华御科技

上网行为管理解决方案

北京华御科技有限公司

2015 年 6 月

目 录

1 网络概述

1.1 网络现状

随着互联网的加速发展、无线网络的普遍覆盖，为人们的提供了更加便利的上网条件，上网终端也由原来的计算机增加到现在的 PAD、手机等各种各样的终端

针对企事业单位，互联网的发展一方面为办公人员提供了更加便利的工作环境，但另一方面却因为缺乏有效的管理机制，导致网络给企事业单位带来更多的安全威胁，互联网资源被滥用的问题日益严峻。在网络缺乏管理的状态下，互联网总出口的压力较大，接到大量关于网络的投诉，反映网络访问速度较慢。

1.2 目前网络面临的问题

1、网络访问日志无法记录，恶意网站访问、非法言论无法进行过滤，无法满足相关法律法规的要求；

2、上班期间无法对浏览购物网站、看电影、玩游戏、炒股等行为进行控制，影响了工作效率；

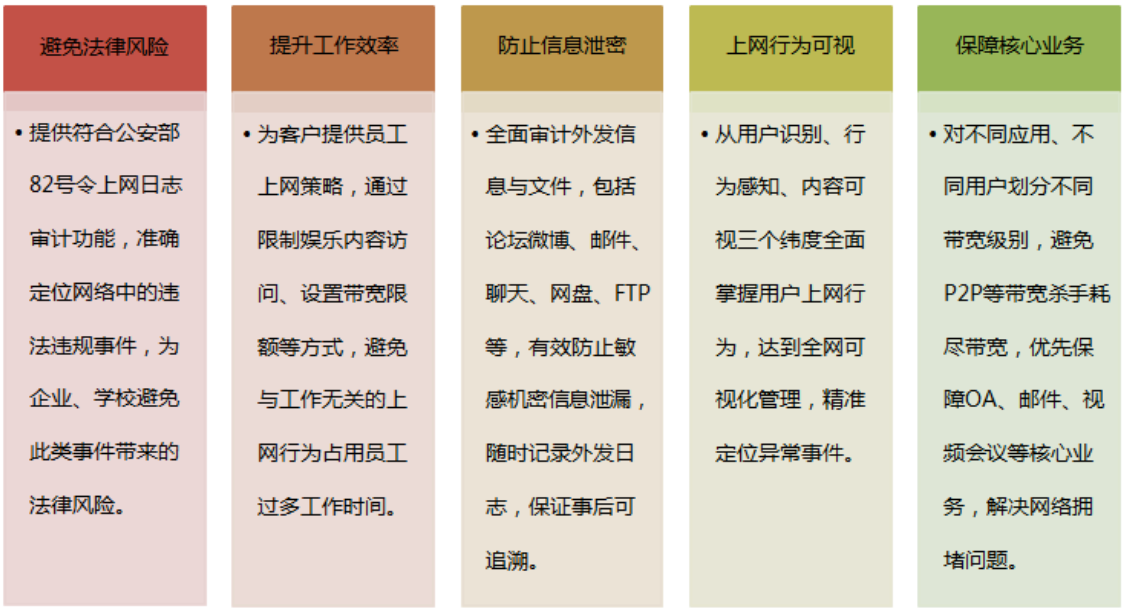
3、利用网络发送敏感信息、泄漏机密文件；

4、网络状况可视化低，不了解网络中各个应用软件、各个人员使用带宽的情况；

5、网络拥堵，上网慢，视频会议、OA 等核心业务无法保障；

1.3 解决方案

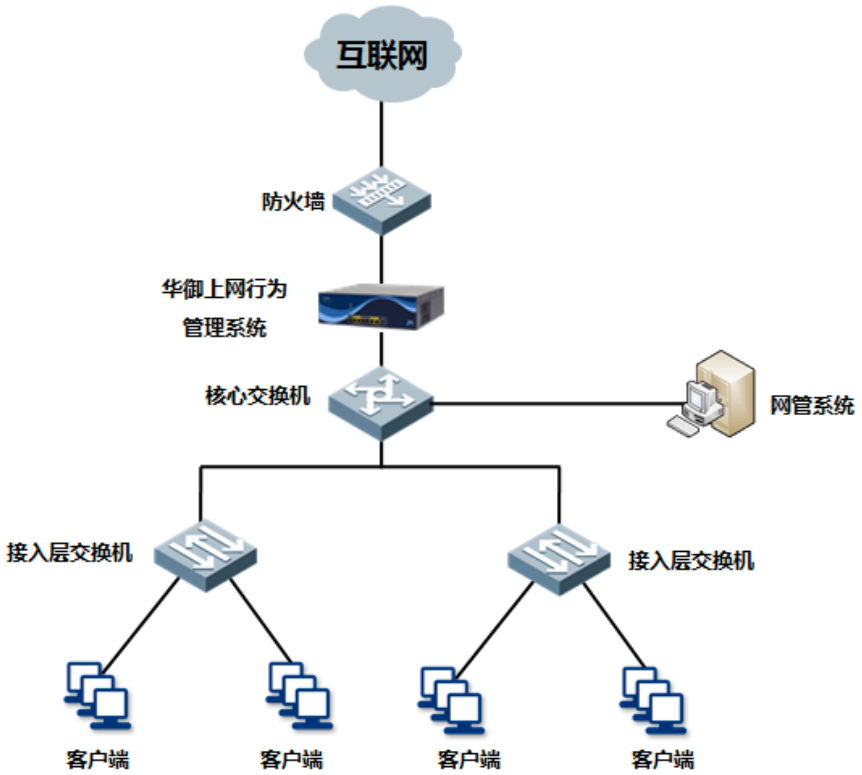
通过华御上网行为管理系统可以对娱乐网站、娱乐应用进行控制从而提高工作效率，对所有的上网日志进行留存，便于追溯查证，洞察上网行为，控制一切上网行为，对外发信息进行过滤，防止信息泄密，监视网络资源、资源合理分配，使网络资源更多的服务于核心业务，提升客户上网体验。



2 华御上网行为管理解决方案

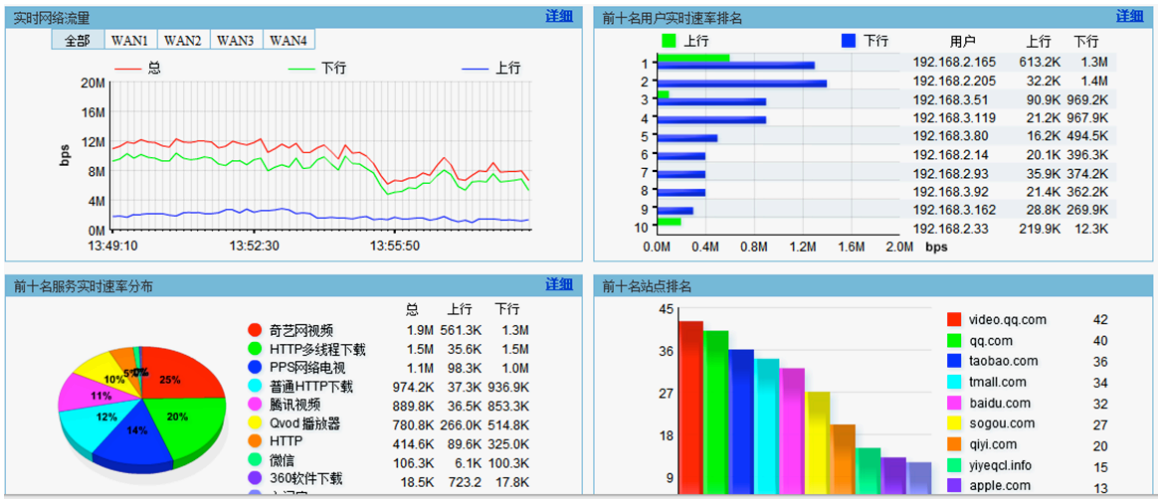
2.1 部署拓扑

将华御上网行为管理系统部署在防火墙与核心交换之间，对互联网的流量进行监视与管理，通过部署华御上网行为管理系统可以精确分析互联网各个应用系统使用网络资源的具体数据，区分不同种类应用的优先级别，划分不同的带宽保障，通过精确的分析，与智能的网络资源分配、审计外发信息、非法网站阻断，使网络健康稳定的运行。具体部署拓扑如下所示：



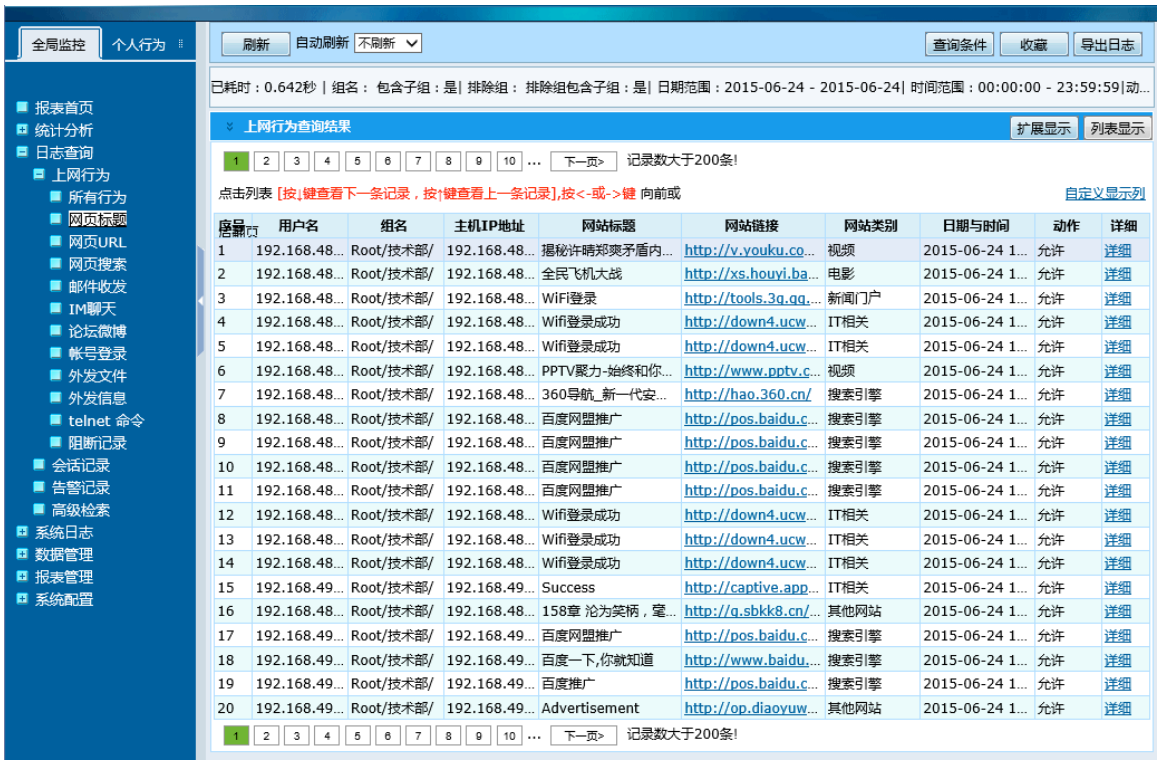
2.2 网络资源可视化

华御上网行为管理系统能够准确定位网络带宽的利用率、网络中不同的应用如下载、看电影、浏览网页等不同的应用使用网络资源比例，各个用户使用网络资源比例；用户都访问了哪些网站，如下图所示：



2.3 网站监管

华御上网行为管理系统内置数百万条 URL，通过分类管理，如新闻、音乐、视频、成人、财经、教育、科技等。用户访问网站时，华御行为管理会统计用户访问的 URL 地址，网页标题，访问时间，源 IP 地址、目的 IP 地址。管理员可以清楚的知道网络中 TOP 网站排名，每个用户的访问情况。管理方面，华御上网行为管理系统可以设定 URL 阻断，URL 黑白名单等，来阻止一些非法网站的访问，如反动、暴力等类型网站。针对要求严格的客户，华御上网行为管理系统可设置 URL 白名单，只允许访问在百名单中的网站，规范用户的上网行为。



2.4 外发信息监管

响应国家政策法规,提供用户完整上网行为日志，包括用户的身份、上网时间、IP、行为、 访问站点等详细信息；准确识别并屏蔽各类提供违法内容的网页、站点；对用户网络外发的内容进行审查,过滤违法、反动言论信息，并通过报警中心及时向管理人员报警；响应国家号召，有效识别并过滤含有黄、赌、毒等不良信息的网站。

华御上网行为管理系统能够对用户使用论坛、微博、博客、微信朋友圈等发布信息进行

日志记录，包括发布的人员，发布的时间，发布的内容等。同时可以设定关键词，包含设定的关键词的信息将被屏蔽，无法发出。

华御上网行为管理系统能够对用户使用百度、sogou、Haosou、谷歌等搜索引擎搜素的关键字进行记录，同时可以设定关键词，包含设定的关键词将无法搜索。

序号	用户名	组名	主机IP地址	搜索关键字	搜索类型	日期与时间	动作	详细
441	192.168.48.103	Root/技术部/	192.168.48.103	nv rgd	百度-百度-网页	2015-06-24 12:41:30	允许	详细
442	192.168.48.103	Root/技术部/	192.168.48.103	nv rgdm	百度-百度-网页	2015-06-24 12:41:30	允许	详细
443	192.168.48.103	Root/技术部/	192.168.48.103	女配是重生的	百度-百度-网页	2015-06-24 12:41:30	允许	详细
444	192.168.48.103	Root/技术部/	192.168.48.103	nvp	百度-百度-网页	2015-06-24 12:41:29	允许	详细
445	192.168.48.103	Root/技术部/	192.168.48.103	nba直播	百度-百度-网页	2015-06-24 12:41:29	允许	详细
446	192.168.48.103	Root/技术部/	192.168.48.103	nv	百度-百度-网页	2015-06-24 12:41:29	允许	详细
447	192.168.48.103	Root/技术部/	192.168.48.103	n	百度-百度-网页	2015-06-24 12:41:29	允许	详细
448	192.168.49.26	Root/技术部/	192.168.49.26	6月24真题	百度-百度-网页	2015-06-24 12:41:28	允许	详细
449	192.168.49.55	Root/技术部/	192.168.49.55	呼和浩特楼盘信息	百度-百度-网页	2015-06-24 12:40:38	允许	详细
450	192.168.49.55	Root/技术部/	192.168.49.55	呼和浩特新交楼盘	百度-百度-网页	2015-06-24 12:39:55	允许	详细
451	192.168.49.55	Root/技术部/	192.168.49.55	呼和浩特新交	百度-百度-网页	2015-06-24 12:39:43	允许	详细
452	192.168.49.55	Root/技术部/	192.168.49.55	呼和浩特天气	百度-百度-网页	2015-06-24 12:39:32	允许	详细
453	192.168.49.55	Root/技术部/	192.168.49.55	呼和浩特	百度-百度-网页	2015-06-24 12:39:32	允许	详细
454	192.168.49.55	Root/技术部/	192.168.49.55	呼和浩特	百度-百度-网页	2015-06-24 12:39:31	允许	详细
455	192.168.49.26	Root/技术部/	192.168.49.26	换了	百度-百度-网页	2015-06-24 12:11:03	允许	详细
456	192.168.49.26	Root/技术部/	192.168.49.26	公务员	百度-百度-网页	2015-06-24 12:11:00	允许	详细
457	192.168.49.26	Root/技术部/	192.168.49.26	公务员考试论坛内蒙古	百度-百度-网页	2015-06-24 12:10:56	允许	详细
458	192.168.49.174	Root/技术部/	192.168.49.174	狩猎	百度-百度搜索建议	2015-06-24 12:07:38	允许	详细
459	192.168.49.174	Root/技术部/	192.168.49.174	狩猎论坛	百度-百度搜索建议	2015-06-24 12:07:38	允许	详细
460	192.168.48.12	Root/技术部/	192.168.48.12	扫描仪驱动下载canon	好搜-好搜-网页	2015-06-24 11:37:52	允许	详细

首页 <上一页 17 18 19 20 21 22 23 24 25 26 下一页> 总纪录数为511条!

2.5 邮件监管

华御上网行为管理系统支持邮件内容的还原以及邮件过滤，支持通过邮件客户端、Web等方式收发邮件内容的还原。同时可以设定邮件内容过滤，设定邮件正文、内容包含某些关键词将被屏蔽。收发邮件的 Email 地址过滤，可以过滤指定的邮件地址。

序号	邮件标题	正文摘要	发件地址	收件地址	邮件类型	用户名	所属组	日期与时间
1	如[redacted]店（苏州/无锡域区,,4...	各位同事好！ 根据公司相关流程，[redacted]酒店（苏...	"[redacted]homeinns....	hom[redacted]all.list...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 17:46:...
2	关于调整2015年运营标准考...	各位老总，大家好！ 运营部开展店长标准考试已有...	d[redacted]iondesk@...	zhiy[redacted]t@ho...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 17:31:...
3	Fw: 表扬		m[redacted]'123@ho...	syq0[redacted]3_002...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 17:03:...
4	Fw: 《[redacted]老友季》邀请	发件人： 网络营销创新中心 发送时间： 2015-06...	m[redacted]109@ho...	1584[redacted]500@...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 17:03:...
5	Fw: 表[redacted]		m[redacted]123@ho...	syq04[redacted]_002...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 16:58:...
6	Fw: [redacted]老友季》邀请	发件人： 网络营销创新中心 发送时间： 2015-06...	mg[redacted]09@ho...	15848[redacted]00@...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 16:57:...
7	老友记日报-6月23日	各位店长：大家好！ 以下为2015年6月23日北华...	qio[redacted]@homei...	mg010[redacted]ho...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 16:31:...
8	答复: 呼和浩特润宇建材[redacted]...	您好，经查看5月工资已结帐。 系统管理员 人力资...	ehr[redacted]ort@ho...	at0471[redacted]om...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 16:28:...
9	Auto-Re:	您好！ 您发送至人力资源部"EHR系统支持"的邮件...	ehr[redacted]ort@ho...	at0471[redacted]om...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 15:22:...
10	呼和浩特润宇建材城店系统结...	您好： 呼和浩特市润宇建材城店，为什么在系统里...	at0[redacted]3@hom...	ehrsupp[redacted]ho...	SMTP邮件...	192.168.48....	Root/技术部/	2015-06-24 15:09:...
11	转发: 关于北华北预付活动的...	各位领导：您好！ 提前预付，锁定客源，已是酒店...	lqd[redacted]omeinn...	mg010[redacted]ho...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 14:33:...
12	[redacted]快捷（上海北域区）--,,...	各位同事好！ 根据公司相关流程，如家快捷（上...	"ito[redacted]omeinns....	homeinn[redacted]list...	POP3邮件...	192.168.48....	Root/技术部/	2015-06-24 14:31:...

1 2 下一页> 总纪录数为29条!

2.6 即时通讯监管

华御上网行为管理系统支持主流的即时聊天工具，如 QQ、MSN、飞信等聊天工具的账号、内容进行审计与管理，可以设定在工作期间禁止使用此类通讯工具，从而提高工作效率。

序号	登录帐号	主机IP地址	应用类型	用户名	所属组	日期与时间	动作	详细
1	[redacted]325623	192.168.49.34	即时通信-QQ	192.168.49.34	Root/技术部/	2015-06-24 18:28:04	允许	详细
2	[redacted]32332	192.168.49.26	即时通信-QQ	192.168.49.26	Root/技术部/	2015-06-24 18:27:36	允许	详细
3	[redacted]56026590139	192.168.49.184	手机ID-IMEI	192.168.49.184	Root/技术部/	2015-06-24 18:26:57	允许	详细
4	[redacted]32332	192.168.49.26	即时通信-QQ	192.168.49.26	Root/技术部/	2015-06-24 18:22:33	允许	详细
5	[redacted]745130	192.168.48.236	生活资讯-腾讯新闻客户...	192.168.48.236	Root/技术部/	2015-06-24 18:19:57	允许	详细
6	[redacted]55028386714	192.168.49.26	手机ID-IMEI	192.168.49.26	Root/技术部/	2015-06-24 18:17:25	允许	详细
7	[redacted]2332	192.168.49.26	即时通信-QQ	192.168.49.26	Root/技术部/	2015-06-24 18:17:12	允许	详细
8	[redacted]007008	192.168.49.26	即时通信-阿里旺旺	192.168.49.26	Root/技术部/	2015-06-24 18:16:51	允许	详细
9	[redacted]920035	192.168.48.209	即时通信-QQ	192.168.48.209	Root/技术部/	2015-06-24 18:15:20	允许	详细
10	[redacted]847180	192.168.48.21	微博-新浪微博	192.168.48.21	Root/技术部/	2015-06-24 18:14:59	允许	详细
11	[redacted]13975	192.168.48.29	即时通信-QQ	192.168.48.29	Root/技术部/	2015-06-24 18:10:34	允许	详细
12	[redacted]32332	192.168.49.26	即时通信-QQ	192.168.49.26	Root/技术部/	2015-06-24 18:10:23	允许	详细
13	[redacted]920035	192.168.48.209	即时通信-QQ	192.168.48.209	Root/技术部/	2015-06-24 18:07:58	允许	详细
14	[redacted]77024784429	192.168.48.28	手机ID-IMEI	192.168.48.28	Root/技术部/	2015-06-24 18:05:09	允许	详细
15	[redacted]56026590139	192.168.49.184	手机ID-IMEI	192.168.49.184	Root/技术部/	2015-06-24 17:57:48	允许	详细
16	[redacted]910311	192.168.49.184	即时通信-QQ	192.168.49.184	Root/技术部/	2015-06-24 17:56:24	允许	详细
17	[redacted]103401	192.168.48.18	即时通信-QQ	192.168.48.18	Root/技术部/	2015-06-24 17:55:03	允许	详细
18	[redacted]68797	192.168.48.21	即时通信-QQ	192.168.48.21	Root/技术部/	2015-06-24 17:52:51	允许	详细
19	[redacted]154651	192.168.48.97	微博-新浪微博	192.168.48.97	Root/技术部/	2015-06-24 17:45:42	允许	详细
20	[redacted]3448	192.168.49.5	即时通信-QQ	192.168.49.5	Root/技术部/	2015-06-24 17:40:52	允许	详细

1 2 3 4 5 6 7 8 9 10 ... 下一页> 记录数大于200条!

2.7 应用监管保障核心业务

华御上网行为管理系统通过 DPI 深度数据包检测，准确识别网络中的 P2P 下载、网络电视、游戏、炒股、视频会议、OA 系统等应用，华御上网行为管理系统能够识别 400 种以上的应用，并进行了分类管理。管理员能够非常清楚，网络中的各个应用的流量大小，哪些人在使用。然后可以针对应用进行带宽的保障、限速、阻断等不同的策略，来保障核心业务的正常运行。

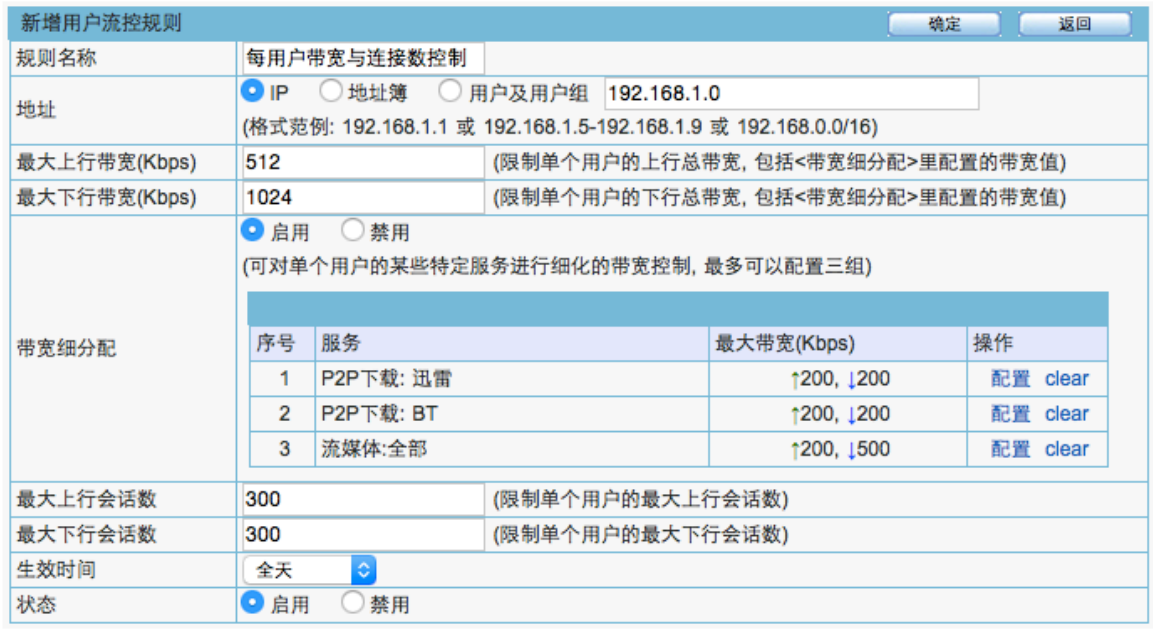
2.8 用户监管

通常网络管理设备通过 IP 地址来定位客户，但如果 IP 地址不固定，管理员定位客户将变得非常困难。华御上网行为管理系统支持 MAC 地址绑定的方式，跨三层 MAC 地址识别绑定，与客户姓名对应。同时也可以通过认证的方式。如上网的人员输入自己的用户信息进行上网，或者与 Radius、Windows 域等外部认证结合。

序号	IP地址	用户名	用户组	总(bps)	上行(bps)	下行(bps)
1	192.168.16.84	路由	六层	3.0M	1.4M	1.6M
2	192.168.11.159	沈汉	安质部（4	一层	596.0K	110.0K	486.0K
3	192.168.12.213	梁东	202	二层	342.6K	326.6K	15.9K
4	192.168.11.234	GCK	站服务器	服务器组	313.9K	292.2K	21.7K
5	192.168.18.2	刘欣		八层	247.3K	20.9K	226.4K
6	192.168.11.125	马赛		一层	174.6K	18.1K	156.5K
7	192.168.13.123	路由		三层	157.6K	18.9K	138.7K
8	192.168.18.239	八层	由	八层	74.8K	16.0K	58.8K
9	192.168.12.233	杨敬	路由206	二层	35.3K	1.6K	33.7K
10	192.168.15.228	陈税	08	五层	18.6K	3.1K	15.5K
11	192.168.11.232	cigis		服务器组	17.8K	16.1K	1.7K
12	192.168.17.144	设计		七层	16.4K	9.7K	6.7K
13	192.168.13.11	王宇	6	三层	10.2K	5.7K	4.5K
14	192.168.13.144	设计		三层	8.6K	5.9K	2.7K
15	192.168.11.60	土工	室	一层	7.6K	2.6K	5.0K
16	192.168.12.155	鲁鄙	07）	二层	4.9K	2.3K	2.6K
17	192.168.18.32	沈商		八层	4.8K	3.2K	1.6K
18	192.168.18.22	李德		八层	4.2K	2.9K	1.3K
19	192.168.11.1	传达		一层	4.2K	1.6K	2.6K
20	192.168.14.194	会议	7	四层	4.0K	2.4K	1.6K
21	192.168.18.15	杨颖		八层	3.8K	1.9K	1.9K
22	192.168.13.23	李宗颖		三层	3.7K	2.0K	1.6K
23	192.168.11.244	档案服务	1	服务器组	1.5K	969.6	519.2

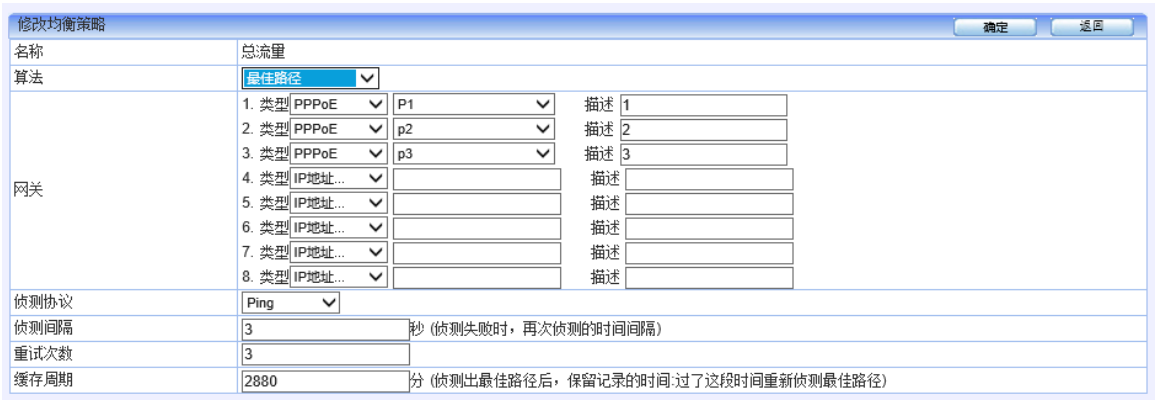
2.9 突发流量监管

网络之所以拥堵有很大部分原因是网络资源分配不均匀导致的，20%的用户使用了 80%的网络资源，下载电影的客户抢占了核心应用的带宽。华御上网行为管理系统具备公平分配网络资源的设定，通过对每个用户带宽、每个用户连接数进行管理，来实现网络资源合理分配，某华御客户拥有 100M 的网络环境中，同时在线用户 300 人左右，可以设定每个用户的下行带宽最大为 1Mbps，上行为 512Kbps。设定好之后可以观察网络带宽是否被占满，根据结果进行调整，以达到最优网络资源分配。同时针对每个用户下所使用的应用也可以进行控制，例如设定每个用户的迅雷、BT 的带宽为 200kbps，流媒体带宽为 500kbps，如下图所示：



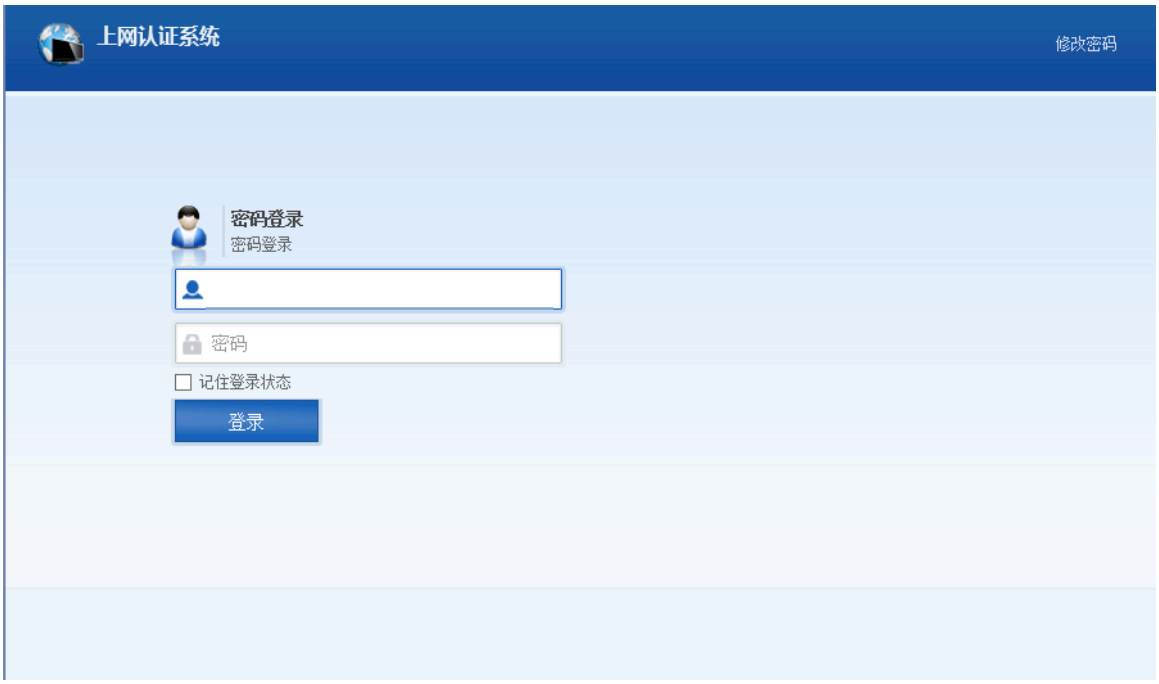
2.10 多链路负载均衡

针对用户具有多条互联网出口，华御上网行为管理系统提供了多链路负载均衡功能，可以将多条互联网出口复用，提升带宽的同时保障了互联网的稳定性。华御上网行为管理系统支持多种链路负载均衡技术，可以针对相同运营商采用流量负载均衡、不同运营商采用最佳路径进行负载均衡。同时支持 PPPOE 拨号上网，最多支持 10 条互联网线路负载均衡。



2.11 上网认证

华御上网行为管理系统提供上网准入功能，可以开启上网认证，支持各类终端的上网认证界面定制，用户需要上网时，通过预设的用户名与密码进行登录。



3 核心价值

1、增强网络安全监管水平

a) 敏感关键字过滤，外发信息审计，防止信息泄密；

b) 用户上网日志记录，避免法律风险；

c) 娱乐应用管理，提升工作效率；

d) 用户上网准入，避免外来用户接入互联网带来的安全风险；

2、提高互联网的运行效率，保障核心业务

a) 应用层精确识别，精确资源分配，使互联网高效运行；

b) 保障信息查询，Web 服务等关键系统；

c) 抑制 P2P 资源对网络的滥用；

d) 每用户最大上限设定，增强网络公平性，缓解基础设备压力；

3、提升网络管理水平

a) 快速展示网络细节，分析网络健康状况；

b) 快速定位网络突发事件，异常流量告警；

c) 操作简便、维护成本低；

4 华御上网行为管理系统优势

最精确地识别能力

- 采用深层数据包检测（DPI）、应用行为认知（BPI）、衍生协议匹配（VPI）多种识别技术，不仅能够识别常见的以及加密、衍生的网络应用。
- 快速对网络中的行为进行识别与监控。
- 专业的协议分析团队，定期的协议库、URL 库、关键字库更新，保障华御上网行为管理系统系统高效稳定运行；

业界最具人性化的分析平台

- 级联查询，从应用到使用者，从使用者到应用，能够将显示信息逐级深入展开，方便用户
- 快捷深入地了解网络使用状况；
- 无需安装任何客户端，节省管理成本，无论查看、管理、查询都通过 B/S 模式完成；
- 每个用户的汇总信息展示；点击任意用户可汇总查看其访问过的网站、收发的邮件、IM 聊天内容、搜素的关键字、玩过的游戏等。

全方位的管控方式

- 支持针对不同的时间段、不同的用户、不同的应用设定不同的控制策略；
- 每用户最大速率控制，均衡网络资源分配，抑制突发流量；
- 每用户最大连接数控制，抑制用户使用 P2P，缓解连接数过大造成的网络设备压力；
- 业界真正的动态保障，单独保障重要的应用可以实现网络资源的最大化利用；
- URL 过滤、关键字过滤、文件传输过滤、邮件过滤等多种过滤手段；

优越的性能

- 全线产品具备旁路（bypass）模块，支持断电旁路自动跳转，高负载自动旁路；
- 超强的处理性能，平均处理转发时间为 0.03 微秒；