痪，同时保证每个人都能平等使用网络（关键人员和关键应用除外）。

- **识别阻断网络攻击**

根据并发连接数可以确定并且阻断 DOS/DDOS 攻击等异常行为，保护网络设备安全。

- **优化动态保障技术：**

2-4 保障通道设置界面

本系统在保障重要人员和关键应用带宽的时候有三种方式：1.静态保障， 2. 一般动态保障，3. 优化动态保障。 根据不同的应用方式，使用不同的优化策略，可以大大优化网络带宽：

- **静态保障**

不管该通道是否有流量，最低保障的带宽都被预留出来。其他通道不能占用，这种保障方式一般给非常关键的应用使用，并且这种应用一般都一直都有流量，例如企业的 VPN 之间的数据传输。

- **一般动态保障**

如果该通道没有流量，则该通道的带宽可以被其他通道使用，如果该通道有流量，则一次性全部给与该通道分配的最低带宽。这种保障方式一般给视频会议使用。

例如我们给视频会议系统分配 2Mbps 的保障带宽。如果没有开视频会议的时候，这个 2Mbps 可以被其他人占用；一旦视频会议系统开始运行（不管实际上使用了多少），则这 2Mbps 其他人都不能占用；视频会议结束后，这个 2Mbps 又立即释放出来给其他人使用。

- **优化动态保障**

是在一般动态保障的基础上做了一个优化。当被保障的应用开始上网的时候，不是一次性分配所有的带宽，而是根据该通道的当前实际使用流量来动态保障带宽，这种方式可以更加优化的使用带宽。这种保障方式最好是给单位重要的员工或者部门使用。

例如我们给单位某员工 A 分配 2Mbps 的保障带宽，如果员工 A 没有上网，这个 2Mbps 可以被其他人占用，如果员工 A 上网，但是只浏览网页占用了 1Mbps 的流量，那么其他人可以使用剩余的 1Mbps 的带宽。

2.3 行为审计

2.3.1 日志记录

近年来，一方面随着国家为了净化互联网环境，逐步建立对互联网行业发展的市场规范，监

管力度不断增强，另一方面，组织出于自身信息安全保护的需求如防止信息资产泄密、预防舆论风险、保留安全事件的相关证据，以及管理上的要求，如考核员工的网络工作效率、分析网络应用情况、提供管理依据等，对于行为记录方案的需求日益明确。

内网用户的所有上网行为本产品都能够记录以满足公安部 82 号令的要求。产品可针对不同用户(组)进行差异化的行为记录和审计，包括网页访问行为、网络发帖、邮件 Email、IM 聊天内容、文件传输、游戏行为、炒股行为、在线影音、P2P 下载等行为，并且包含该行为的详细信息等。

近年来信息防泄密方案备受组织管理员关注，内网员工无意或有意将组织机密信息泄露到互联网甚至竞争对手，或向论坛 BBS 发布不负责的言论、网络造谣等，将给组织带来泄密和法律风险。产品不仅能基于关键字过滤、记录员工通过 Mail（包括 Webmail）、BBS、Blog、QQ 空间等发布的网络言论，还支持实时报警功能。

对于使用 HTTP、FTP、mail 等方式传送文件所引发的风险（如将研发部的核心代码发送出去），首先本产品可以禁止用户使用 HTTP、FTP 上传下载指定类型的文件，对于上传的文件产品也可以全面记录文件内容，做到有据可查。

序号	时间	员工姓名	源IP	发件人	收件人	标题	邮件大小	附件	附件名	目标IP	源MAC	目标MAC	源端口	目标端口
1	2017-03-10 11:03:59		192.168.6.249	luoyz@qqinet.cn	909850783@qq.com	擎企网络流量综合管理系统-产品白皮书	9036KB	2	擎企网络流量综合管理系统-产品白皮书.doc;擎企网络流量综合管理系统(v4.0).ppt	42.120.219.29	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	62718	25
2	2017-03-10 10:47:02		192.168.6.249	luoyz@qqinet.cn	307317536@qq.com	转发：擎企网络流量综合管理系统-产品白皮书	9037KB	2	擎企网络流量综合管理系统-产品白皮书.doc;擎企网络流量综合管理系统(v4.0).ppt	42.120.219.29	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	59872	25
3	2017-03-10 10:39:25		192.168.6.249	luoyz@qqinet.cn	songxuepeng@126.com	擎企网络流量综合管理系统-产品白皮书	9035KB	2	擎企网络流量综合管理系统-产品白皮书.doc;擎企网络流量综合管理系统(v4.0).ppt	42.120.219.29	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	59105	25
4	2017-03-09 15:43:39		192.168.6.249	luoyz@qqinet.cn	yang_yan_guang@126.com	擎企网络流量综合管理系统-产品白皮书	9035KB	2	擎企网络流量综合管理系统-产品白皮书.doc;擎企网络流量综合管理系统(v4.0).ppt	42.120.219.29	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	55808	25
5	2017-03-07 21:44:35		192.168.10.193	resume@quickmail.51job.com	zhuzhp@126.com	(51job.com)申请贵公司c/c++高级工程师（北京）- 肖云龙	286KB	1	resume.html	123.125.50.23	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	59833	110
6	2017-03-07 20:59:34		192.168.10.193	news@mail1.hua.com	zhuzhp@126.com	先先生 3.8女人节到了，这一天，，值得送她们一束鲜花：妈妈、、爱的她，女神	12KB	0		123.125.50.23	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	57912	110
7	2017-03-07 19		192.168.10.1	resume@quickmail.51job	zhuzhp@126.com	(51job.com)申请贵公司信息安全/网络安全/技	77KB	1	resume.html	123.125.50.23	34-6A-C2-0D-10-A8	40-E0-00-B4-71-BD	54468	110

2.3.2 报表分析

大型组织可能在短短 60 天就产生数百 G 行为日志，仅仅实现日志的海量审计尚不足以帮助组织管理员透彻了解网络状况，而通过本产品独立数据中心丰富报表工具，管理员可以根据组织的现实情况和关注点定制、定期导出所需报表，形成网络调整依据、组织网络资源使用情况报告、员工工作情况报告，等。报表工具主要包括：

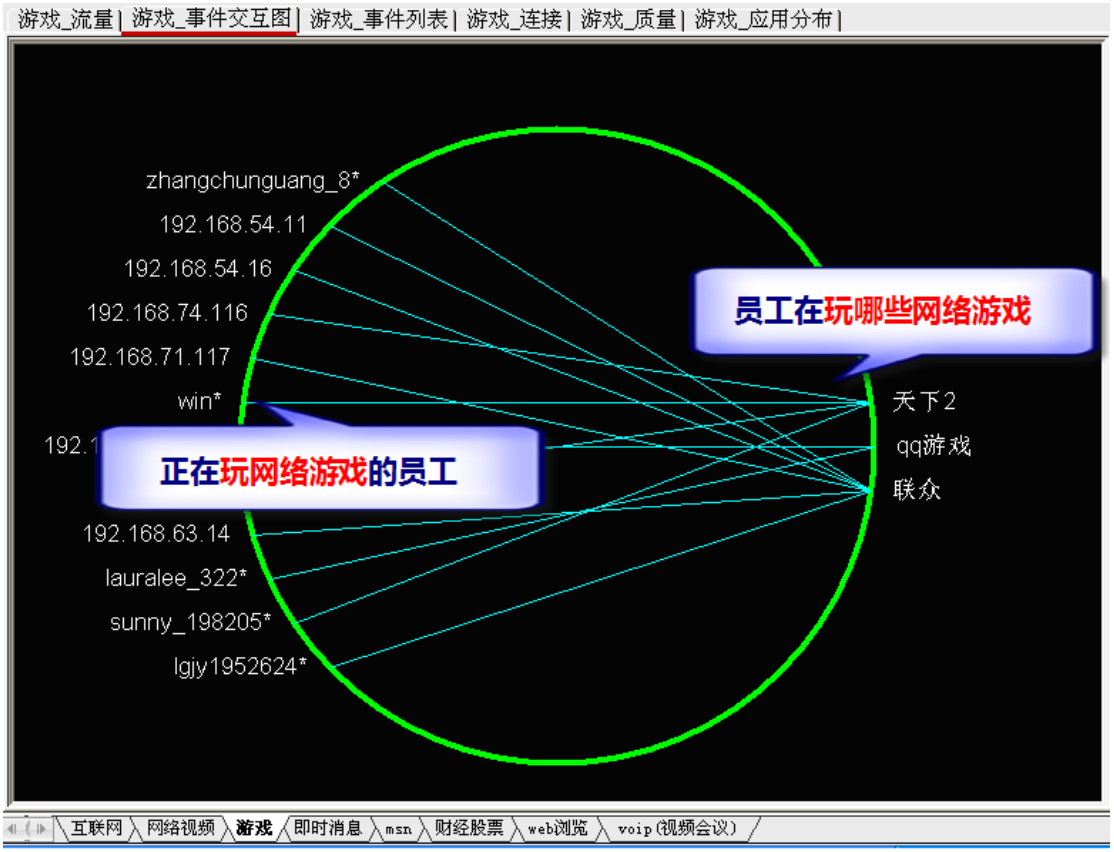
- 内置超过 60 多种报表模板，并支持自定义报表，管理员可手动设定时间、用户对象、应用对象、报表周期等；
- 对比报表：汇总对比、指定用户组/指定用户的对比、指定时间的对比等；
- 统计模板：上网流量/行为/时间统计、病毒信息统计、关键字报表、网络热帖报表、热门论坛报表、外发文件行为报表、危险行为报表；
- 智能报表：管理员可手动设定基于行为特征的风险智能报表，如离职风险报表、工作效率报表、泄密风险报表、异常思想倾向报表，等；
- 趋势：流量趋势、行为趋势、IM 趋势、邮件趋势、炒股趋势等；
- 查询工具：流量查询、行为查询、时间查询、病毒日志查询、安全日志查询、操作日志

查询等；

- 内容检索：网页搜索、邮件搜索、IM 搜索、关键字搜索、Webmail/BBS 搜索等

2.4 上网行为管理

规范员工上网行为；保障单位内部信息安全；规避单位法律风险；提高员工工作效率



2-2 网络事件交互图

- **上网行为分析**

提供数十种统计报表，可以对单位、部门、个人的上网流量、上网时间、网站访问、邮件收发、聊天信息、财经炒股、网络游戏等网络行为进行分析。

- **上网行为控制**

简单易用的七层 ACL。可以设置任意时间段内禁止员工使用某种网络应用，例如禁止员工

在上班时间上网炒股、游戏、P2P 下载等。同时可以通过设定非法网站的 URL 关键字，让您轻松阻断公司员工访问非法或违规网页。通过上网行为控制，可以提高员工的工作效率和规避法律风险。

2.5 安全防护（企业级状态防火墙）

2.5.1 七层 ACL 防火墙

设备内置基于状态检测技术的企业级防火墙，对进出组织的数据包提供过滤和控制。公司开创性的将 7 层 ACL 引入到上网行为管理产品中，支持 ASPF。 ASPF（application specific packet filter）是针对应用层的包过滤，即基于状态的报文过滤。它和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过。

2.5.2 防攻击

设备可以有效的阻止 SYN Flood，UDP Flood，ICMP Flood，UDP Fraggle，DNS Query Flood，tearDrop ,Lan 等攻击，保障内网的安全。

2.5.2.1 异常流量控制

随 U 盘等潜入组织内网的木马、间谍软件等为了隐藏自己 ,通常会通过常用的 TCP 80、443、25、110 等端口泄漏内网机密数据及接受黑客控制。传统设备防火墙等解决方案在开放了常用端口后并不能识别该端口中传输的数据及内容 ,组织的信息资产安全如何保障？黑客远程控制内网终端形成僵尸网络如何避免？设备的异常流量感知技术能够识别常用端口中的如上异常流量，并能够实时报警，帮助 IT 管理员掌控您的网络，防范风险。

2.5.2.2 无线热点发现

随着无线移动互联网的迅速发展，智能手机、平板电脑等这些移动终端愈来愈流行，但由于 iPad 等智能终端只能采用无线网络来上网，有些员工出于便捷考虑可能自己在工位旁私自拉一些无线 AP，在公司通过无线 AP 到公司网络出口，而且这些 AP 由于安全措施薄弱，极容易被外人破解，可能导致内网暴露，信息安全遭受威胁。通过设备的“无线热点发现”功能，可以帮管理员找到内网违反公司规定安置的无线 AP，并可以对这些热点进行拒绝封堵。

2.6 IP 地址管理

杜绝随意更改 IP 地址导致的网络混乱，准确定位故障主机或者问题主机。

2.6.1 IP-MAC 绑定

在二层网络环境下，本系统可以让每台主机的 IP 和 MAC 进行地址绑定。如果绑定的主机修改了 IP 地址，本系统则自动对该主机告警，且该主机也无法再访问网络。

1） 本系统可以让每台主机的 IP 和 MAC 进行地址绑定，不能修改地址。如果绑定的主机修改

了地址，则该主机会自动被告警,而且该主机也无法访问任何网络应用。

2） 本系统还设置了访客区地址，对于访客的地址不进行 IP-MAC 的绑定。这样大大方便的网络管理员对于访客的管理。

3） 如果普通员工将自己的地址改成访客的地址，网络也能够自动发现，并且给该主机发出告警。

2.6.2 ARP 欺骗防护

网络经常遭到 ARP 病毒的袭击，导致网络瘫痪。使用 ARP 欺骗防护功能，可以在根本上抑制 ARP 病毒，保障网络通讯。

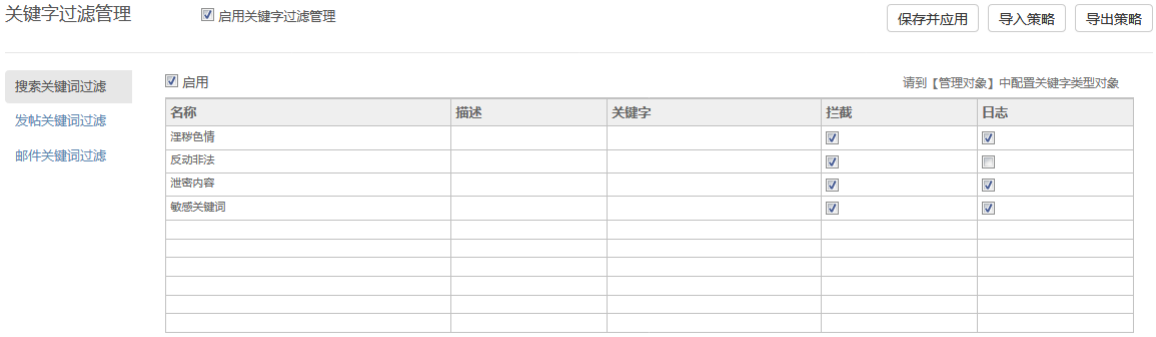
2.6.3 三层交换环境网络下的 IP 地址管理

在三层交换的网络环境中，由于不能得到主机的 MAC 地址，因此不能象二层环境那样做到 IP-MAC 的绑定。但是我们还是可以对 IP 地址进行管理的。我们的管理方法是：

首先通过自动学习，得到目前网络所有主机的 IP 地址。然后选择可以上网的 IP 地址，没有被选中的 IP 地址则不能上网。通过这种方式，也可以限制员工随意的改变 IP 地址。

2.7 关键字过滤

对传输信息进行预先的程序过滤、嗅探指定的关键字词，并进行智能识别，检查网络中是否有违反指定策略的行为。对内容中包含关键词的信息进行阻断连接、和记录并且告警。



2.8 上网认证管理

防止外来人员随意违规接入网络，保障单位的信息安全，降低单位的法律风险

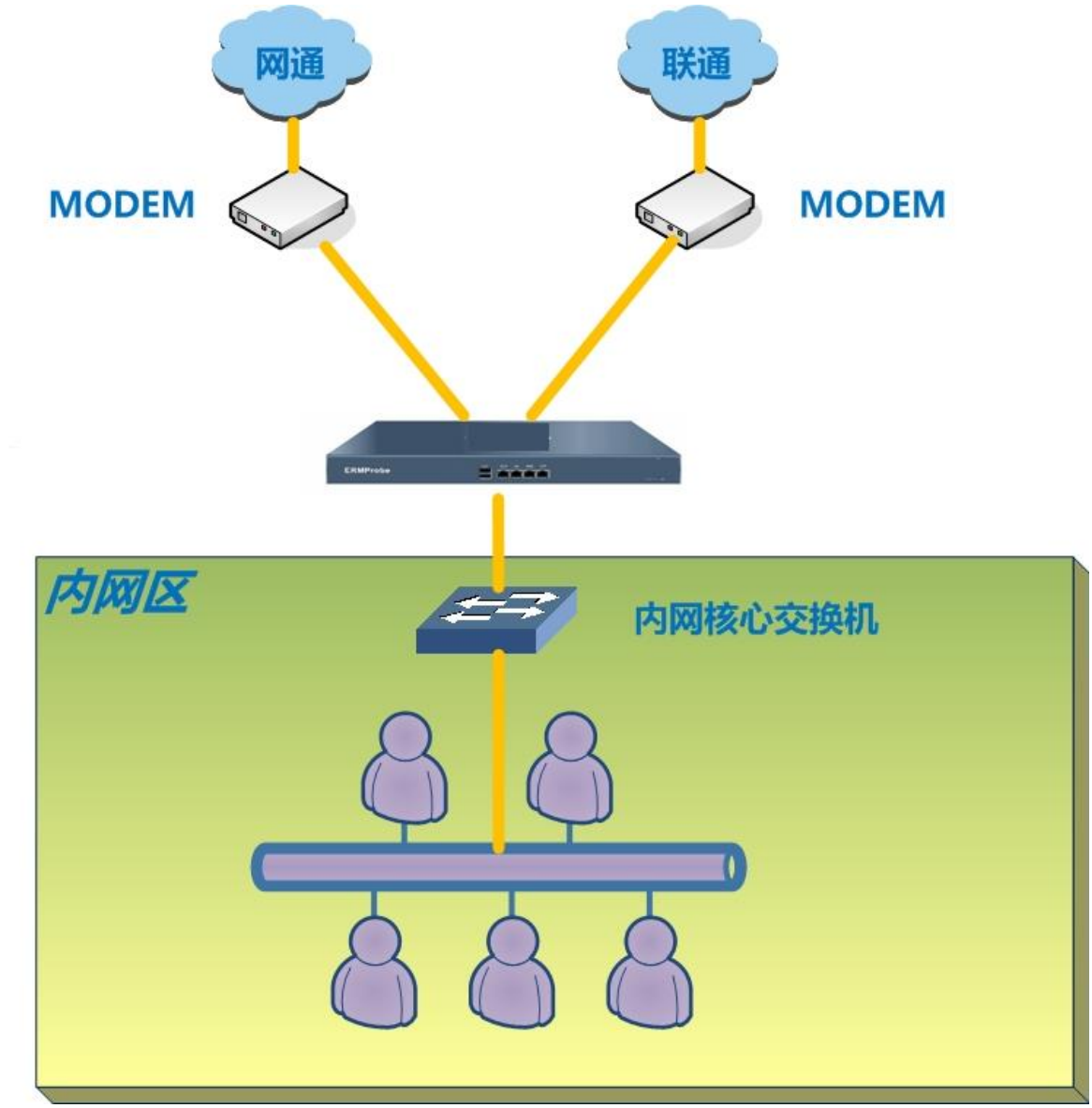
没有严格的认证，就无法有效区分用户，也就无法部署差异化流量控制和审计策略。

本系统可以存储用户名/密码信息 ,也可以与单位现有的 LDAP、微软的 AD 域控制器、Radius 服务器、邮件服务器等进行联动；还支持与利用单位的邮件认证系统或者 Proxy 的认证系统来完成上网认证，而无需管理员逐一添加用户帐号，对于上百人甚至上千人的大型网络来说，这个特性是极其重要和必要的。

设备支持也微信认证，短信认证等流动场所使用的认证方式。


上网认证
启动上网认证
保存并应用
导入策略
导出策略
注销所有员工认证
认证方式
认证参数
Web认证
微信认证
短信认证
单点登录
请在下面列表中添加认证方式
序号
认证模式
地址范围
操作
1
web认证
192.168.100.0-192.168.100.200
2
单点登录
192.168.110.0-192.168.110.255
账号来源
本系统数据库
配置认证账号
POP邮件服务器
配置POP服务器
LADP服务器
配置LADP服务器
Radius服务器
配置Radius服务器
认证白名单（以下内网地址无需认证即可上网）
单点认证方式配置
启用单点认证-域方式
配置域认证方式
启用单点认证-POP邮件方式
配置POP认证方式
启用单点认证-第三方Portal
配置第三方Portal认证方式
启动单点认证-数据库服务
配置据库认证方式

2.9 链路负载均衡



国内不同的电信运营商互联网线路互相访问时速度差异很大，为提高访问效率企业通常租用多条不同的运营商的互联网线路。然而存在流量负载分担不均、链路资源利用率低下、网络不稳定等问题。越来越多的企业开始使用负载均衡设备来改善用户体验，提高网络带宽利用率。本系统可以通过智能的互联网线路流量管理和控制技术保证网络持续高效运行。

支持带宽叠加：将多条宽带绑定成一条，降低对网络的投资，以最小的投入获得最高效稳定的网络环境。

支持线路备份：当一条链路出现故障时，可以迅速切换到其他可用链路，保证网络的高可用性和业务延续性。

解决南北互通问题：有效解决了南北因电信、网通的差异导致了普遍存在的“南北互通”问题。

支持多链路负载均衡：高度保证企业网络的稳定性和业务的延续性避免系统宕机、链路中断或拥塞等对企业运营带来不利影响。

拥有多项先进的技术：集 HTTP 压缩，SSL 加速、智能数据压缩、基于内存的高速缓存、TCP 连接复用、单边 TCP 加速等多项技术于一身，减少响应时间，显著改善终端用户体验。

丰富的算法与策略：拥有多种均衡算法和丰富的负载均衡策略，让用户更高效合理的使用网络资源，极大提升链路利用效率，保障业务高效运行。

保障关键业务：支持链路、应用状态监控，支持会话保持，避免业务访问中断，保障关键业务的延续性。

安装部署配置简便：安装简单，部署方便，图形化的配置界面，简单直观，降低用户配置复杂度，便于系统管理和维护。

2.10 企业级路由器

网络已成为企业的重要组成部分，稳定可靠的网络是企业发展的基础，路由器的性能优劣直接决定企业网络的质量。

本系统是我们自主研发的定位于企业网络骨干层的路由功能。其具备以下特色：

高可用性、高可靠性：采用业界先进的设计技术和依托高性能的硬件平台，具备优越的处理性能，保证系统 7*24 小时不间断高负载运行，充分满足用户需求。

接入能力丰富：可同时连接多条线路，支持 ADSL、光纤等多种接入方式。

全面支持路由协议：遵循 RFC 标准和主流的业界标准，全面支持 RIP、OSPF、BGP、IGMP 等路由协议。

运维管理方便：采用全中文的管理界面，操作简单，设置界面人性化，便于用户学习使用，让所有的网络管理员甚至非网络管理员都能够简单轻松的进行管理。

技术领先产品可靠：体系结构先进，设计可靠，业务特性丰富，是企事业单位的最佳选择。

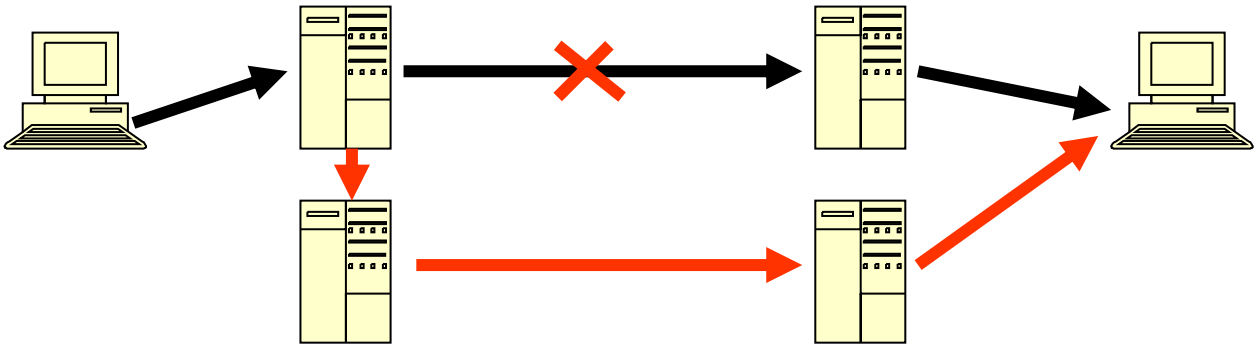
2.11 IPSEC-VPN

2.11.1 多线路互为备份，保证 VPN 稳定运行

为保证 VPN 系统的高可靠性，IPSec VPN 同时提供了两种备份方案。

方案 1：

在两个网络间架设两套 IPSec VPN，正常情况下，数据都是经过主的 VPN 系统传送，如黑色线路所示；但主系统发生故障后，将自动切换到备用系统，无需人工干预，如下图红色线路所



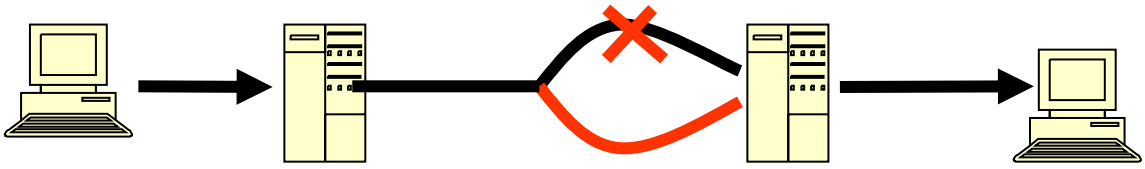
示。

方案 2：

由于 Internet 线路具有不稳定性的特点，使用 Internet 线路存在断线的可能性，对 VPN 网络的稳定运行产生了隐患，因此采用线路备份是一种比较经济的解决方案。IPSec VPN 软件可以支持多达 10 条上网线路。使用该项技术可以保证，当一条线路出现故障后，数据自动倒换

到其他正常的 Internet 线路上，从而保证 VPN 隧道不会因为单条 Internet 线路中断而中断。

如下图所示：



2.11.2 单臂模式下的多线路，更加稳定可靠

单臂模式无需改变用户原有网络结构 ,并因能避免网络单点故障所以成为很多高端客户广泛采用的一种部署方式。但传统的 IPSec VPN 由于技术等原因无法在单臂部署下实现和网关模式同样的多线路功能，构建的 VPN 网络的稳定性和可靠性就无法通过多线路强大的功能来保障，并严重降低了用户应有的 IPSec VPN 使用价值。

IPSec VPN 支持单臂模式下的多线路，通过与前置网关设备的配合，使 VPN 单臂部署就可实现在网关模式下多线路的全部功能 ,在单臂模式部署下仍能为用户提供更可靠、更稳定的 VPN 网络。

2.11.3 断线重连，自动恢复

为了保证 VPN 网络的稳定性， IPSec VPN 内置断线快速恢复技术，在 VPN 连接异常中断后立刻启动检测机制，当网络物理连接恢复正常后，VPN 隧道将在 3 秒钟内自动恢复，从而保证 VPN 网络能够迅速恢复，保证 VPN 网络的高可用。

2.11.4 冗余容量设计，应对突发

IPSec VPN 产品的设计容量大大超过一般用户的实际容量。VPN 软件设计容量最高可支持

500,000 条隧道，这种冗余容量的设计保证 VPN 网络即使遇到业务突发高峰，也能稳定运行。

2.12 SSL-VPN

2.12.1 多虚拟 IP 池支持

通过产品 IP Tunnel 技术可以完美支持 IP 层以上的所有数据。为了让用户更好的使用 IP 资源，IPTunnel 必须获得相应的虚拟 IP 才可以正常的工作。但是对于一些大型的集团公司来说，已经规划好了 IP，需要实现根据远程接入的 IP 来实现身份的绑定，产品可以针对每个人绑定固定的虚拟 IP，从而实现用户身份与虚拟 IP 的绑定。如果对于用户接入没有那么严格的要求，但是对于集团内部各个部门已经规划好了 IP 段，为了实现通过 IP 段来区分不同的部门，产品可以实现用户组与 IP 池的绑定。

2.12.2 强化的网络防护－VPN 虚拟专线功能

虚拟专线指用户登录 SSL VPN 以后，和内部业务系统构成一条虚拟的专线，此时用户将不再能访问虚拟专线以外的网络资源。用户一旦启用虚拟专线功能后，一方面外部网络上面的不安全因素无法再对 VPN 系统构成威胁 ,同时也可以避免客户端上的不安全因素造成泄密的可能性，避免因客户端引发的安全隐患，确保内部业务系统的安全性。

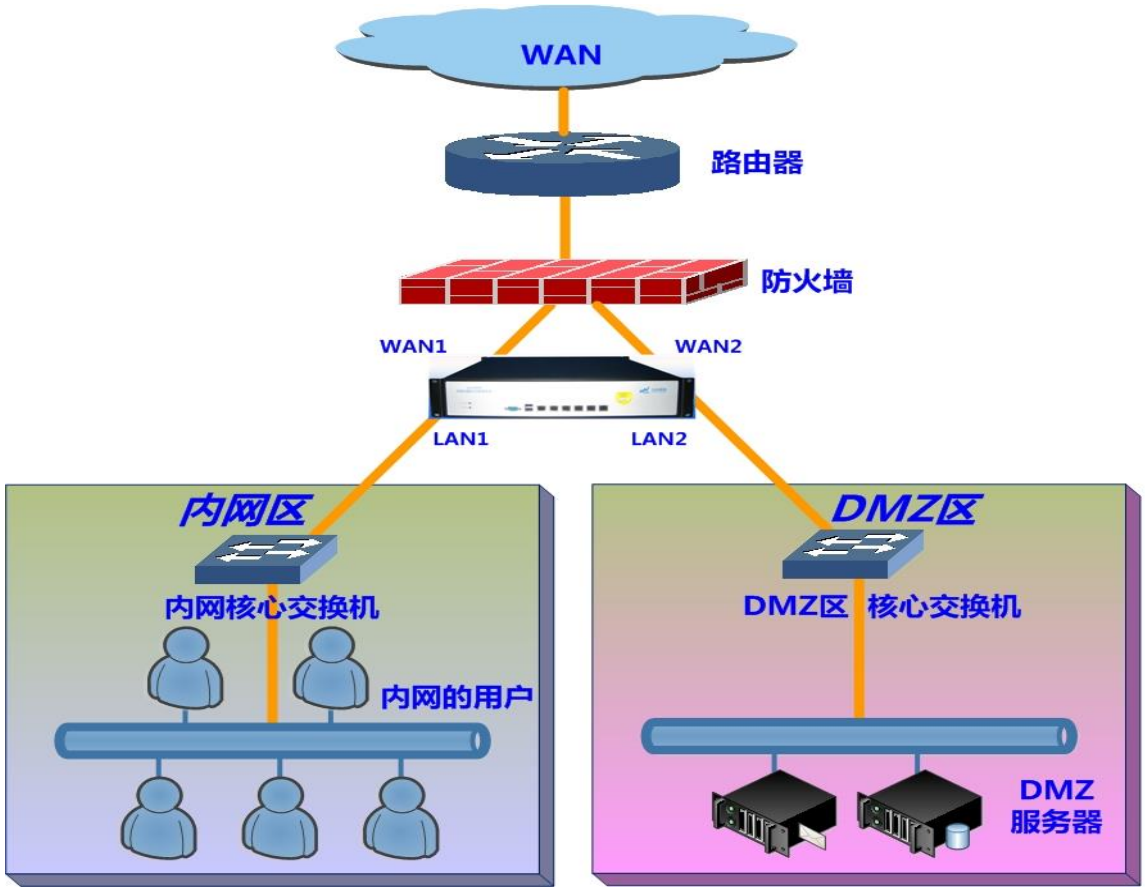
2.12.3 会话自动恢复，提高网络适应能力

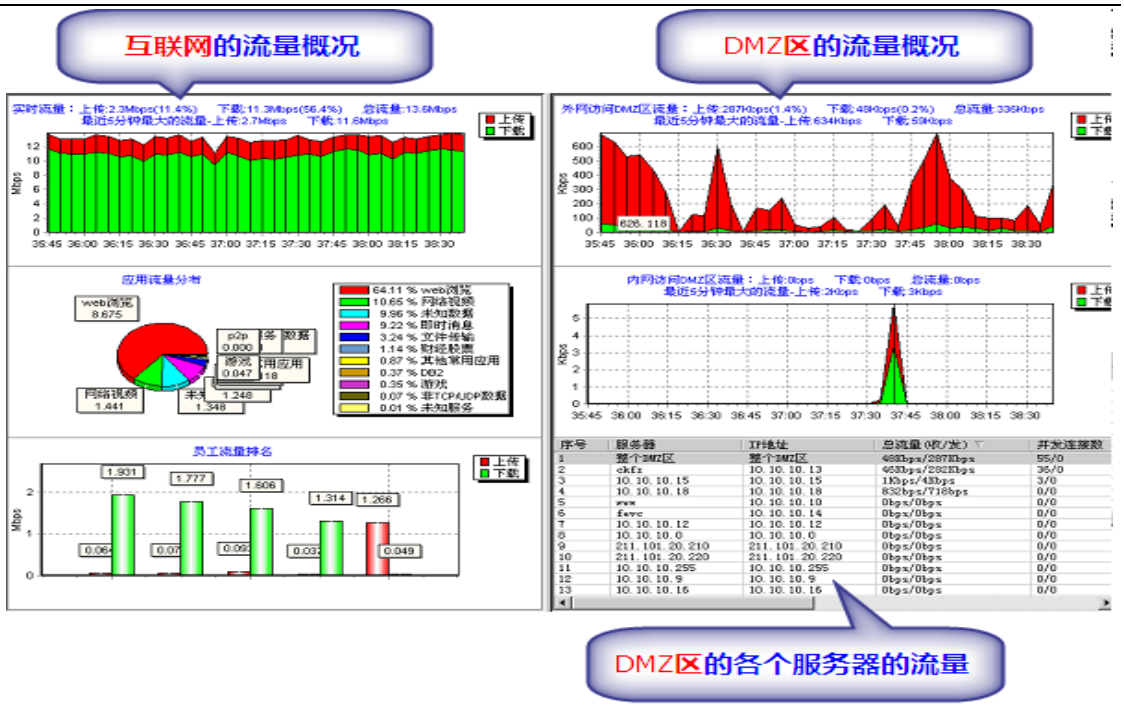
SSL VPN 提供了看门狗提供自动恢复功能和配置备份功能，支持 ADSL 断线重拨功能。若由于线路中断而造成的 VPN 隧道中断，一旦线路恢复， SSL VPN 随即将自动恢复，无需人工干预。

2.13 内网服务器（或者 DMZ 服务器）流量管理

企业将自己的服务器放在 DMZ 区或者放在内网通过地址映射让外网来访问。分析服务器的流量和行为与分析员工上网的流量和行为有很大区别。

产品可以从多个角度，全面的透视外网访问服务器区的整体流量情况，对比 DMZ 区和内网占用带宽的比例情况，为带宽分配提供科学依据。更能透视 DMZ 区中每个服务器的工作情况，及时发现异常工作的服务器 ,定位攻击服务器的攻击源 ,并且能够及时阻断对服务器的网络攻击。





2.13.1 外网访问服务器的流量分析

产品可以从多个角度，全面的透视外网访问 DMZ 区的流量情况。快速发现服务器工作是否正常以及是否遭到各种网络攻击。

- 可以实时了解当前 DMZ 区网络流量是多少？占用网络带宽的比例是多少？
- 可以实时知道 DMZ 全网流量最大的是哪个服务器？
- 可以实时知道某个服务器的对外流量，访问人数。
- 可以实时知道主要是哪些 IP 在访问 DMZ 区 ,他们在访问哪个服务器？他们是从哪里来的？
- 可以查询服务器的访问情况如何？应用网络的质量怎样？连接成功率、数据重传率是多少？
- 可以分析服务器的运行历史趋势以及预测未来的发展。
- 可以准确、快速定位到异常服务器或者外网 IP。

2.13.2 外网访问服务器的流量控制

因为外网访问 DMZ 区和员工上互联网是共享一条带宽的。如何在这两边之间平衡使用带宽，保障两者之间互不干扰就变得很重要。

- **保障某些关键服务器的网络带宽，也可以保障外网某些 IP 访问 DMZ 的带宽。**

对于单位关键的服务器，运行着单位重要的应用。如果外网访问这些服务器的响应速度慢就可能会严重影响单位的形象，甚至会给业务带来损失。产品可以有力的为这些服务器的提供保障带宽，从而确保关键应用的顺利运行。

- **限制某些不重要服务器的带宽，从而节省出宝贵的带宽给其他服务器使用。**

对于单位中某些不是很重要的服务器，例如让外网下载非重要资料的服务器，我们希望这个服务器能够对外提供服务，但是不要占用太多带宽。产品可以准确地控制这些不重要服务器的带宽，从而节省出宝贵的带宽给其他服务器使用。

- **限制外网 IP 的访问流量，保证公平性**

有些外网的 IP 使用某些特别的软件到服务器上访问或者下载内容，导致网络拥塞，也导致服务器特别繁忙。这个时候其他人访问这些服务器就变得很慢甚至访问不了。产品可以让所有的外网 IP 公平的使用网络服务，不会因为一个外网访问者的流量太大而导致其他外网访问者不能进行对这些服务器的访问。

第3章 主要功能列表

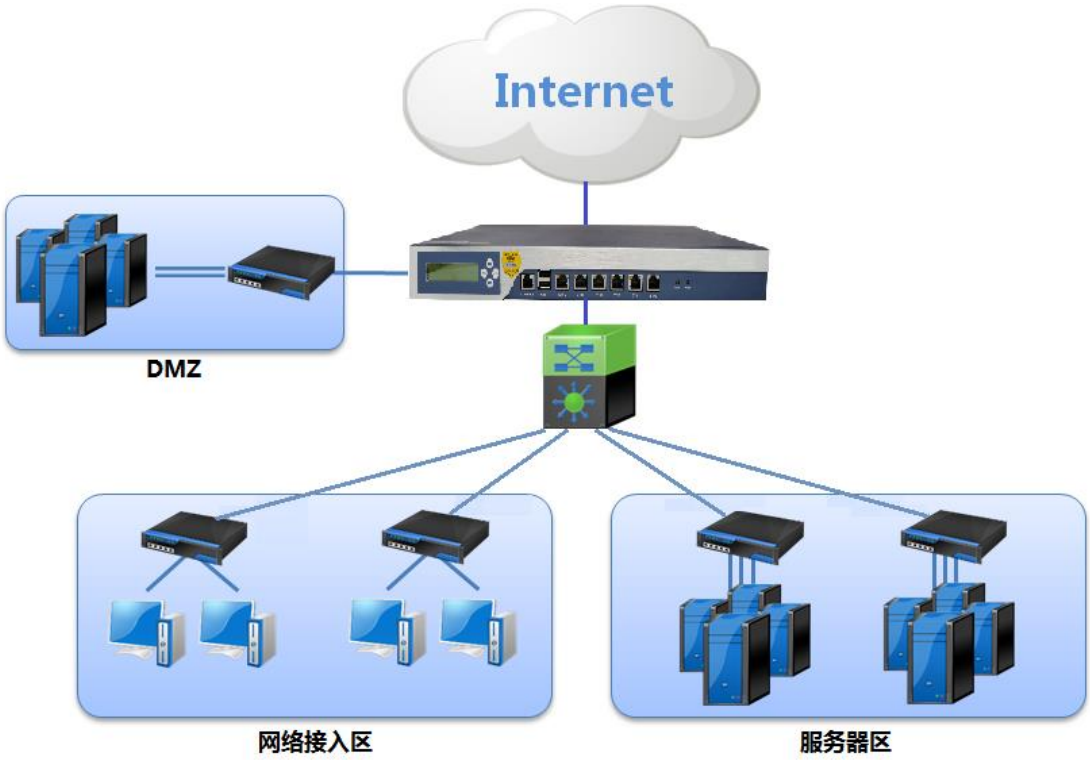
含上网行为管理、上网日志记录、7 层流量控制、防火墙、路由器、负载均衡，服务器流量管理…		
部署方式	支持路由模式	代替以前的路由器或防火墙。
	支持透明网桥模式，支持旁路监听模式	透明模式不改变原有拓扑(保留以前路由或者防火墙)
	支持单卡一号多拨,一卡多拨;支持多 LAN，支持 DMZ 区；	一号多拨,一卡多拨；多 LAN 之间互访控制。
行为管理	能够按照不同的人，不同的时间段进行给员工分配上网权限	禁止员工玩游戏炒股票，使用迅雷和其他 P2P 工具
	完善的 URL 库，禁止员工上班时间上无关或者非法的网站	视频网站，购物网站，交友网站，财务网站，…
	QQ 账号管理	可以禁止某些 QQ 或者只允许某些 QQ 上网
	收发邮件控制	可以控制只能将邮件发送给指定人或者指定邮箱后缀； 可以控制只能从某些邮箱或者邮箱后缀接收邮件；
上网审计	记录员工浏览网页,收发邮件(包括附件），搜索词，论坛发帖	包括记录 URL，发帖内容，搜索关键字
	foxmail,outlook，webmail 收发邮件的审计	记录邮件的收发人，邮件标题，内容，和附件
HTTPS 加密内容审计	支持对使用 SSL 加密协议传输的内容的审计	支持 HTTPS，POPS,SMTPS 等加密内容的审计
关键字过滤	对传输信息进行预先的程序过滤、嗅探指定的关键字词，并进行智能识别，检查网络中是否有违反指定策略的行为。	对内容中包含关键词的信息进行阻断连接、和记录并且告警
流量控制	真正专业级流控设备，流控的效果不是一般的路由器能达到的	7 层的 DPI/DFI 协议识别，支持多达近千种应用； 可以针对不同的人不同的时间配置不同的流控策略；

		可以同时支持 IP，MAC，认证账号和应用进行流控。
7 层（应用层）防火墙	完全包含了一个高性能的企业级状态防火墙的所有功能	开创性的将 7 层 ACL 引入到上网行为管理产品中，支持 ASPF。ASPF（application specific packet filter）是针对应用层的包过滤，即基于状态的报文过滤。它和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过。
防攻击	全面的防止网络的外部攻击，包含网络安全。	有效的阻止 SYN Flood，UDP Flood，ICMP Flood，UDP Fraggle，DNS Query Flood，tearDrop ,Lan 等攻击
IPSEC-VPN	支持多达 50000 路 IP-SEC 会话	支持隧道（tunnel）模式和传输(transport)模式。帮助您构建安全的 VPN
SSL-VPN	支持接入 50000 个 SSL-VPN 终端	帮助单位实现移动 VPN 办公
负载均衡	多 WAN 接入，带宽叠加，智能负载均衡	能够自动按照不同的运营商进行智能选路
	支持按照源或目标地址，应用和域名进行选路	支持会话保持；完美解决网银的负载均衡问题
无线的管理	禁止手机，PAD 等移动设备上网（除了白名单）	一键禁止内网所有的移动设备上网
	二级路由检测和阻断（随身 360 WIFI 检测）	可以检测和禁止二级路由器和随身 WIFI
认证和计费	支持 5 万人同时在线的 PPPOE 服务	支持设定每个账号的带宽，每个账号的共享主机数
	支持多种认证方式，防止违规接入	支持 Web 认证，域认证，LDAP 认证，邮件认证等
统计报表	输出员工的使用互联网的流量和时长统计	还可以自动给管理员发送定制的统计报表
服务器流量管理	通过对服务器流量进行深度分析，提供策略保护服务器免受外部攻击。	分析内网访问服务器流量和质量 分析外网访问服务器流量和质量 控制外网访问服务器流量，防止服务器被攻击。
IP 管理	IP-MAC 绑定，防止 ARP 欺骗，指定主机（IP-MAC)上网	防止违规接入，以及出现问题可以准确定位到人
HA	高可用性	设备支持双机的双主模式以及主备两种模式。

第4章 系统接入方案

4.1 路由模式

产品以路由模式部署在组织网络中，所有流量都通过设备处理，实现对内网用户上网行为的流量管理、行为控制、日志审计等功能。作为组织的出口网关，本产品的安全功能可保障组织网络安全，支持多线路技术扩展出口带宽，NAT 功能代理内网用户上网，实现路由功能等。这个时候产品就代替以前的路由器和防火墙了。



部署方式：

- 产品的 WAN 口与广域网接入线路相连，支持光纤、ADSL 线路或者是路由器；
- 产品的 LAN 口（DMZ 口）同局域网的交换机相连；
- 内网 PC 将网关指向产品的局域网接口，通过产品代理上网。

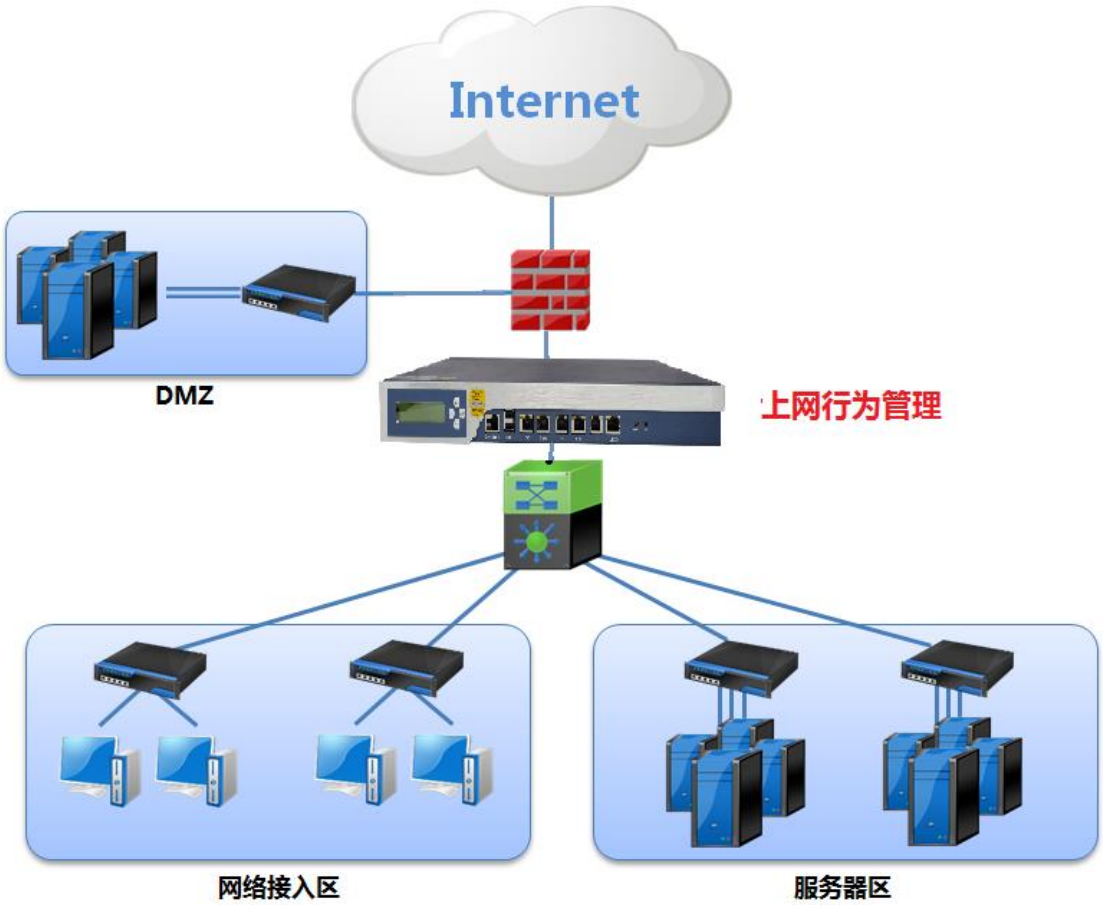
4.2 透明网桥模式

比与其他厂家网桥的突出优势是，我们设备的网桥是真正的透明网桥，不需要给网桥配置任何地址。这种纯透明网桥模式，转发性能最好，安全性最高。

4.2.1 单网桥模式

产品以网桥模式部署在组织网络中，如同连接在出口网关和内网交换机之间的“智能网线”，

实现对内网用户上网行为的流量管理、行为控制、日志审计、安全防护等功能。网桥模式适用于不希望更改网络结构、路由配置、IP 配置的组织。

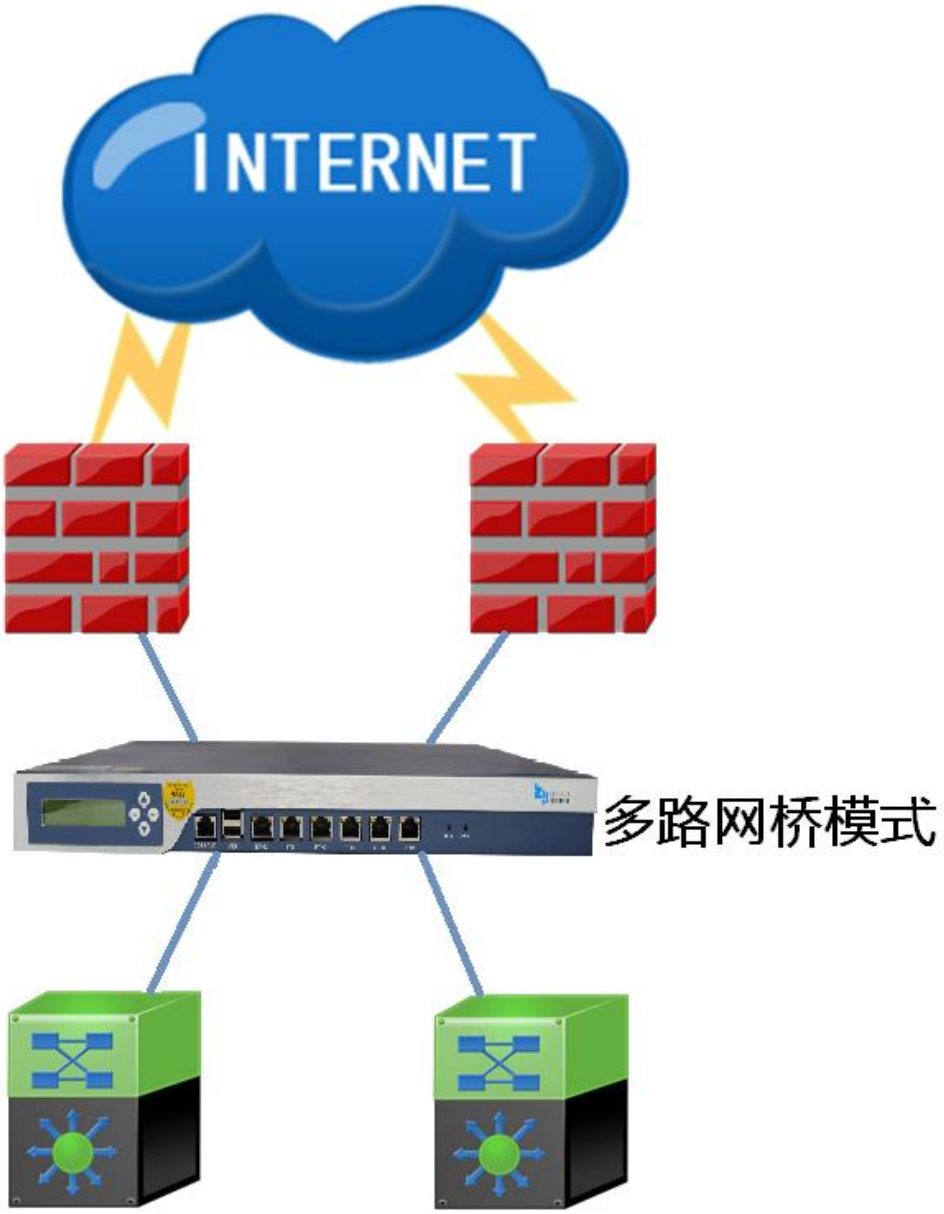


部署方式：

- 产品的 WAN 口连接防火墙或者路由器，LAN 口连接交换机。产品的 LAN 口和 WAN 口不需要配置任何 IP 地址。
- LAN 口（DMZ 口）同核心交换机连接；
- 局域网内的任何网络设备和 PC 都不需要更改 IP 地址。

4.2.2 多网桥模式

组织考虑到网络的稳定性、可靠性，往往采用双机、双线路构建基础网络。设备支持多路桥接模式，适应组织的多机网络环境要求。在不影响原有双机、双线路前提下，对流经设备的所有数据流进行审计、控制、拦截、流量管理等操作。



部署方式：

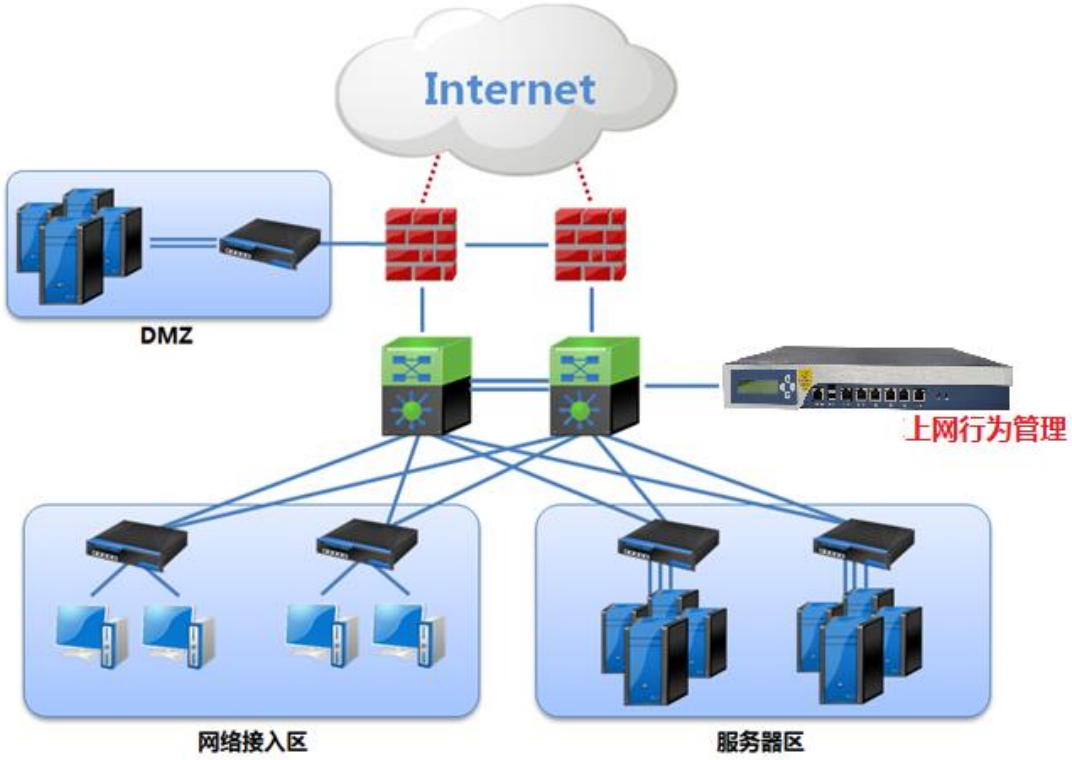
- 通过配置界面，定义两对桥接口（WAN1-LAN1，WAN2-LAN2）；
- 产品的 LAN 口和 WAN 口不需要配置任何 IP 地址。
- LAN 口（DMZ 口）同核心交换机连接；
- 局域网内的任何网络设备和 PC 都不需要更改 IP 地址。

4.2.3 BYPASS

当设备工作在透明网桥的时候，设备支持软硬件 BYPASS。当设备出现故障甚至设备没有接电源的时候，设备只是停止工作，但是用户的网络还是保持通畅，不受影响。

4.3 并联（旁路）模式

产品以旁路模式部署在组织网络中，与交换机镜像端口相连，实施简单，完全不影响原有的网络结构，降低了网络单点故障的发生率。此时产品获得的是链路中数据的“拷贝”，主要用于监听、审计局域网中的数据流及用户的网络行为。

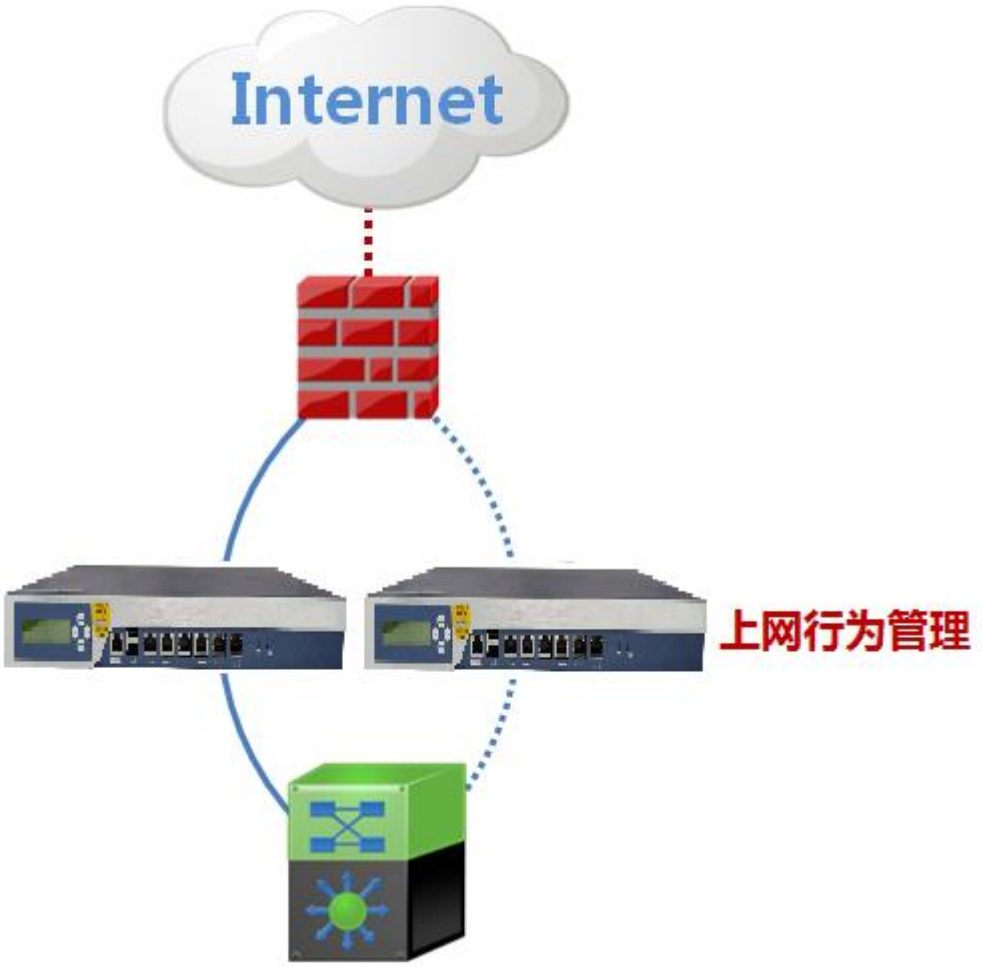


部署方式：

- 配置出口交换机的镜像端口，与产品的镜像口相连，实现对内网数据包的监听。

4.4 双机模式

组织为了网络稳定可靠，同时部署两台设备，支持两台设备以双机模式运行。两台设备通过网线（HA 口）相连，一主一备，当主设备发生故障时自动切换到备用设备，提高网络的稳定可靠性。在这种环境中，设备以单网桥模式或者多网桥模式部署在组织网络中。


Internet
上网行为管理

第5章 公司简介

北京擎企网络技术有限公司是注册于中关村科技园区的高新技术企业，专注于电信和企业领域的网络安全研究。作为业内领先的设备与服务提供商，我们一贯致力于通过提供高品质的产品及卓越的服务，帮助客户提升网络使用价值。

公司拥有一支高素质研发团队，国内安全行业知名专家为技术带头人，核心成员来自华为、中兴、Juniper 等国内外著名的厂商。深厚的专业经验积淀和雄厚的技术实力使公司在应用安全与管理领域处于行业领先地位。

公司一方面注重自有产品的研究，另一方面加强和业内专家的合作，先后和北京邮电大学、北京交通大学，中国科学院、公安部第三研究所等科研所建立了良好的技术合作关系。

公司拥有“电信网络安全产品部”和“企业网络安全产品部”两个独立的安全产品部门，分别专注于运营商和企事业单位。公司在电信领域的安全产品有：宽带业务分析、代理监测、骨干网网络内容审计、宽带业务 QOS 管理等；在企业领域的安全产品有：流量控制，上网行为管理，链路负载均衡，防火墙等。

我们公司是中央政府采购协议供货厂商之一，公司自主研发的多款产品已经入选中央政府“信息类产品协议供货”产品选型采购名录。本产品已广泛应用于政府机关、金融、电信运营商、能源、教育、出版、制造、科研院所、大型集团企业等众多行业。

第6章 附录 A：销售许可证

计算机信息系统安全专用产品

销售许可证

证书编号：XKC60108

有效期：自 2018年 03月 09日

至 2020年 03月 09日

中华人民共和国公安部监制

北京擎企网络技术有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）擎企上网行为管理应用系统 T6500/V3.0 网络通讯安全审计（国标-基本级）安全专用产品进入市场销售，特发此证。

2018 年 03 月 09 日

第7章 附录 B：技术特点

技术特点	描述
深层数据包检测 （DPI）	在网络 2-7 层（Application Layer）上进行数据包特征匹配，使数据包检测更加完备和灵活。
深层流检测（DFI）	通过统计和分析应用的数据流特征，与系统中的数据流模板进行匹配，从而识别各种加密或者动态的应用协议。
动态协议识别	使用了衍生协议识别技术，通过深层数据包检测分析父数据流中的信息识别出该数据流属于哪种协议，同时分析该数据流中的衍生信息，预判子数据流的 IP 地址、协议和端口并对其进行监控，从而识别出整个协议簇的全部数据。
模糊协议识别	模糊协议识别技术对加密的点对点协议识别率超过 90%，在模糊协议识别技术帮助下所有想逃避监管的应用和数据都将无从遁形，这也是我们帮助您管理网络的前提。
SSL 内容识别与管理	设备具有对 SSL 加密内容的完全管控能力，支持识别、管控、审计经由 SSL 加密的内容，如支持基于关键字过滤 SSL 加密的搜索行为、发帖行为、网页浏览行为，审计 SSL 加密行为如邮件发送行为，为组织打造坚固无漏洞的管理。

技术特点	描述
支持 SNMP	带有我们公司的任何产品，均提供 SNMP 等网络管理的 API。用户可以通过 SNMP 把本产品管理功能集中到用户现有的任何基于 SNMP 的管理系统中。
精细速率整形	通过 TCP 速率控制、UDP 速率控制和高级列队技术，共同形成一个平滑、均匀的流动速率，从而最大化网络吞吐率，避免网络拥塞。
TCP 加速	网络时延造成的响应时间减慢很大程度上是因为 TCP 协议在等待确认，本系统的数据流加速技术可以很好的解决该问题。
网络延时检测	通过网络延时分析（TDA），网管人员可以得到精确的网络响应时间数据。本系统将每一个响应时间分成远端网络传输延迟、本地网络传输延时和应用响应延迟 ,从而帮助网管人员定位性能瓶颈所在，发现性能最低的用户和服务器。
多重带宽控制技术	可以将所有用户的带宽控制在一定的范围内 ,同时还能保证某些应用的带宽控制在指定的范围内。
智能专家分析	内嵌智能专家分析引擎，可以对网络资源滥用、网络安全事件、网络性能劣化等事件进行自动告警 ,并且使用预先设置的事件处理策略，主动控制和管理网络中存在的影响关键应用的因素，保障网络的高性能稳定运行。

技术特点	描述
一体化的性能管理解决方案	本流量综合管理系统提供了从上网行为管理、流量分析、带宽管理、智能预警到安全审计的全方位的网络综合性能管理解决方案。它实现了在一个平台内部完成了涵盖当前网管必须的绝大多数功能 ,能够让网络管理人员无需进行大量的数据分析和设备操作，即可对网络进行高效的管理。
电信级硬件平台	设备硬件采用高速网络通信处理器作为核心处理引擎。使用八层 PCB 板的高可靠性设计，使得设备性能出众、稳如磐石。设备采用高速搜索优化算法，数据转发时延极小，满足时间特性要求苛刻的高速网络应用。
智能旁路功能	本流量综合管理系统能够在设备出现故障或掉电时 ,自动闭合网络物理连接，不影响整个网络的使用。本系统全部采用工业化的作业系统，具备 7×24 小时的作业能力，智能旁路设计在即使发生不可预测的故障时亦保证你的网络畅行无阻。
提供 AppFlow 分析功能 ,准确分析业务的 QoS 质量指标	本流量综合管理系统能够提供独创的 AppFlow 信息，在应用层上进行 QoS 指标分析，达到完整的七层应用的服务质量分析，针对性的提供 QoS 保障策略。
支持 VLAN 功能	系统能够根据不同的 VLAN，完成不同的优先级控制，本系统还支持 802.1Q 协议的 VLAN。

技术特点	描述
P2P 业务带宽限制能力	常见的 P2P 控制手段，都仅仅采取简单的阻断，势必造成用户的使用不方便。本系统能够识别出互联网中的 P2P 应用，并对它们进行带宽控制，减轻了网络负担，但是并不阻塞 P2P 应用。
丰富的业务提供能力	针对不同用户不同业务的特征，可以分别提供 CBR（rt-CBR、nrt-CBR）、VBR、UBR 业务，在不具备 QoS 能力的 IP 网络中提供类似专线业务的能力。
基于 AppFlow 的流量识别	可以支持哪些应用业务的区分控制 ,是评价一个带宽管理系统的重要指标之一 ,本流量综合管理系统产品支持数百种通信协议与应用服务，包括 WEB、FTP、POP3、数据库服务、多媒体服务、Microsoft 网络服务等等。可以根据应用场合的不同，灵活的配置，保障某些关键业务，抑制某些非核心业务。
面向应用的行为控制	能够对当前肆虐的 P2P 应用进行正确的引导，限制其资源占用。对常用的 QQ、OICQ、MSN 等聊天工具软件的管理控制，支持常见的 CS 等网络游戏联网控制，支持常见网上炒股软件的识别与控制、支持常用的网络视频识别与控制，支持 BBS、网站访问管理控制，针对应用层面进行网络控制管理，可以定制应用层管理策略，轻松管理网络用户的上网。

技术特点	描述
分布式协同处理	在日益复杂的网络环境中 ,单纯在网络出口进行流量管理已经难以彻底解决问题。本系统支持全网分布式应用 ,可在广域网出口、子网出口、拓扑关键节点部署设备 , 对全网范围内的用户和业务进行精细化控制和管理 , 实现网络带宽资源的全局优化使用 , 更高效的解决网络性能、故障、安全问题。
完善的访问控制	管理员可以根据在系统中设定灵活的访问控制政策。系统提供了管理员和审计员、操作员、观察员等多种级别的用户优先权： 1、 管理员（admin）类型：用户拥有所有权限。包括审计和配置权限。 2、 操作员（operator）类型：用户除了不能看审计信息之外，拥有和 admin 类型用户相同的权限。 3、 审计员（audist）类型：用户可以有查看的权限，包括查看审计信息。不能对系统进行配置。 4、 观察员（guest）类型：用户可以有查看的权限，但是不能查看审计信息。也不能对系统进行配置。
多层登录权限设置	系统支持多层登录权限 , 管理人员可以灵活设置权限 , 例如建立专门进行行为审计的人员。
自身安全保障	数据处理端口无需配置 IP 地址，避免安全攻击和病毒入侵，管理端口的系统通信使用复杂安全加密算法，保障系统自身安全

技术特点	描述
强大的警戒功能	系统对受到的攻击设有完备的记录功能，记录方式有简短记录、详细记录、发出警告、记录统计、（包括流量、连接时间、次数等）等记录。
完善的报表分析功能	提供完全用户自订制的报表系统 ,为管理人员提供深度的分析报告。
美观易用的界面	系统采用灵活的 C/S 架构，但与普通的 C/S 架构不同。首次安装通过 IE 浏览器直接获取客户端，减少了客户端分发的困难，之后客户端可以智能检测自动下载新的版本。同时基于 C/S 的特点提供简洁、易用、直观的操作界面，即使没有操作手册也能轻松使用。
完全本土化的设计	本系统充分考虑了中国国情；界面、帮助文档、使用说明等资料全部采用中文编写。
软件升级	提供简洁的软件升级策略 ,产品的软件和网络协议库将定期升级，支持在线和离线两种升级方式： 1. 在线升级方式：客户可以通过互联网直接升级。 2. 离线升级方式：也可以将升级包下载到本地进行升级。