



华御  
HUAYU.BJ

# 华御科技—Cross 流量控制系统

2018年1月



华御  
HUAYU.BJ

# 网络概述

# 互联网管理面临的挑战

缺乏网络可视化的工具

缺乏对网络资源的合理分配

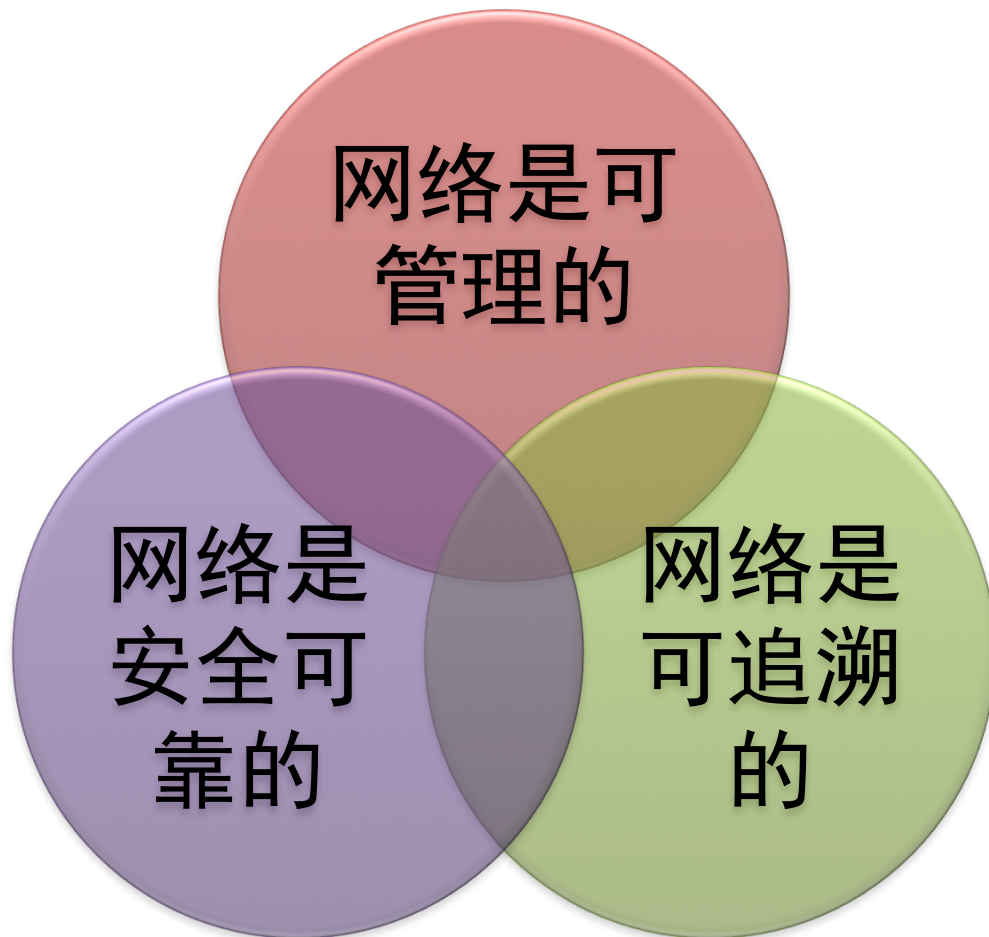
缺乏对非法网站的检测与管理

缺乏对上网者言论的审计与管理

# 网络同样需要管理



# 网络流量控制对用户的重要性





华御

HUAYU.BJ

# Cross流量控制解决方案

# Cross系统在网络中的位置

应用层

表示层

会话层

传输层

网络层

数据链路层

物理层



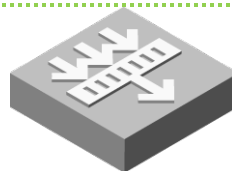
华御

HUAYU.BJ

华御解决方案



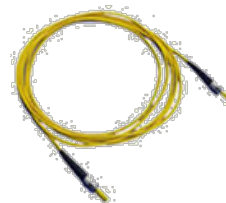
交换机



防火墙



路由器

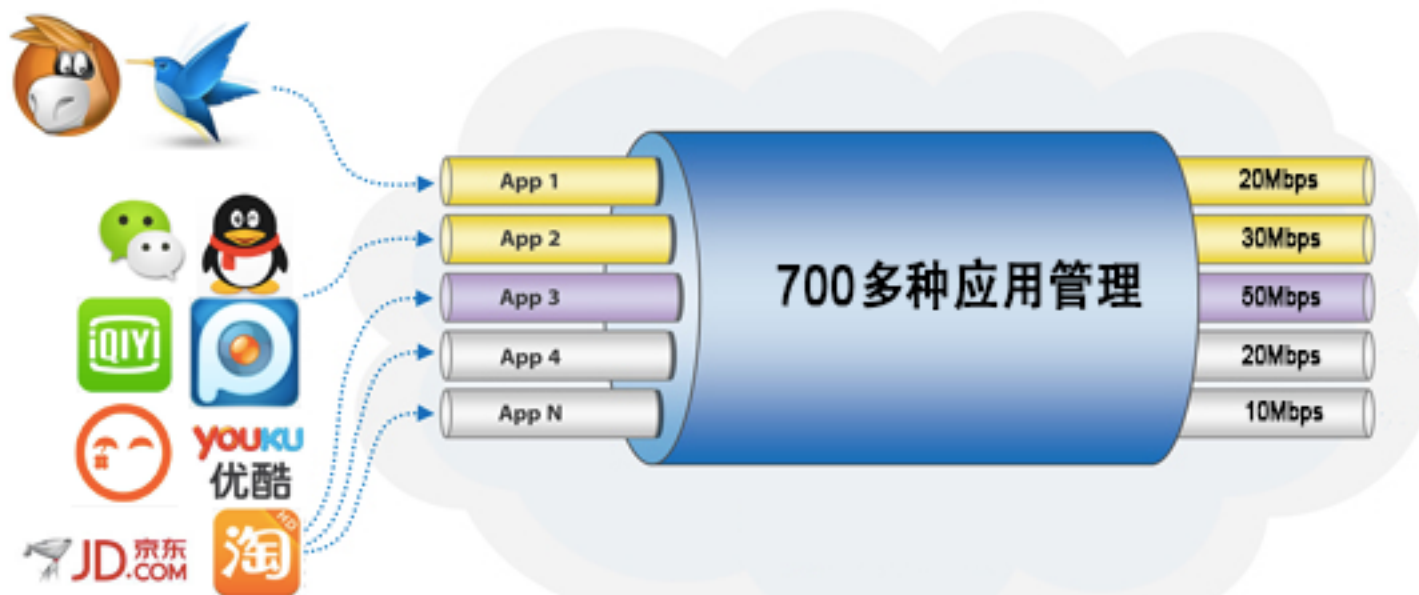


华御

HUAYU.BJ

# 网络应用识别

- 呈现当前网络流量图表，实时掌握网络的资源占用情况,准确了解带宽占用较大的用户和应用;
- 对各类带宽资源占用大的 P2P 下载和在线视频应用进行精准识别,并限制其对带宽的滥用;





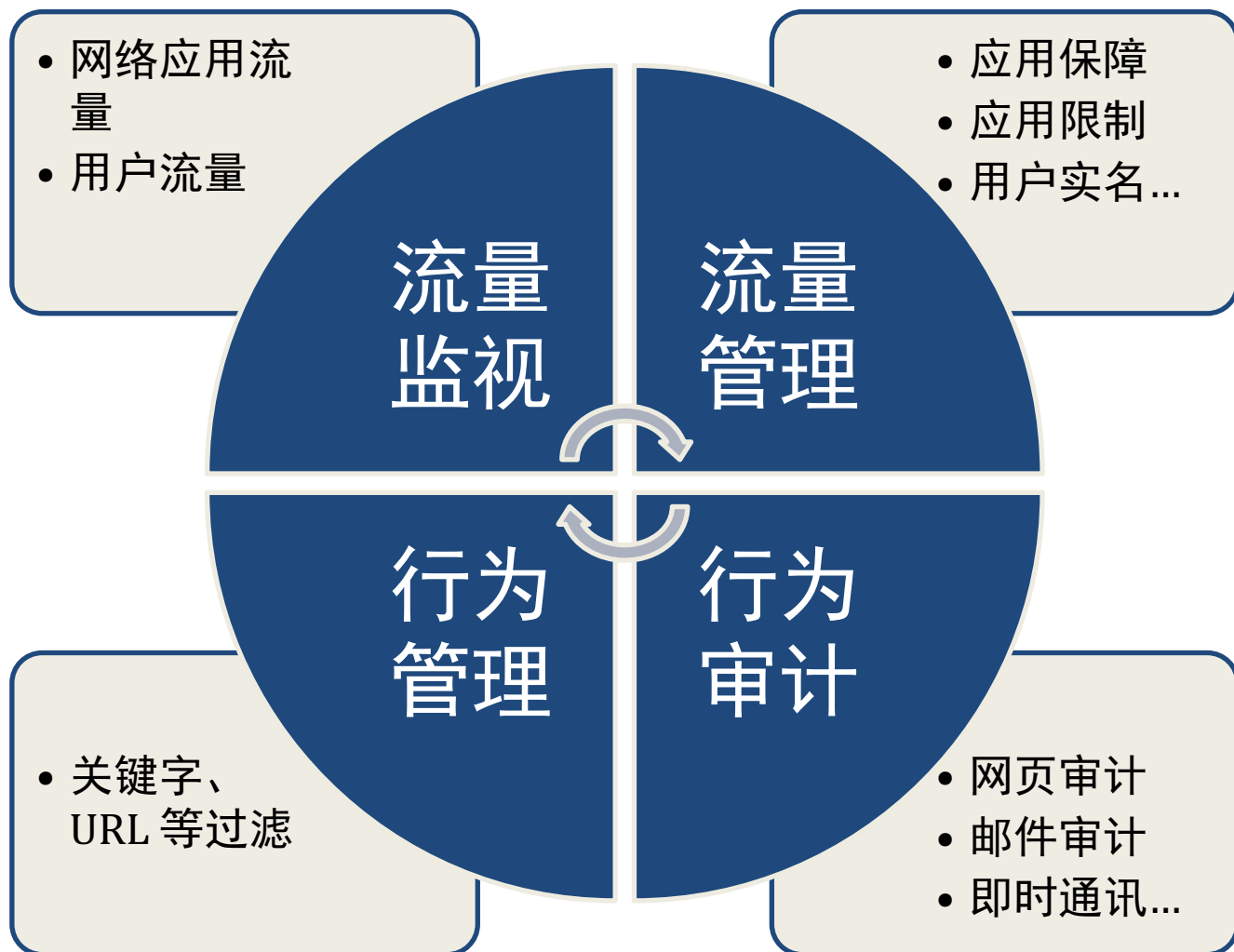


华御

HUAYU.BJ

# 产品功能

# Cross系列产品主要功能



# 网络流量监视

服务流量分布图：  
各应用使用了多少带宽？

网页排名图：  
经常访问的网站有哪些？

HUAYU.BJ

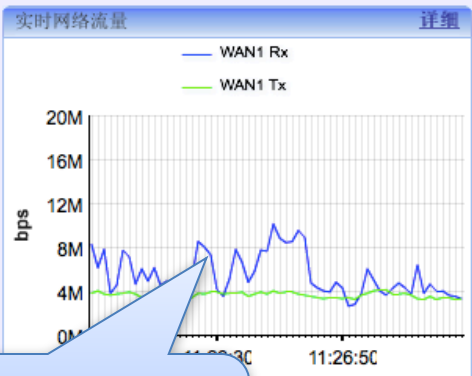
ipv4 ipv6

刷新 保存 注销

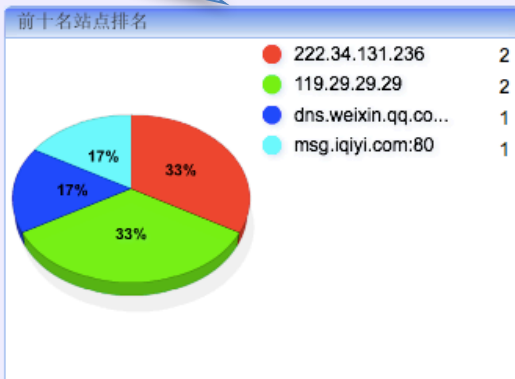
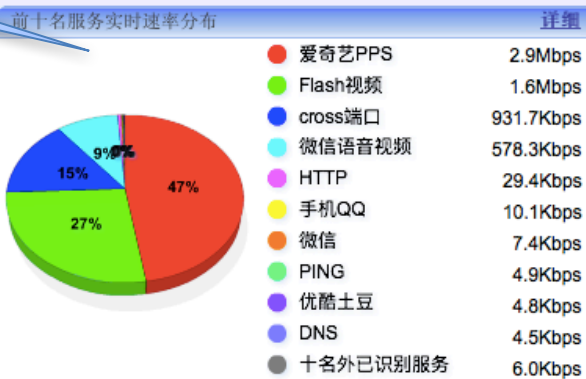
- 设备状态
- 实时监控
- 系统配置
- 系统对象
- 网络配置
- 防火墙
- 组织管理
- 流量管理
- 行为管理
- VPN配置
- HA 配置
- 系统日志
- 故障排除
- 报表中心

设备版本信息	
系统版本	Cross8100-20-1.7.6
应用特征库	AIS-2.4.3.5
URL库	URL-2.4.3.5
授权类型	正式授权

设备资源	
CPU使用率	9.7%
内存使用率	27.6%
活跃会话数	2976/512000
在线用户数	95
在线认证用户数	0



整体网络流量图：  
当期网络使用了多少？



前十名用户实时速率排名

排名	用户	上行	下行
1	李成路由	80.1K	1.5M
2	靳南方路由	25.9K	900.7K
3	周兴	320.6K	398.3K
4	张巍	511.1K	61.1K
5	丁顺全	352.1K	39.4K
6	王文猛	296.3K	40.0K
7	于大军	295.8K	37.9K
8	长春硬盘	304.3K	19.6K
9	春哥师傅	277.9K	37.2K
10	培训中心路由器	23.2K	281.5K

最近五次事件日志

时间	内容
2018-01-28 11:30:03	管理员登录成功, 用户名: admin, IP地址: 60.10.192.123
2018-01-28 11:01:27	管理员登录成功, 用户名: admin, IP地址: 60.10.192.123
2018-01-28 10:06:19	管理员登录成功, 用户名: admin, IP地址: 192.168.1.47
2018-01-27 08:07:00	管理员注销, 用户名: admin, IP地址: 192.168.1.218
2018-01-27 07:46:59	管理员登录成功, 用户名: admin, IP地址: 192.168.1.218

用户流量排名图：  
哪些人用了多少带宽？

# 用户详细流量分析

查看某个用户正在干什么

ipv4 ipv6

刷新 保存 注销

192.168.1.146 (李成路, Root/实名组/2M组) 活跃服务

序号	服务	下行速率 (%)	下行速率	下行流量	上行速率 (%)	上行速率	上行流量	在线时长	最后响应
	总计		1.5Mbps	2.1GB		176.4Kbps	368.7MB		
1	cross端口	74.9%	1.2Mbps	1.2GB	82.4%	145.3Kbps	124.4MB	66:22:44	0
2	Flash视频	15.1%	233.6Kbps	96.6MB	6.6%	11.7Kbps	4.6MB	0:14:32	2
3	今日头条	9.7%	150.5Kbps	1.7MB	8.9%	15.6Kbps	154.0KB	0:11:43	0
4	DNS	0.1%	2.0Kbps	112.2MB	0.7%	1.2Kbps	62.8MB	575:43:14	1
5	HTTP							22:31	0
6	正在识别的TCP协议							21:39	0
7	Oppo软件商店							00:31	0

查看某个特定的应用有哪些人使用

爱奇艺PPS 在线用户

序号	IP地址/用户名/用户组	在线时长	累计在线时间(秒)	累计在线流量(Byte)	平均速率(bps)
总记录数:13 页码:1/1					
1	192.168.1.105 任春元 Root/实名组/2M组	91:13:38	0	↑ 7.8G, ↓ 2.5G	↑199.0K, ↓64.0K
2	192.168.1.237 王文猛 Root/实名组/3M组	53:55:01	0	↑ 5.7G, ↓ 2.5G	↑244.3K, ↓107.8K
3	192.168.1.90 于大军 Root/实名组/2M组	29:23:59	0	↑ 3.0G, ↓ 1.4G	↑237.4K, ↓113.3K
4	192.168.1.241 丁顺全 Root/实名组/5M组	11:24:29	0	↑ 2.0G, ↓ 613.4M	↑410.0K, ↓122.4K
5	192.168.1.23 安检-王刚 Root/实名组/10M组	2:30:11	148	↑157.1M, ↓ 1.5G	↑140.6K, ↓ 1.4M
6	192.168.1.122 春哥师傅 Root/实名组/2M组	5:26:56	0	↑615.0M, ↓805.2M	↑256.8K, ↓336.3K

IB	0.1%	232.0bps	19.2MB	52:05:13	4
IB		0.0bps	2.3KB	0:00:28	27
IB		0.0bps	1.1KB	0:00:29	29
IB		0.0bps	727B	0:00:30	30

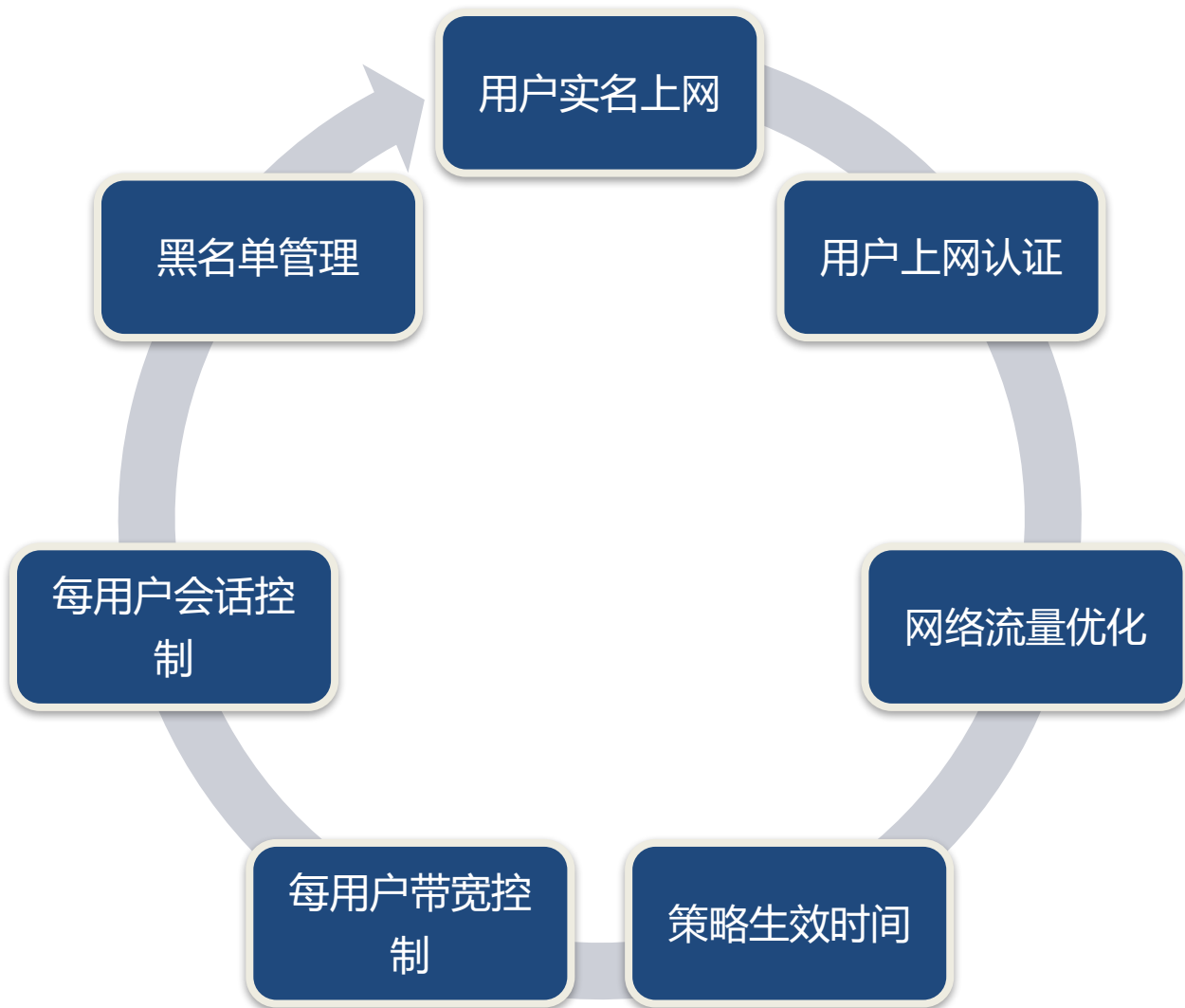


- 设备状态
- 实时监控
- 系统配置
- 系统对象
- 网络配置
- 防火墙
- 组织管理
- 流量管理
- 行为管理
- VPN配置
- HA配置
- 系统日志
- 故障排除
- 报表中心



- 设备状态
- 实时监控
- 系统配置
- 系统对象
- 网络配置
- 防火墙
- 组织管理
- 流量管理
- 行为管理
- VPN配置
- HA配置
- 系统日志
- 故障排除
- 报表中心

# 流量管理



# 用户实名管理

序号	IP地址	用户名	用户组	总(bps)	上行(bps)	下行(bps)
1	 192.168.17.197	贺国良722	七层	3.0M	131.9K	2.9M
2	 192.168.17.144	设计三所	七层	2.4M	89.3K	2.3M
3	 192.168.11.1	传达室	一层	1.2M	40.0K	1.1M
4	 192.168.15.186	路由505	五层	910.7K	870.8K	39.8K
5	 192.168.18.23	路由828	八层	579.7K	40.9K	538.8K
6	 192.168.12.98	廖红伟207	二层	484.1K	144.1K	340.0K
7	 192.168.12.233	杨敬亮路由206	二层	304.8K	40.3K	264.5K
8	 192.168.11.73	周末竟108	一层	156.2K	33.1K	123.0K
9	 192.168.12.181	路由218	二层	117.3K	28.8K	88.6K
10	 192.168.16.159	郝615	六层	77.1K	21.4K	55.7K
11	 192.168.15.18	军图所518	五层	76.7K	33.1K	43.6K

# 认证管理

- 本地认证
- 第三方
  - Radius
  - PPPOE
  - AD域
  - LDAP
  - POP3
  - HTTP单点

The screenshot displays the 'AD SSO' configuration page in the Huayu management system. The interface includes a top navigation bar with 'ipv4' and 'ipv6' tabs, and a left sidebar with a tree view of system settings. The main content area is titled 'AD SSO' and contains several configuration options:

- 启用AD SSO:域登录脚本方式
  - 强制要求Windows PC必须登录到域, 才能SSO成功
  - 域服务器: [不设定]
  - 如果在【组织结构>LDAP/AD导入】界面尚未导入 AD 域组织结构, 但同时期望获取用户的"显示名"来统计各项数据的情况, 需设定一个 AD 服务器; 否则选择[不设定]。
- 启用AD SSO:监听计算机登录域的数据, 获取登录信息
  - 对于用户登录域的数据包不经过设备的情况, 则需要把登录数据包镜像到设备。在"SSO镜像设置"中启用镜像功能
- 启用AD SSO:启用集成windows身份验证
  - 启用此功能, 将要求客户端计算机及设备本身都加入Active Directory域。
  - 启设备将使用以下信息加入域。
  - 计算机名称: HOSTNAME
  - 域名: [输入框]
  - 域DNS服务器: [输入框]
  - 域帐号: admin
  - 域帐号密码: [输入框]
  - [测试有效性]
- 启用AD SSO:启用域监控单点登录
  - 主动到AD域控制器上检索日志, 以获取登录的用户信息
  - 域监控单点登录

序号	域名	域DNS服务器	域帐号	域帐号密码	操作
[新增]					

# 流量管理 - 网络优化

- 定义内部
- 定义外部
- 定义服务
- 设置策略
- 设置时间

策略流控规则										新增	修改状态	删除所有	计数清零
序号	规则名称	内网地址	外网地址	服务	带宽(Kbps)	生效时间	匹配计数	<input type="checkbox"/> 状态	操作				
线路: WAN1										删除本组			
1	P2P	全部	全部	P2P下载:全部	阻断流量	全天	0	<input checked="" type="checkbox"/>	修改 移动 删除				
2	股票	全部	全部	股票交易:全部	阻断流量	全天	0	<input checked="" type="checkbox"/>	修改 移动 删除				

提示: 同一线路的规则, 序号越小优先级越高, 可通过<插入>或<移动>来改变规则的先后顺序.

新增策略流控规则		确定	返回
规则名称	<input type="text"/>		
生效线路	<input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2		
内网地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 用户组 <input type="text" value="全部"/> (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
外网地址	<input checked="" type="radio"/> IP <input type="radio"/> 地址簿 <input type="radio"/> 用户组 <input type="text" value="全部"/> (格式范例: 192.168.1.1 或 192.168.1.5-192.168.1.9 或 192.168.0.0/16)		
服务	<input checked="" type="radio"/> 所有 <input type="radio"/> 自定义 (如要控制一种或多种服务, 请选择<自定义>, 然后点击<选择服务>按钮进行服务的选择)		
流控行为	<input checked="" type="radio"/> 控制带宽 <input type="radio"/> 阻断流量		
优先级	中 (优先级较高的报文优先传送)		
最大带宽	上行:	<input type="text" value="不限制"/> (Kbps)	<input type="text" value="100"/> %
	下行:	<input type="text" value="不限制"/> (Kbps)	<input type="text" value="100"/> %
(本规则流量能使用的最大带宽,百分比为占用本线路带宽值的比例)			
保障带宽	上行:	<input type="text" value="不保障"/> (Kbps)	<input type="text" value="0"/> %
	下行:	<input type="text" value="不保障"/> (Kbps)	<input type="text" value="0"/> %
(带宽空闲时,其它规则流量可借用当前空闲带宽,百分比为占用本线路带宽值的比例)			
	上行:	<input type="text" value="不预留"/> (Kbps)	<input type="text" value="0"/> %

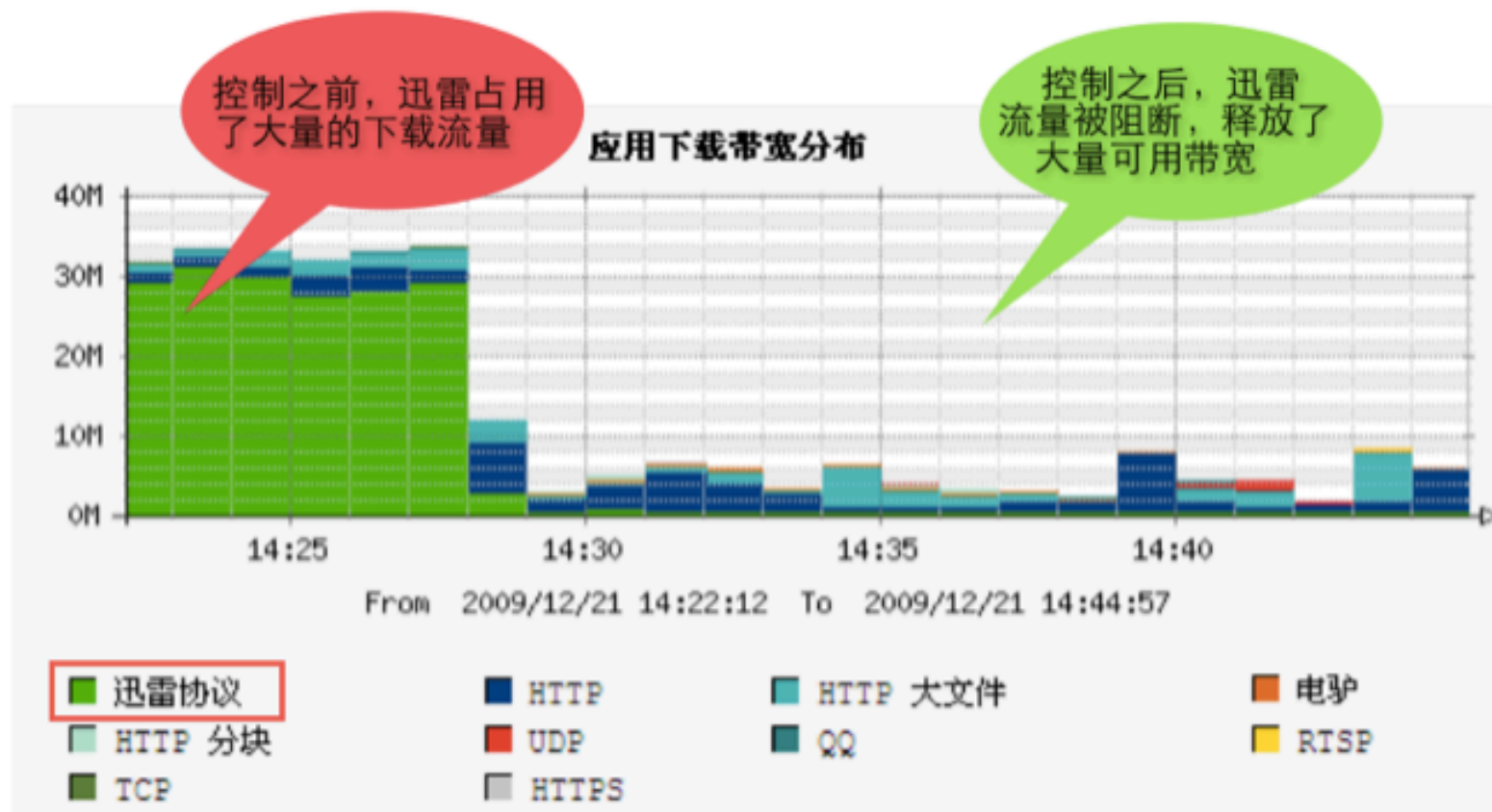


# 流量管理 – 增强资源分配公平

- 增强网络公平性、缓解设备压力
  - 每个用户最大带宽，及带宽细分（其使用应用的带宽）
  - 每个用户最大会话

修改用户流控规则		确定	返回
规则名称	VIP		
地址	<input type="radio"/> IP <input type="radio"/> 地址簿 <input checked="" type="radio"/> 用户及用户组 选择 Root/实名组/VIP组		
流控方式	<input checked="" type="radio"/> 静态带宽 <input type="radio"/> 智能带宽		
最大上行带宽(Kbps)	20480	(限制单个用户的上行总带宽, 包括<带宽细分分配>里配置的带宽值)	
最大下行带宽(Kbps)	20480	(限制单个用户的下行总带宽, 包括<带宽细分分配>里配置的带宽值)	
带宽细分分配	<input type="radio"/> 启用 <input checked="" type="radio"/> 禁用 (可对单个用户的某些特定服务进行细化的带宽控制, 最多可以配置三组)		
最大上行会话数	不限制	(限制单个用户的最大上行会话数)	
最大下行会话数	不限制	(限制单个用户的最大下行会话数)	
生效时间	全天		
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用		
快速链接	[地址簿]	[生效时间]	

# P2P类应用阻断



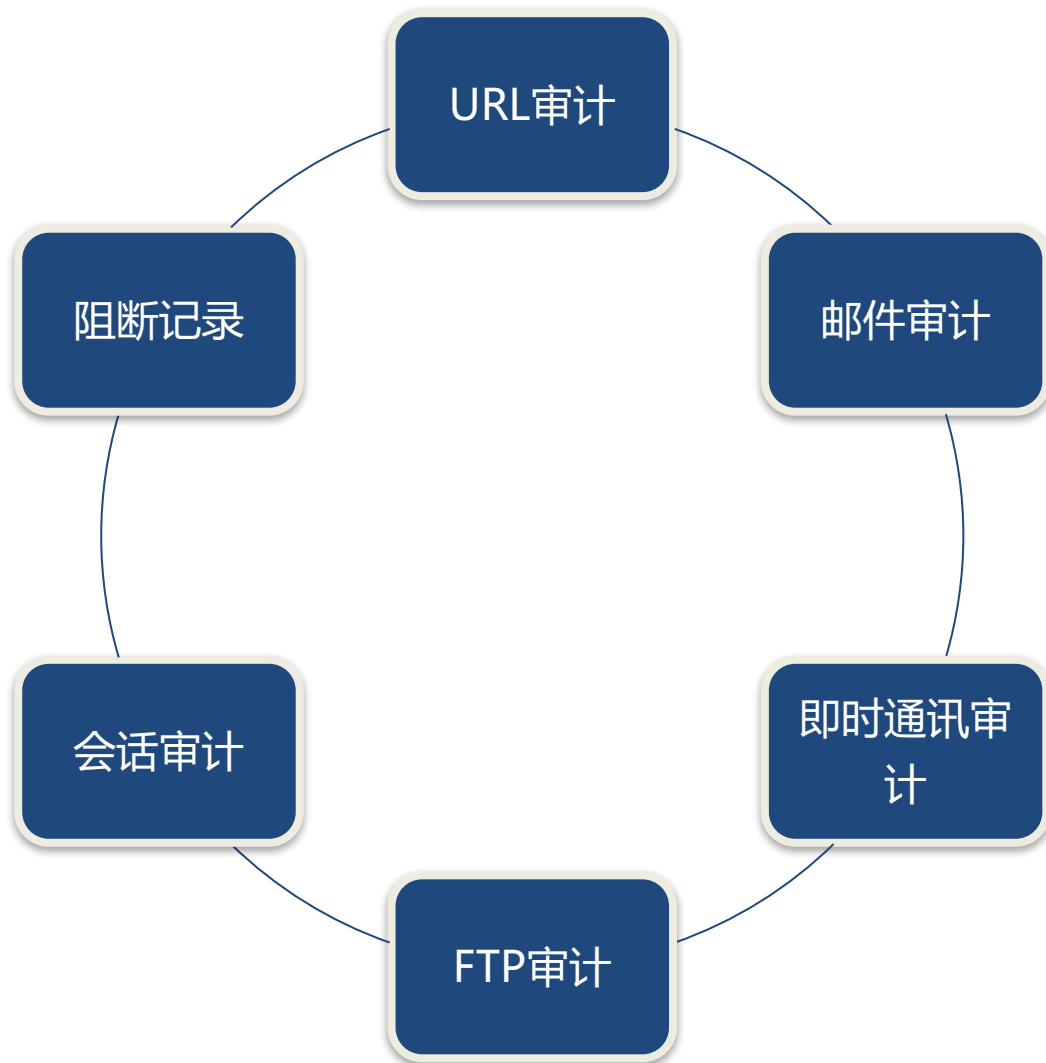
# 黑白名单

## ■ 黑名单

- 每日流量限定
- 每周流量限定
- 每月流量限定
- 最大速率
- 最大会话数
- 惩罚方式
- 惩罚时长
- 加倍惩罚

新增黑名单规则				确定	返回
名称	黑名单规则				
每日流量配额(KB)	总流量 200	上行流量 100	下行流量 100		
每周流量配额(KB)	总流量 不限制	上行流量 不限制	下行流量 不限制		
每月流量配额(KB)	总流量 不限制	上行流量 不限制	下行流量 不限制		
最大速率(Kbps)	连续 15 分钟速率持续超过				
	上行 100	下行 50			
最大会话数	连续 5 分钟会话数持续超过				
	上行 不限制	下行 不限制			
惩罚方式	<input type="radio"/> 强制下线 <input checked="" type="radio"/> 修改带宽和会话数				
	上行带宽 12 Kbps	上行会话数 10			
	下行带宽 不限制 Kbps	下行会话数 不限制			
惩罚时长	1	<input type="radio"/> 分钟 <input checked="" type="radio"/> 小时 <input type="radio"/> 天			
加倍惩罚	在一周内	连续进入黑名单超过 5 次			
	惩罚时长变为原来的 3 倍				
生效时间	全天	在生效时间内才进行黑名单的控制。在生效时间外,不对用户的速率和会话进行限制,用户产生的流量也不记入黑名单的流量配额内。			

# 网络行为审计



# URL审计

## ■ 网站标题、发帖、搜索关键字、网页上传文件



The screenshot displays a web monitoring application interface. On the left is a navigation menu with categories like '设备状态', '实时监控', '统计分析', and '行为分析'. The main area shows a table titled '网页标题记录' (Web Page Title Records) with columns for '序号' (Serial Number), 'IP地址/用户名/用户组' (IP Address/Username/User Group), '网页标题' (Web Page Title), '网站类型' (Website Type), 'URL地址' (URL Address), '记录时间' (Record Time), and '操作' (Action). The table contains 10 rows of data, including records for '迷你首页', 'Qzone精彩由你而来', '智能电脑芯, 酷睿炫视界', and various news articles from Sina.com.cn.

序号	IP地址/用户名/用户组	网页标题	网站类型	URL地址	记录时间	操作
1	172.17.1.43 172.17.1.43 Root	迷你首页	新闻门户	http://minisite2009.qq.com/othercity/all...	2011-06-24 17:35:30	详细
2	172.17.1.43 172.17.1.43 Root	Qzone精彩由你而来	新闻门户	http://imgcache.qq.com/qzone/gift/view_s...	2011-06-24 17:35:13	详细
3	172.17.1.43 172.17.1.43 Root	Qzone精彩由你而来	新闻门户	http://imgcache.qq.com/qzone/gift/gift_v...	2011-06-24 17:35:08	详细
4	172.17.1.100 172.17.1.100 Root	智能电脑芯, 酷睿炫视界	其他	http://www.intel.com/cn/11newcore/?dfaid...	2011-06-24 17:35:04	详细
5	172.17.1.100 172.17.1.100 Root	<![CDATA[[]]>	新闻门户	http://dcads.sina.com.cn/html.nq/c=video...	2011-06-24 17:35:01	详细
6	172.17.1.100 172.17.1.100 Root	新闻中心新闻博客推荐内容_新浪网	新闻门户	http://pfp.sina.com.cn/iframe/2008/1023/...	2011-06-24 17:34:58	详细
7	172.17.1.100 172.17.1.100 Root	新闻中心_新浪网	新闻门户	http://news.sina.com.cn/iframe/485/2008/...	2011-06-24 17:34:58	详细
8	172.17.1.100 172.17.1.100 Root	新闻中心_新浪网	新闻门户	http://news.sina.com.cn/iframe/485/2008/...	2011-06-24 17:34:58	详细
9	172.17.1.100 172.17.1.100 Root	新浪网	新闻门户	http://pfp.sina.com.cn/iframe/no/2010-08...	2011-06-24 17:34:58	详细
10	172.17.1.100 172.17.1.100 Root	新闻中心_新浪网	新闻门户	http://news.sina.com.cn/iframe/485/2008/...	2011-06-24 17:34:58	详细

# 邮件审计

- POP、SMTP邮件审计、Webmail邮件审计
  - 邮件地址、主题、正文、附件、时间

The screenshot displays a web-based mail audit interface. On the left is a navigation menu with options like '设备状态', '实时监控', '统计分析', '行为分析', 'WEB记录', '邮件记录', '允许的邮件', '过滤的邮件', '即时通讯', 'FTP记录', '会话记录', '阻断记录', '数据管理', and '报表管理'. The main area is divided into 'SMTP邮件查询' (SMTP Mail Search) and 'SMTP邮件记录' (SMTP Mail Record). The search section includes fields for '所属组' (Group), '时间范围' (Time Range) set to '2011-06-24 00:00:00 - 2011-06-24 23:59:59', 'IP地址/用户名' (IP Address/Username) with radio buttons for 'IP地址' and '用户名', '邮件地址' (Mail Address) with checkboxes for '邮件地址', '发件人', and '收件人', '关键字' (Keywords) with checkboxes for '邮件主题', '邮件附件', and '邮件内容', and '每页显示记录数' (Records per page) set to 20. The record section shows a table with columns: '序号' (Serial Number), 'IP地址/用户名/用户组' (IP Address/Username/User Group), '邮件地址' (Mail Address), '发件人' (Sender), '收件人' (Receiver), '邮件主题' (Mail Subject), '邮件附件' (Mail Attachment), '记录时间' (Record Time), and '操作' (Action). Two records are listed, each with a '详细' (Details) link. The interface also features buttons for '导出为Excel' and '导出为HTML'.

**SMTP邮件查询**

所属组:  选择组

时间范围: 2011-06-24 00:00:00 - 2011-06-24 23:59:59  按时间降序排列  按时间升序排列

IP地址/用户名:  IP地址  用户名

邮件地址:   邮件地址  发件人  收件人

关键字:   邮件主题  邮件附件  邮件内容

每页显示记录数: 20

**SMTP邮件记录**

总记录数: 2 页码: 1/1

序号	IP地址/用户名/用户组	邮件地址	发件人	收件人	邮件主题	邮件附件	记录时间	操作
1	172.17.1.100 172.17.1.100 Root	zcmvcom@163.com	zcmvcom@163.com	zcm8483@gmail.com	测试		2011-06-24 17:40:21	<a href="#">详细</a>
2	172.17.1.19 172.17.1.19 Root	wangzhi@rexen.com.cn	wangzhi@rexen.com.cn	zhuchunmao@rexen.com.cn	覆盖	[1]	2011-06-24 17:39:21	<a href="#">详细</a>

总记录数: 2 页码: 1/1

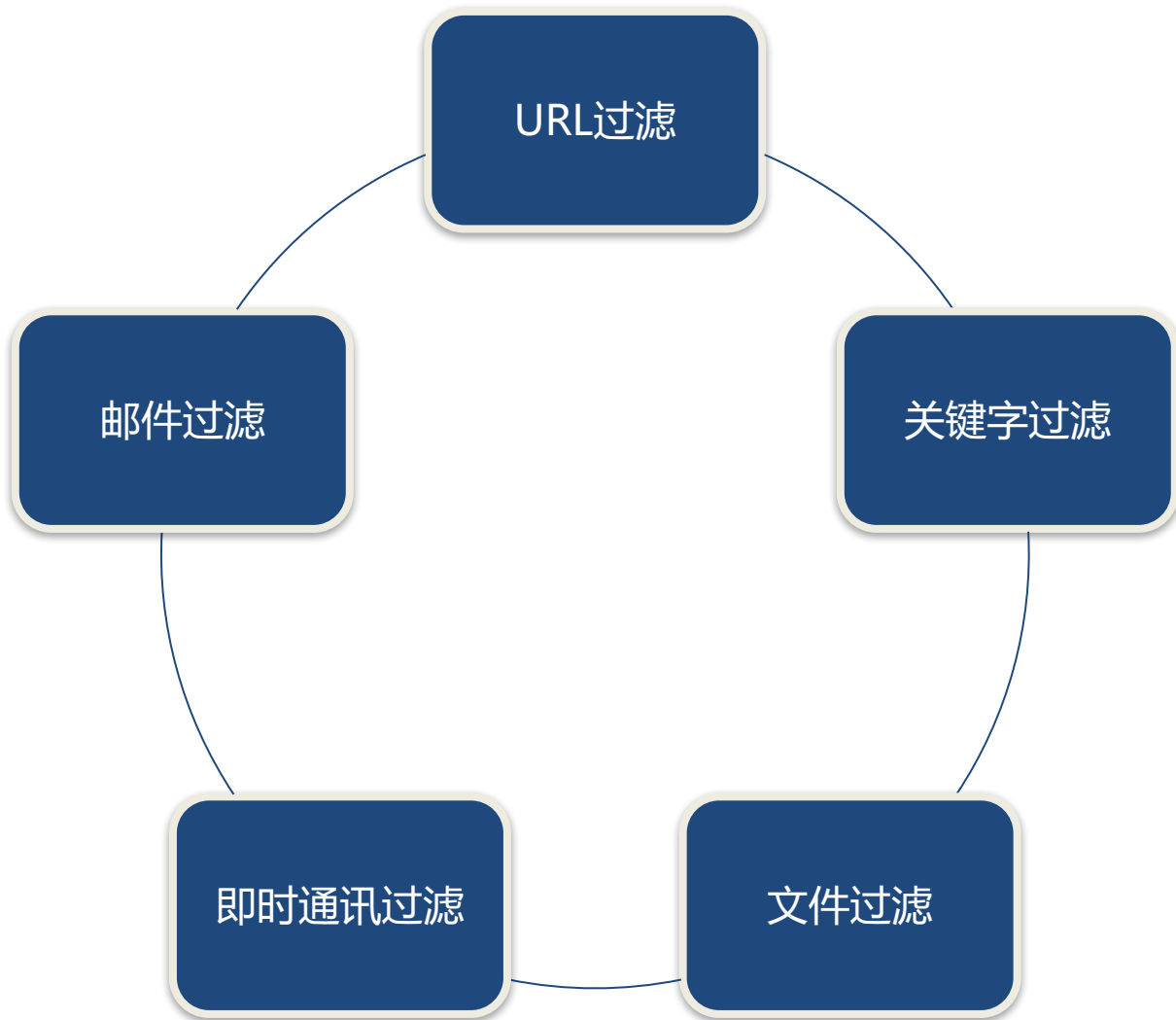
# 即时通讯审计

- QQ、MSN、Yahoo通、飞信
  - 账号、内容、时间、传输的文件

The screenshot displays a web-based interface for network monitoring. The left sidebar contains a navigation menu with categories like '全局监控' (Global Monitoring) and '个人行为' (Individual Behavior). Under '个人行为', there is a sub-menu for '即时通讯' (Instant Messaging) which includes 'MSN', 'QQ', 'Yahoo', 'ICQ', 'FETION', 'GTALK', 'FTP记录', '会话记录', '阻断记录', '数据管理', and '报表管理'. The main content area is titled 'MSN登录查询' (MSN Login Query) and includes search filters for '所属组' (Group), '时间范围' (Time Range) set to '2011-06-24 00:00:00 - 2011-06-24 23:59:59', and 'IP地址/用户名' (IP Address/Username) with radio buttons for 'IP地址' and '用户名'. Below the search area is a table titled 'MSN登录记录' (MSN Login Records) with columns for '序号' (Serial Number), 'IP地址/用户名/用户组' (IP Address/Username/User Group), 'MSN帐号' (MSN Account), '记录时间' (Record Time), and '操作' (Action). The table contains 6 rows of data.

序号	IP地址/用户名/用户组	MSN帐号	记录时间	操作
1	172.17.1.99 172.17.1.99 Root	zimingwz@hotmail.com	2011-06-24 17:52:22	详细
2	172.17.1.99 172.17.1.99 Root	zimingwz@hotmail.com	2011-06-24 17:51:48	详细
3	172.17.1.100 172.17.1.100 Root	zcm8483@hotmail.com	2011-06-24 17:50:51	详细
4	172.17.1.100 172.17.1.100 Root	zcm8483@hotmail.com	2011-06-24 17:50:20	详细
5	172.17.1.100 172.17.1.100 Root	zcm8483@hotmail.com	2011-06-24 17:50:19	详细
6	172.17.1.100 172.17.1.100 Root	zcm8483@hotmail.com	2011-06-24 17:50:19	详细

# 网络行为管理





# 关键词过滤

## ■ 网页搜索

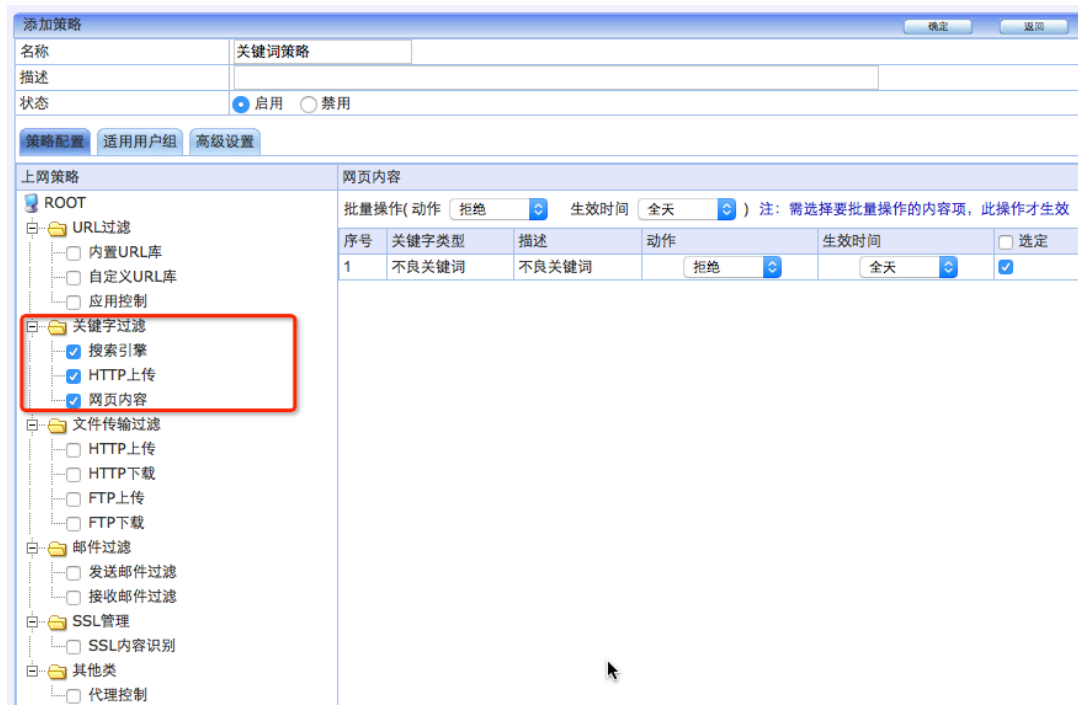
- 百度搜索
- Google搜索
- 360好搜
- sogou搜索

## ■ HTTP上传

- 上传内容包含关键词

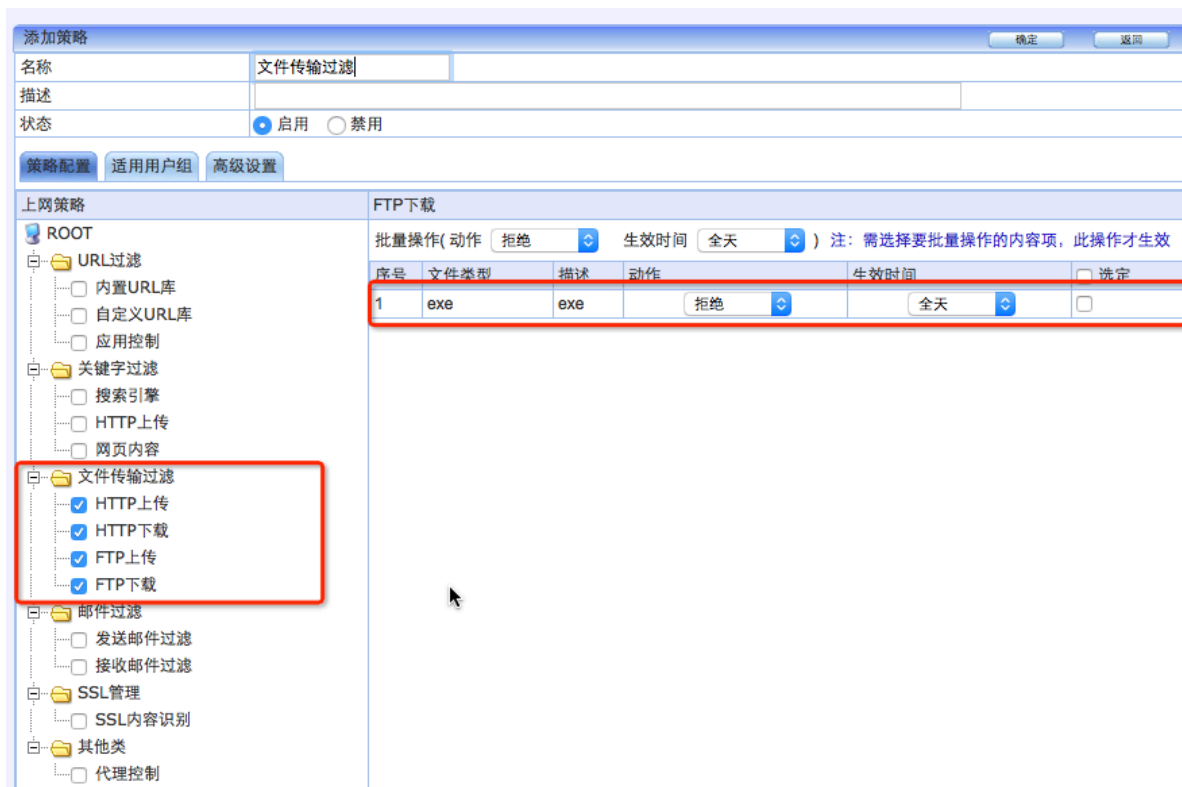
## ■ 网页内容

- 网页内容中包含关键词



# 文件传输过滤

- 支持过滤类型
  - HTTP上传
  - HTTP下载
  - FTP上传
  - FTP下载
- 过滤方式
  - 自定义文件类型



# 邮件过滤

## ■ 收发邮件地址

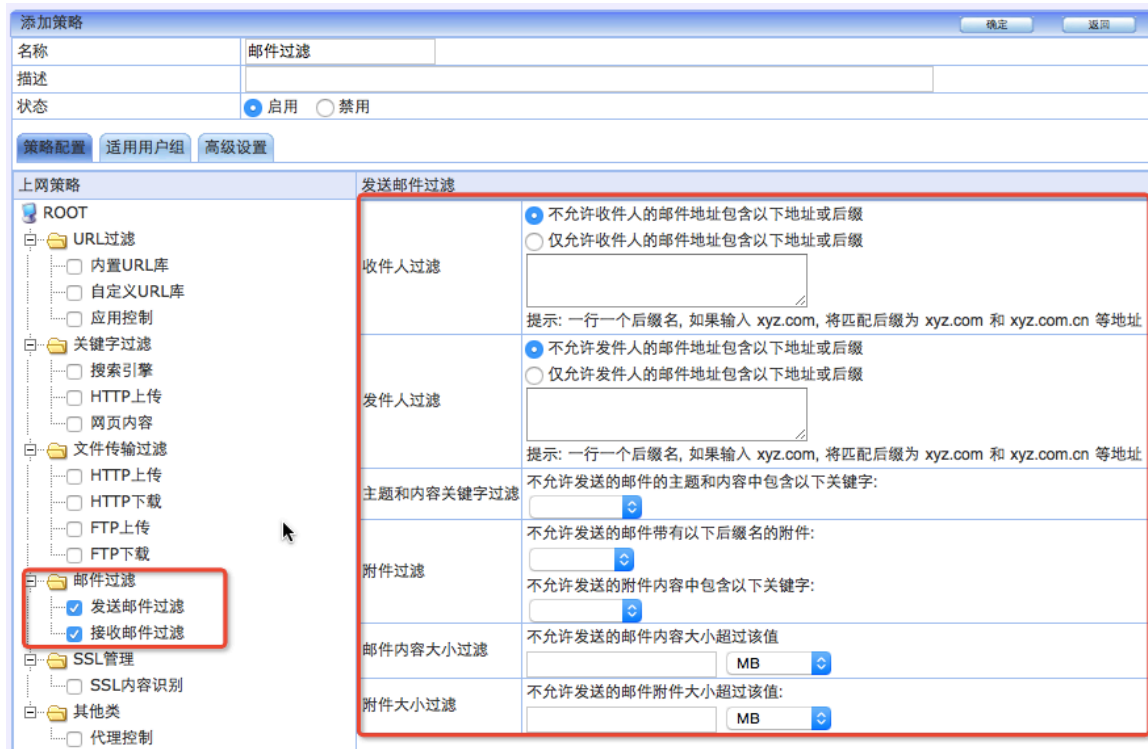
- 地址
- 域名后缀

## ■ 主题和内容

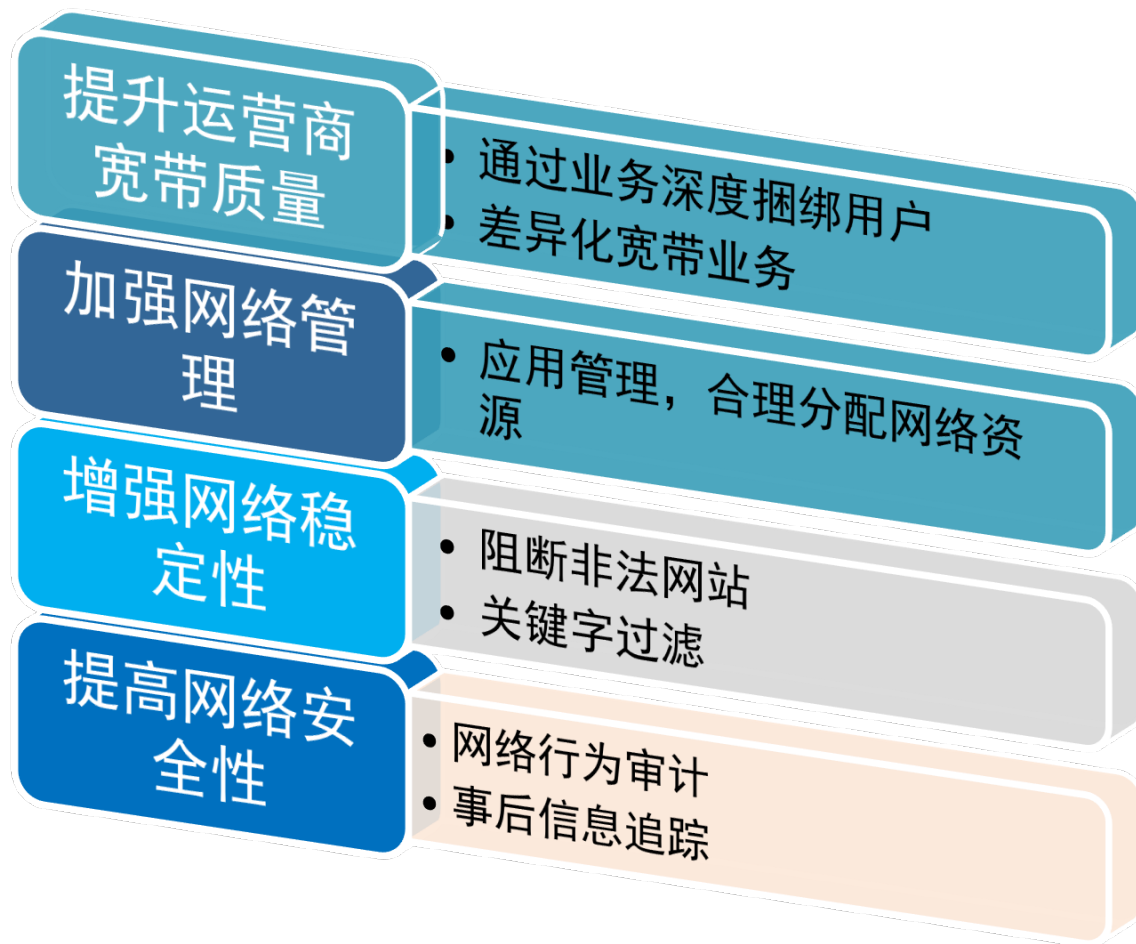
- 关键字过滤
- 邮件内容大小

## ■ 附件过滤

- 文件类型
- 关键词
- 附件大小



# Cross 带来的价值



# 产品优势

## 国内领先的URL库

- 国内最大URL库
- 每天更新10万条

## 超强的稳定性

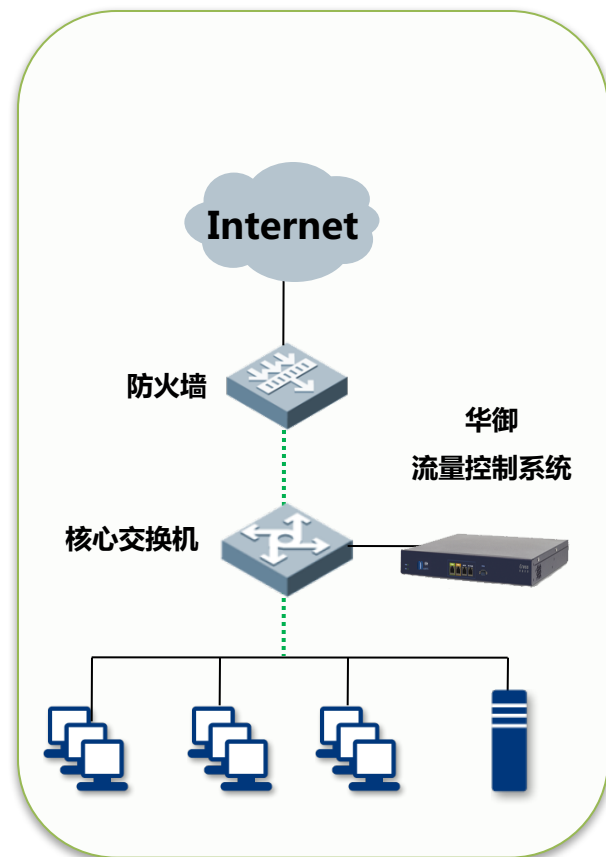
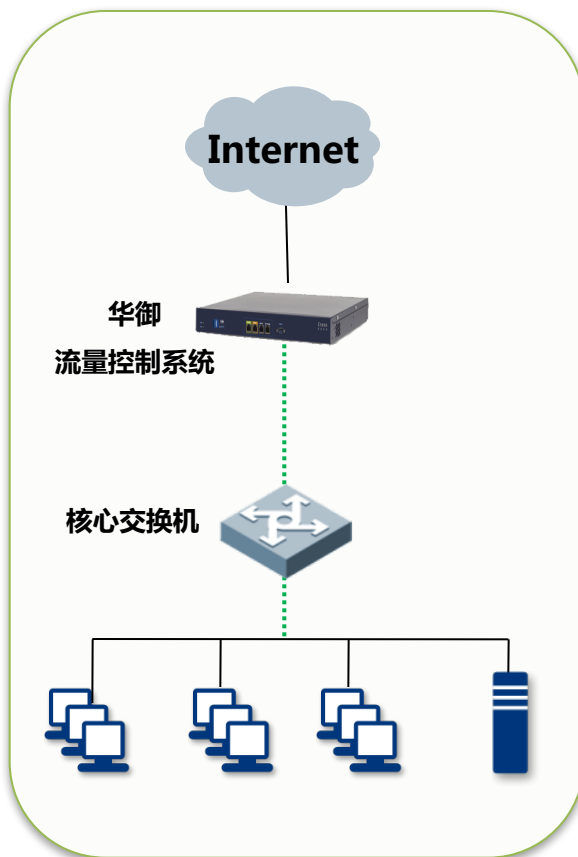
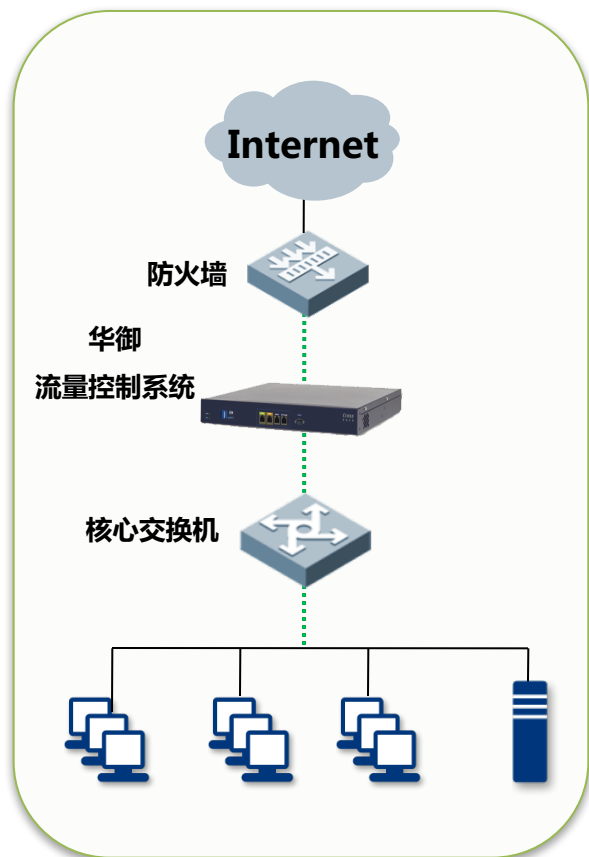
- 99.999%的稳定性
- 拥有大量超过5年的用户

## 精准的网络应用识别

- 95%以上的识别率
- 700种以上的应用识别与管控

# 产品部署

支持多种部署模式，网桥模式，网关模式，旁路模式



# 选型参考

规格说明		Cross8100-10	Cross8100-20	Cross8100-25	Cross8100-30	Cross8100-40	Cross8100-50	Cross8100-60	Cross8100-70
<b>性能参数</b>									
性能参数	适用用户数	400人	800人	1500人	2000人	3000人	5000人	20000人	50000人
	吞吐量	100Mbps	200Mbps	400Mbps	600Mbps	1Gbps	2Gbps	4Gbps	6Gbps
	管理带宽	50M	100M	200Mbps	300M	500M	1G	2G	3G
	最大并发连接数	80万	100万	120万	150万	180万	200万	300万	400万
<b>硬件参数</b>									
接口	板载接口	6电千兆	6电千兆	6电千兆	6电千兆	6电千兆	2千兆电口	2千兆电口	2千兆电口
	扩展插槽	无	无	1个扩展插槽	1个扩展插槽	1个扩展插槽	4个扩展插槽	4个扩展插槽	4个扩展插槽
	USB接口数量	2	2	2	2	2	2	2	2
	RS232串口(RJ45)	√	√	√	√	√	√	√	√
旁路模块	内置电口旁路模块	√ (二路)	√ (二路)	√ (二路)	√ (二路)	√ (二路)	×	×	×
	内置光口旁路模块	×	×	×	×	×	×	×	×
	支持外置光口旁路模块	×	×	可选	可选	可选	可选	可选	可选
存储	硬盘	500G	500G	500G	500G	500G	1T	1T	1T
电源	电源及电压	交流110~240V	交流110~240V	交流110~240V	交流110~240V	交流110~240V	交流110~240V	交流110~240V	交流110~240V
	最大功率	100W	100W	350W	350W	350W	350W	460W	600W
	冗余电源	×	×	× (可选配件)	× (可选配件)	× (可选配件)	× (可选配件)	√	√
设备规格	机箱尺寸(WxDxH mm)	426*330*44	426*330*44	430*434*88	430*434*88	430*434*88	430*560*88	430*560*88	430*560*88
	机箱高度	1U	1U	2U	2U	2U	2U	2U	2U
	设备重量(Kg)	6	6	15	15	15	20	20	20

# 选型参考

规格说明		Cross8100-10	Cross8100-20	Cross8100-25	Cross8100-30	Cross8100-40	Cross8100-50	Cross8100-60	Cross8100-70
扩展接口	扩展插槽	-	-	4端口千兆以太网电接口卡(RJ45) - 内置2对电口bypass		-	-	-	-
扩展接口	扩展插槽	-	-	4端口千兆以太网光接口卡(SFP) - 无内置bypass		-	-	-	-
扩展接口	扩展插槽	-	-	2端口千兆以太网电接口卡(RJ45) + 2端口千兆以太网光接口卡(SFP) - 内置1对电口bypass		-	-	-	-
扩展接口	扩展插槽	-	-	2端口千兆以太网光接口卡(SFP) - 内置1对光bypass		-	-	-	-
扩展接口	扩展插槽	-	-	2端口万兆以太网光接口卡(XFP) - 无内置bypass		-	-	-	-
扩展接口	扩展插槽	-	-	2端口万兆以太网光接口卡(XFP) - 内置1对万兆光bypass		-	-	-	-
扩展接口	扩展插槽	-	-	-	-	2端口千兆以太网电接口卡(RJ45) + 2端口千兆以太网光接口卡(SFP) - 内置1对电口bypass			
扩展接口	扩展插槽	-	-	-	-	4端口千兆以太网电接口卡(RJ45) + 4端口千兆以太网光接口卡(SFP) - 内置2对电口bypass			
扩展接口	扩展插槽	-	-	-	-	8端口千兆以太网电接口卡(RJ45) - 内置2对电口bypass			
扩展接口	扩展插槽	-	-	-	-	2端口万兆以太网光接口卡(XFP) - 无内置bypass			



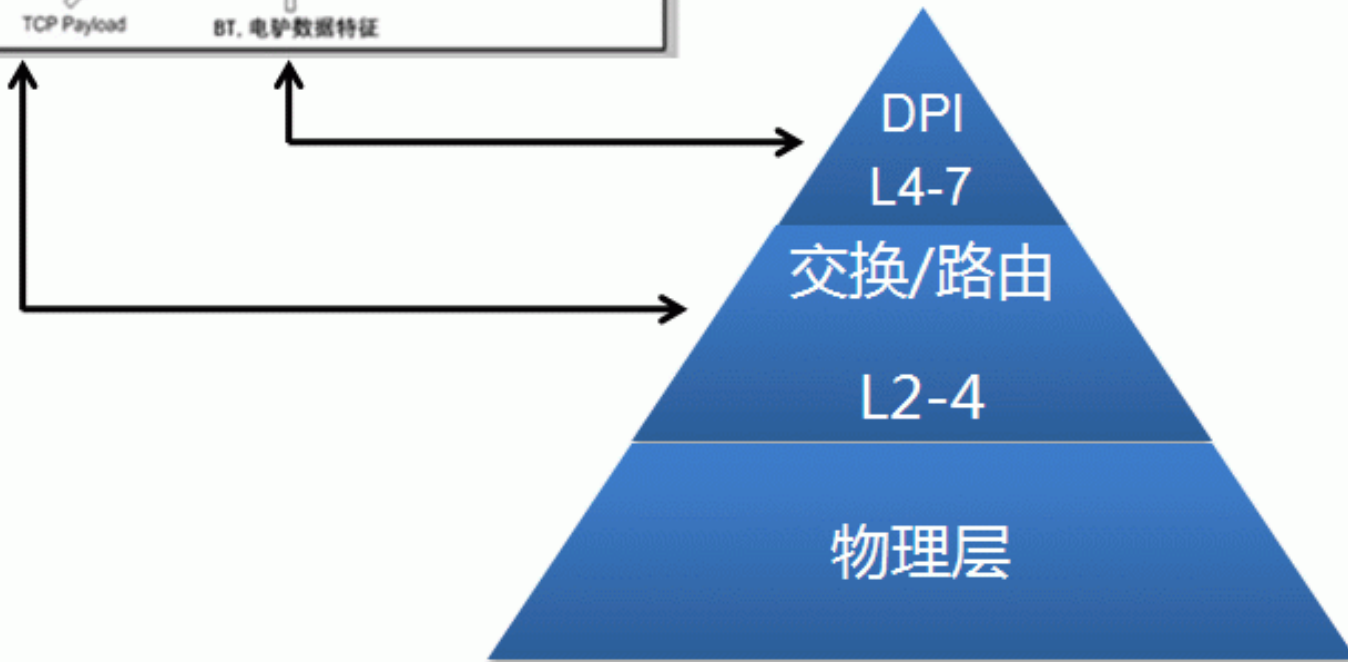
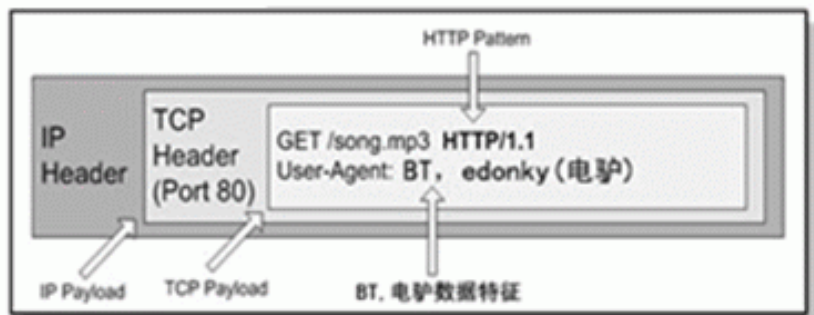


华御  
HUAYU.BJ

# 核心技术

# 深层数据包检测技术

深层数据分析示例：



# 应用行为识别技术

- 应用范围 — 加密方式传输的协议
  - 特点：有效载荷部分无特定规律
- 应对方法：根据传输行为区分，如包大小、TTL、TOS、IPID等

## Packet 1

数据包头 1 16字节  
数据包头 2 48字节  
数据包头 3 16字节  
数据包头 4 1412字节  
有效载荷 65500 字节  
.....

## Packet 2

数据包头 1 16字节  
数据包头 2 48字节  
数据包头 3 16字节  
数据包头 4 1412字节  
有效载荷 384 字节  
.....

# 衍生流识别技术

父数据流

## ■ 应用范围 —— 工作时衍生出的子数据流

1110....1010010...

- 子数据流属于没有直接父数据流
- 子数据流的流量占整个协议簇的很大部分

## ■ 传统的流控产品的识别率较低的原因

- 不能很好区分出子连接的父连接属性
- 由于限制 **101...01** 流量而 **001...11** 的子数据

流抢占更多网络资源的此消彼长的局势

子数据流1

子数据流2

# 精准的识别率



# 产品功能列表

功能分类	详细指标
部署模式	支持网关、网桥、旁路、多路网桥等部署模式，支持双机热备、多台集中管理；
设备管理	支持Web、CLI、SSH等管理方式、管理员支持分级管理，能将所有功能按需分配给不同的管理员
实时监控	支持提供设备实时CPU、内存、磁盘占用率、会话数、在线用户数、网络接口等设备资源信息；支持实时提供用户、应用流量排名、所有线路应用速率、流量管理状态；支持实时显示当天安全状况，最后发送的安全事件、时间、类型、次数等；
用户识别	支持以IP、MAC、IP + MAC绑定、用户名密码等方式认证用户，支持LDAP / AD / RADIUS / POP3等第三方认证手段；支持指定网段 / 帐号强制单点登录；支持帐号私有、共用控制、临时帐号申请；支持帐号有效期控制；用户帐号导入、IP + MAC地址扫描导入，或从AD服务器导入帐号和组织结构信息。
认证机制	新用户支持根据源IP段以IP / MAC / 计算机名等方式实现帐号自动命名，支持认证冲突检测，支持认证失败后权限管理，支持认证成功后页面跳转控制。
终端控制	能够控制终端使用操作系统类型、系统进程、硬盘文件、注册表进行控制，不满足预设规则不允许终端上网。

# 产品功能列表

功能分类	详细指标
文件控制	支持HTTP上传 / HTTP下载 / FTP上传 / FTP下载 / Email附件等形式外发文件的行为，支持基于扩展名识别并拦截外发文件；
网页管控	内置海量URL库且支持手工创建，支持基于URL地址 / 搜索词条 / 网页正文内包含的关键词过滤网页访问行为，同时可基于关键词过滤网络发帖、邮件外发行为，支持看帖但不准发帖，能收邮件但不准发邮件的细致管控功能。
高级管控	支持过滤SSL加密网站、加密邮件内容识别能够识别和过滤使用91VPN、51VPN、SogoVPN、UltraVPN、非常代理、无界浏览、自由门、非凡VPN、L2TP、PPTP等VPN软件来试图规避管理的行为，能够控制通过安装代理软件将自己的上网权限共享给他人的行为
应用识别	内置700多种网络主流应用，并进行了20多种分类，识别和管控IM聊天、Web视频、视频网站浏览、网上银行、网络电话、网络存储、网络游戏、网络炒股、P2P、流媒体、远程控制、代理翻墙软件等用户常用的网络协议；
P2P智能识别	通过DPI + DFI识别迅雷、Flashget、QQ旋风、等30多种常见P2P应用软件，利用智能P2P识别技术实现变种P2P、未知P2P全面识别与管控
邮件管控	支持完全封堵邮件收发行为，支持基于主题和内容关键字、收发件人地址、附件类型、大小等多种条件过滤外发邮件；

# 产品功能列表

功能分类	详细指标
上网安全	内置防火墙、能够防御DOS攻击、ARP欺骗防护、TCP / UDP / ICMP连接超时管理、等影响网关稳定性的多种安全风险。
上网授权	支持与组织结构一致的多级用户账号管理方式，可基于用户账号、IP、应用、行为、内容、时间段等多种因素管控上网权限、结合对象化的上网策略模版，实现上网权限在不同用户和用户组间的复用、集成、强制继承等效果；支持对用户的指定应用行为累计使用时长及最高流速进行监控，超出配额将采用禁止上网一段时间等措施解决，充分减少管理员人工干预的工作量。
流量管理	支持多线路复用、虚拟线路、虚拟自通道等功能；可基于应用类型、网站类型、文件类型及用户、时间、目标IP、优先级等条件分配带宽资源；支持由外网访问内网的流控；支持所有哦难怪乎带宽、连接数平均分配；
实时监控	实时监控CPU、硬盘、流量、连接、会话等状况，以及在线用户信息、流量排名、连接排名、应用排名等；实时查看用户上网日志纪律等。
上网审计	记录用户访问的网址、网页标题、网页内容；记录HTTP、FTP等外发文件行为，记录下载文件行为；记录发帖、发微博、微信朋友圈、Email、Webmail；记录QQ、MSN、雅虎通、飞信、Skype等聊天内容；纪律网游、炒股、影视娱乐、P2P下载、Telnet等应用行为；统计用户流量、上网时长等信息；



# 产品功能列表

功能分类	详细指标
多出口负载均衡	支持多互联网出口负载均衡、支持PPPOE拨号、支持根据比重带宽大小、固定指派、最佳路径算法等多种方式的负载均衡，满足接入相同运营商、不同运营商的链路负载均衡。
NAT地址转换	支持NAT地址转换、支持一对一地址转换、端口映射服务器地址池等功能
DHCP	支持DHCP自动地址分配、租期、固定地址分配、DHCP中级等。
告警	支持CPU、内存、会话数、网口流量超过限额告警，支持违规网站、违规搜索、违规发帖、违规上传、违规邮件、违规IM告警
VPN	支持IPsecVPN、SSLVPN，满足公司总部与分支机构加密互联、出差或在家办公人员加密登录公司服务器
百名单	支持IP百名单，百名单的IP将全部放行，并不受流量管理与审计、支持URL百名单，百名单中的URL全部放行、即时通讯百名单，只有在百名单中的账号才可以登录。
准入管理	支持用户准入互联网控制，通过MAC地址绑定（支持跨三层交换识别）、分配账号登录等不同方式实现用户互联网准入管理。



华御  
HUAYU.BJ

# 案例分析

# 案例1 - 湖南移动

## 网络接入现状

- 湖南移动集团客户数据接入业务的高速发展
- 移动WLAN网络逐步覆盖政府、金融、教育等集团单位及重要热点区域
- 网络行为管理问题逐渐凸显

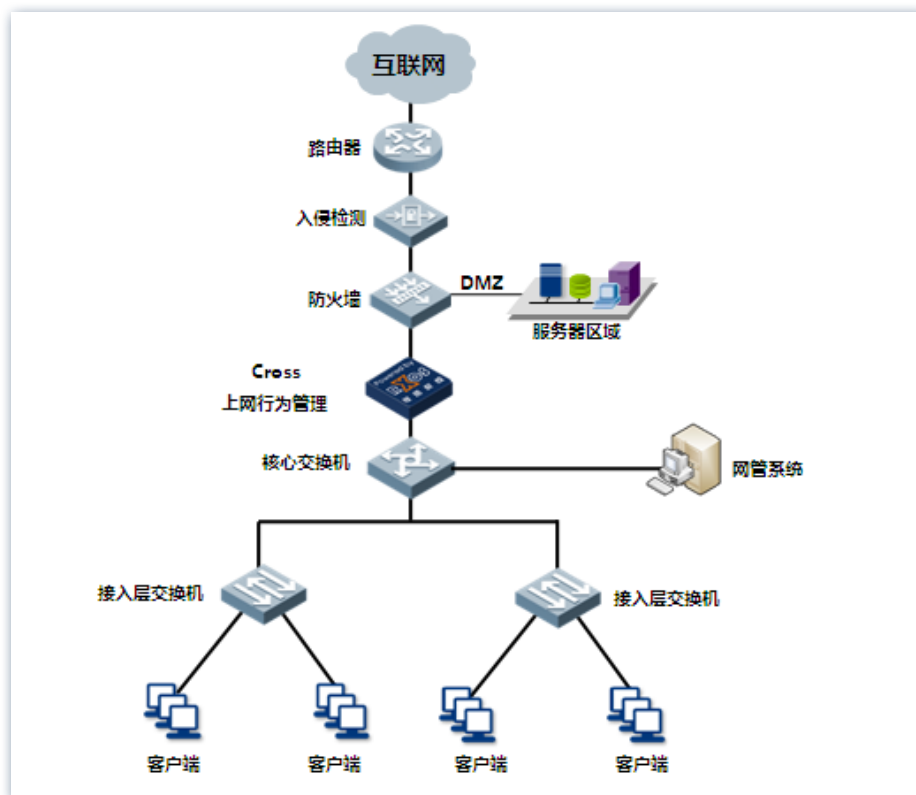
## 客户面临的网络行为管理问题

- 缺乏对敏感信息的审计与追踪
- 缺乏对非法言论、关键字进行有效过滤
- 缺乏对核心业务带宽的保障
- 缺乏对P2P下载、视频流量的有效控制
- 缺乏对网络行为的可视化

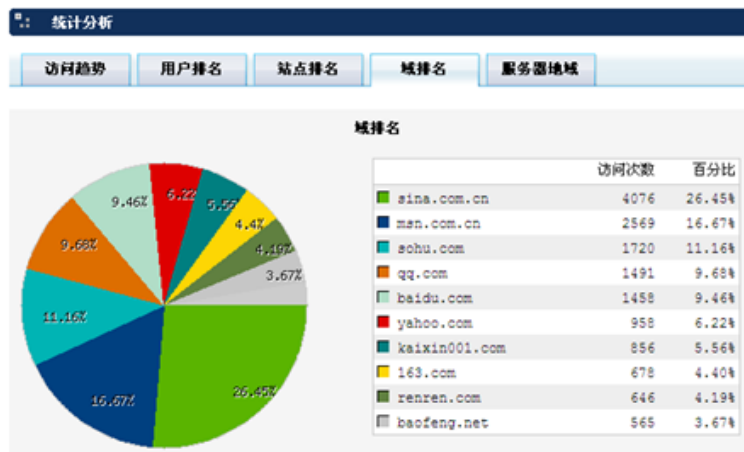
# 校园案例

## ■ 某校园现状

- 上网人数众多，高峰期达8000多人
- 缺乏对用户上网日志的审计
- 缺乏对外发信息的关键字过滤
- 少数用户占用 80% 的网络资源
- 连接数过大，造成基础设备压力较大
- 应用众多，缺乏管理



# 湖南移动 - 某校园网络现状



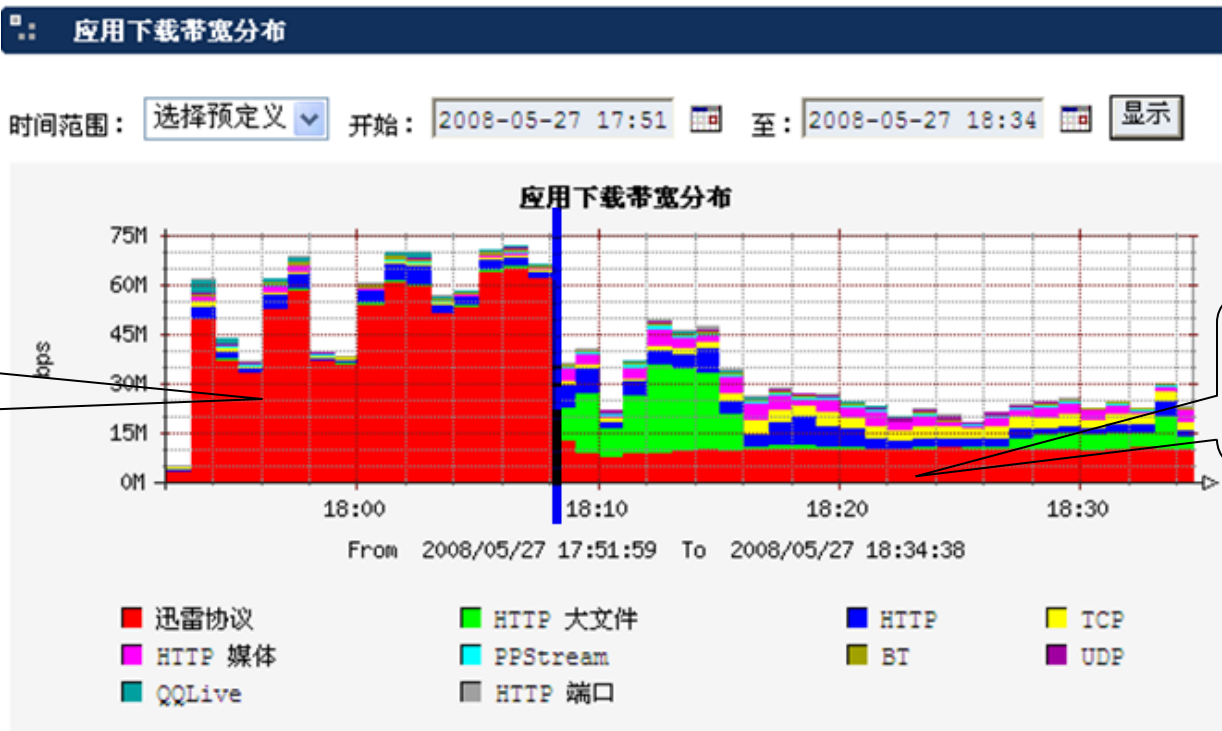
# 湖南移动 - 某校园网络现状

关键字		
编号	关键字	时间
1	蝎潘纺猫△旌肆	2009-12-21 14:59
2	北京找人化妆	2009-12-21 14:59
3	潜在在办公室	2009-12-21 14:59
4	filamin-repeat重复序列	2009-12-21 14:59
5	filamin repeat重复序列	2009-12-21 14:58
6	filamin repeat.	2009-12-21 14:58
7	找人化妆	2009-12-21 14:57

The screenshot displays the 'Cross' network management system. The main navigation bar includes '网络展示中心', '流量监视', '上网行为管理', '优化管理', '统计报告', and '系统设置'. The left sidebar lists various management functions such as '网页访问管理', '统计分析', 'URL 访问记录', '论坛发帖查询', '邮件管理', 'IM 聊天管理', and '新浪 UC'. The main content area shows the path '» 上网行为管理 » 邮件管理 » POP3 邮件记录'. Below this, a table titled 'POP3 邮件记录' lists email entries with columns for '帐号', '主题', '客户端', '发件人/收件人', and '时间'.

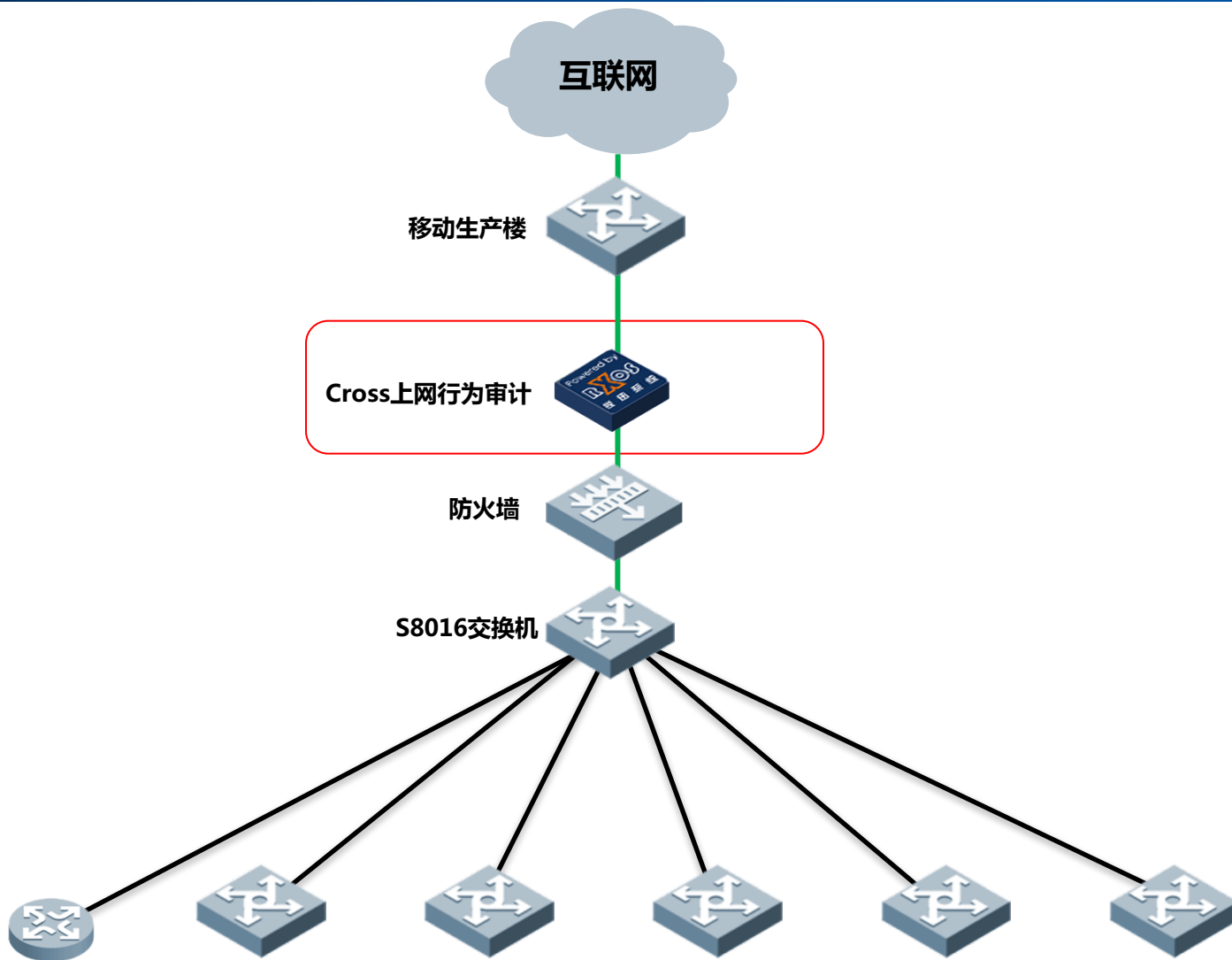
帐号	主题	客户端	发件人/收件人	时间
unknown <RECV> zhan@... .com	Up to 76% off on all watches while stocks last Size: 6065 Byte	10.4.133.208 00:1D:46:E1:CD:40	ba...@... .com zh...@... .com	2009-12-21 14:20:47
unknown <RECV> z...@... .com	Masters degree with no efforts. Size: 1363 Byte	10.4.133.208 00:1D:46:E1:CD:40	s...@... .com z...@... .com	2009-12-21 14:16:47
unknown <RECV> ...@... .com	111111 Size: 7916 Byte	10.4.133.208 00:1D:46:E1:CD:40	z...@... .com z...@... .com	2009-12-21 13:54:04

# 湖南移动 - 某校园网络现状



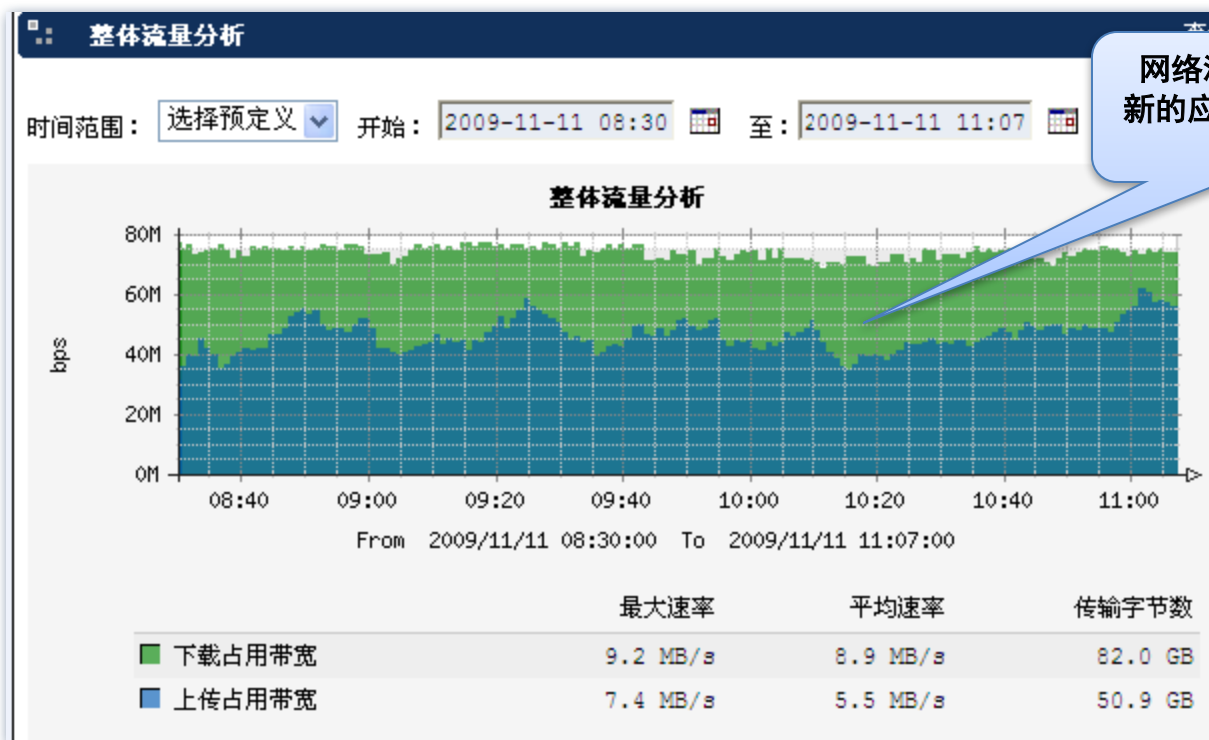
- **效果提升：**
- 关键字过滤、外发信息审计，提升了网络安全。
- 帮助用户提升了网络管理水平，随时可以看到网络中的细节，且即看即管。
- 整体带宽可利用率由原来的 25% 变为 55%，为新业务系统保驾护航。

# 案例2 - 白城市教育局





# 用户网络现状



网络满负荷运行  
新的应用无法打开

# 用户网络现状

资源分配严重失衡

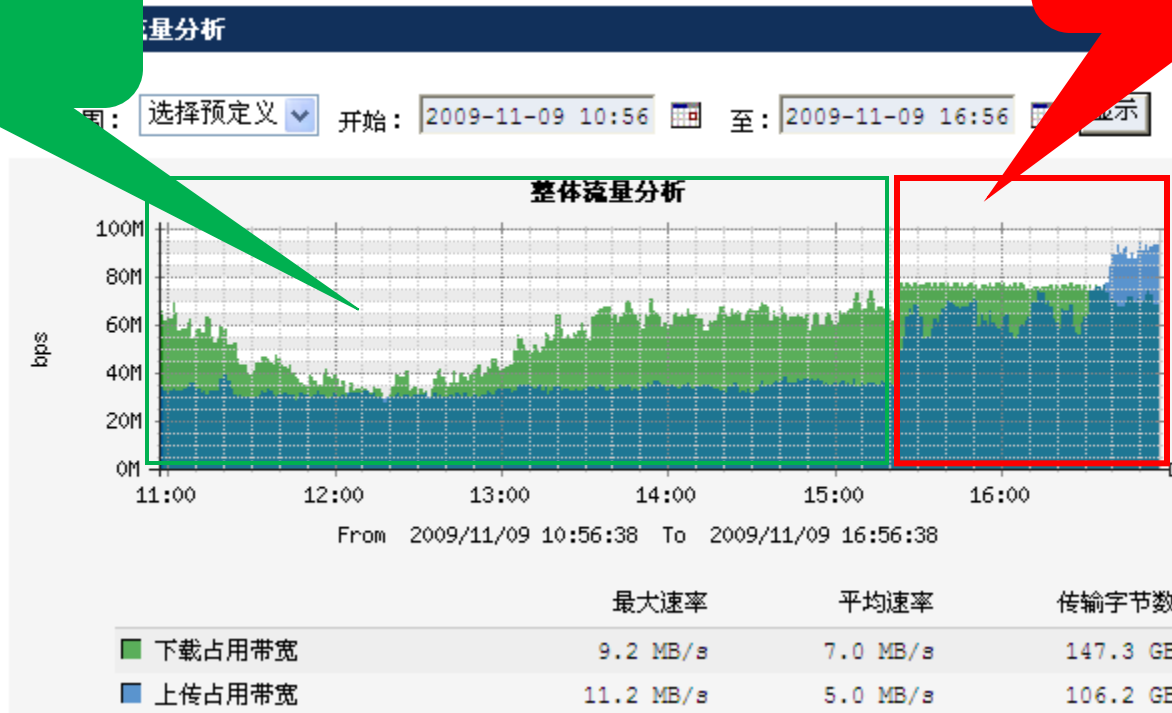
应用协议名称		占用百分比	备注
HTTP信息查询		14.5%	信息查询不到 20%
P2P 下载	迅雷	57.3%	娱乐性流量消耗了70%的 带宽
	HTTP 分块、大文件		
	BT		
视频	PPStream	14.8%	
	QVOD		
	风行		
其他		13%	

缺乏管理手段

# 方案效果

优化状态：平均下行带宽为60M，上行为35M，有充足的带宽给新应用

未优化状态：平均下行带宽为78M，已达到峰值，网络出现拥塞，响应缓慢



# 关于华御

## 公司

注册资金1000万

成功服务与国内外5000家以上客户

## 团队

拥有多位资深行业专家

绝大部分在应用优化领域超过8年以上经验

## 产品

上网行为管理产品、流量控制产品

下一代防火墙、VPN

## 资质

公安部销售许可，电信入网许可、软件著作权

# 华御部分客户

运营商	湖南省移动公司 吉林省白城市移动公司 吉林省长春市移动 吉林省长春市电信公司
政府行业	国家建设部 北京市政府 内蒙古自治区省政府 内蒙古出口检验检疫管理局 北京市消防局 吉林省建设厅 吉林省交通厅 吉林省统计局 吉林省财政厅 吉林省进出口检验检疫管理局 白城市政府 吉林省公安厅
教育行业	大连理工大学 河北科技大学 北方工业大学 白城市教育局 首都师范大学 北京市政管理学校 北京财贸职业学院 北京师范大学附属育新中学 北京经贸职业学院 南海教育局
电力行业	华北电力总部、山西省电力公司、中国冶金科工集团、神华亿利电厂、枣矿集团下属单位
建设行业	中国铁路第五集团有限公司 中国铁路第六集团有限公司 北京城建道桥集团
研究院	中国食品发酵研究院、北京市测绘设计研究院、北京勘察设计研究院、北京机电研究院、建设部综合勘察研究院、北京电影研究所、北京声学研究所
军队	中国人民解放军空军司令部 中国人民解放军海军司令部



华御  
HUAYU.BJ

谢谢