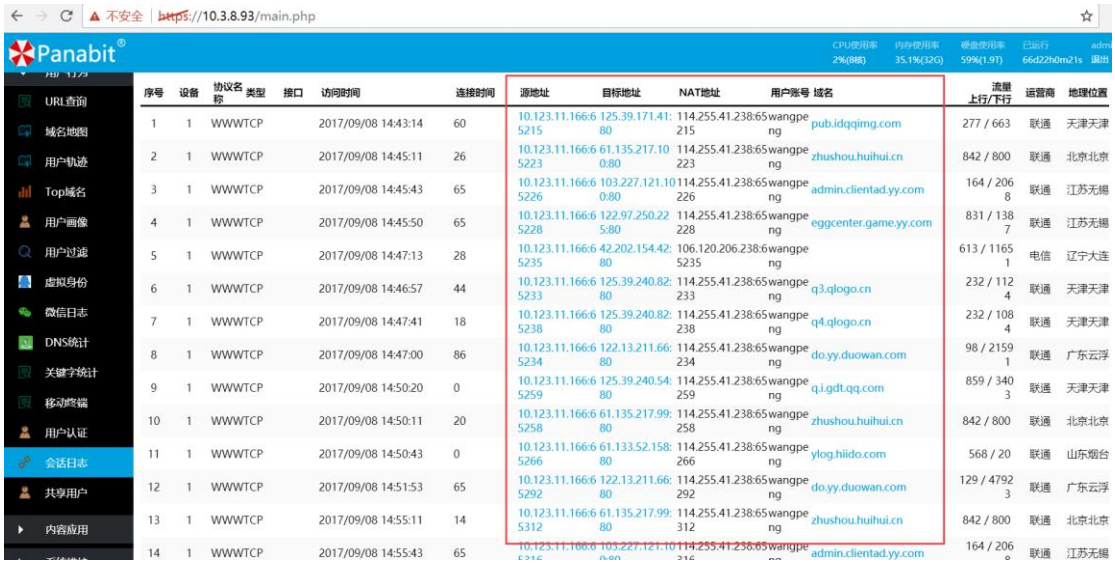
校园网上网数据分析解决方案

满足“151 号令”和《网络安全法》需求—会话日志

校园网内部人员非常多，学生上网访问的内容也难免会有一些不符合国家相关规定或者涉及到“黄、赌、毒”内容。作为校园网网络总出口，必须留存相关人员上网记录，以便发生网络安全事件后进行追查。例如：某人上网攻击了政府的某个部门的网站，需要通过校园网出口 NAT 日志来定位到攻击来源自那个网吧的那台计算机，再根据当时的时间，定位到人。Panabit 提供全网统一用户认证日志+NAT 日志+URL 日志，同时提供 1:1 的日志输出，在一张表里面可以体现访问时间、源地址、目标地址、NAT 地址、账号信息、域名、协议类型、7 层协议名称、流量等元素，完整保留网络中的相关信息。当发生相关网关安全事件时候，通过 NAT 日志、帐号的登录信息以及 URL 访问等记录信息，可以定位到具体上网用户，满足《网络安全法》和“151 号令”相关要求。



满足“151 号令”和《网络安全法》需求—虚拟身份日志

微信、QQ 等聊天工具的发展，增加了人们的沟通方式。但如果某人通过 QQ 群，微信群发表不良言论（尤其是涉及到反动、危害民族团结言论）网监有可能要求校园网出口通过 QQ 号码或者微信 ID 来对应于上网人员。Panabit 还提供这个功能，通过 QQ 号码，微信 ID、邮箱地址或者论坛用户名查询到到底这些虚拟身份对应是谁。

序号	设备	QQ号码	用户地址	MAC	用户账号	访问时间	目标地址
101	26	29[redacted]35	10.9.12.6:4031	ac-74-09-c2-a6-01		2018/11/07 14:25:21	125.39.132.147:8000
102	26	20[redacted]7754	10.93.224.77:63369	ac-74-09-c2-a6-01	2016220494	2018/11/07 14:27:04	163.177.71.224:80
103	26	274[redacted]360	10.97.17.73:63383	ac-74-09-c2-a6-01	2015221407	2018/11/07 14:27:10	123.151.176.23:8080
104	26	254[redacted]6259	10.93.16.201:55389	ac-74-09-c2-a6-01	2017220305	2018/11/07 14:27:24	123.151.176.23:8080
105	26	201[redacted]7754	10.93.224.129:53698	ac-74-09-c2-a6-01	2016220494	2018/11/07 14:27:47	123.151.176.23:8080
59	26	2745[redacted]60	10.97.17.73:63383	ac-74-09-c2-a6-01	2015221407	2018/11/07 14:27:10	123.151.176.23:8080
60	26	2542[redacted]259	10.93.16.201:55389	ac-74-09-c2-a6-01	2017220305	2018/11/07 14:27:24	123.151.176.23:8080
61	26	2015[redacted]754	10.93.224.129:53698	ac-74-09-c2-a6-01	2016220494	2018/11/07 14:27:47	123.151.176.23:8080

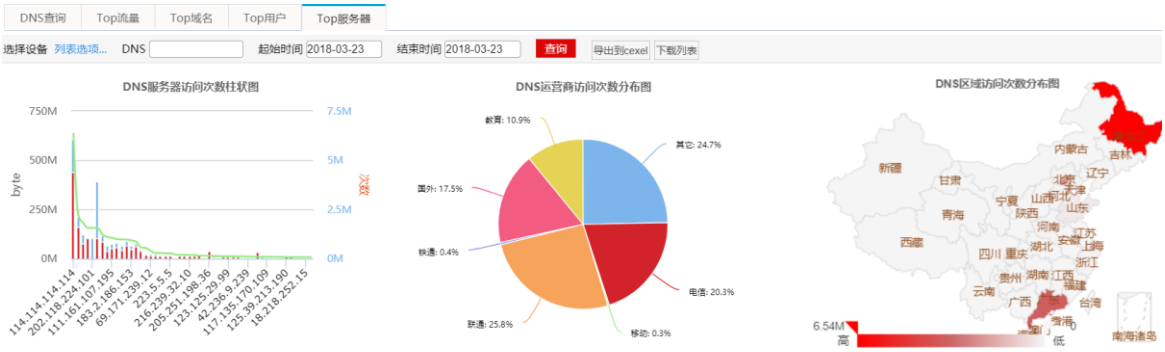
对外访问 TOP 域名分析

域名日志的访问频率和吞吐的变化，经常会伴随着网络上一些关键事件的发生。观察域名排名变化，是追踪分析这些事件的有效手段。例如一个不熟悉的域名，突然访问量急剧上升，一般都伴随着病毒或者网站挂马的发生。一些互联网营销手段也会推动域名的急剧变化，比如 360 推送微软升级，会引起微软升级服务器访问频率急剧上升。同时，观察某个域名的流量上下行比例，也可推测它提供的服务是否存在问题。

序号		域名	访问次数	访问差量	上行流量(Byte)	下行流量(Byte)	总流量(Byte)
1	+	client.9yin.woniu.com 域名分析	170220	170220	33.14M	24.8G	24.84G
2	+	www.playwkc.com 域名分析	18973	18973	30.89M	46.65M	77.54M
3	+	ff14.clientdown.sdo.com 域名分析	12641	12641	3.53M	3.98G	3.98G
4	+	liven.9666.info 域名分析	5086	5086	2.26M	2.39M	4.65M
5	+	videocdn.quweikm.com 域名分析	2938	2938	1.3M	44.69M	45.99M
6	+	speed.swarma.org 域名分析	2663	2663	1.3M	1.6M	2.9M
7	+	iqiyi.com-l-iqiyi.com 域名分析	2232	2232	1.91M	506.4M	508.31M
8	+	videocdn.hndtl.com 域名分析	1749	1749	1.64M	29.13M	30.77M
9	+	images.uppublish.com 域名分析	1621	1621	666.28K	80.59M	81.25M
10	+	helpgamemoney1.ksmobile.com 域名分析	1577	1577	1.26M	8.3M	9.56M
11	+	dmd-fifajs-native-major.youku.com 域名分析	1460	1460	851.04K	1.54G	1.54G
12	+	3graugmt1gy51hp3zfa5uo.ourdvsss.com 域名分析	1434	1434	643.67K	5.31M	5.96M
13	+	dl.ms.ccnu.edu.cn 域名分析	1174	1174	401.83K	305.85M	306.25M
14	+	ttdbj.com 域名分析	1143	1143	620.55K	37.89M	38.51M
15	+	alcdn.normal.vip.lixian.xunlei.com 域名分析	1111	1111	342.99K	583K	925.99K

校园网 DNS 服务器统计分析

在校园网网络优化中，对用户体验影响最大的辅助协议是 DNS，它关系到客户访问很多应用的使用感受，以下是当前在网 DNS 服务器排名、流量的运营商分布和地域分布。



序号	设备	DNS	访问次数	上行流量	下行流量	总流量	运营商	地理位置
1	1	114.114.114.114	6347952	157.01M	420.26M	577.27M	其它	114DNS
2	1	8.8.8.8	2234001	51.45M	151.98M	203.43M	国外	GOOGLE
3	1	101.226.4.6	1823046	41.85M	73.97M	115.82M	电信	上海
4	1	202.1[illegible]24.177	1558180	0	99.71M	99.71M	教育	黑[illegible]江
5	1	202.1[illegible]4.101	1555901	99.67M	3.94K	99.68M	教育	黑[illegible]江
6	1	61.1[illegible]177	1554041	271.92M	99.59M	371.51M	联通	[illegible]
7	1	202.9[illegible]4.69	1224060	34.67M	79.61M	114.28M	联通	[illegible]江
8	1	182.254.20.198	1101121	28.14M	35.29M	63.43M	电信	广东
9	1	111.161.107.195	1055210	20.29M	50.12M	70.41M	联通	天津

如图所示：某高校的校内 DNS 排在第四和第五名，大量用户使用校外 DNS。这类使用外部 DNS 的现象，对校园网有两个重要影响：

1) 使用校外 DNS 可能造成部分校内的网站无法解析，特别是出于安全考虑不对外公开的内部网站。

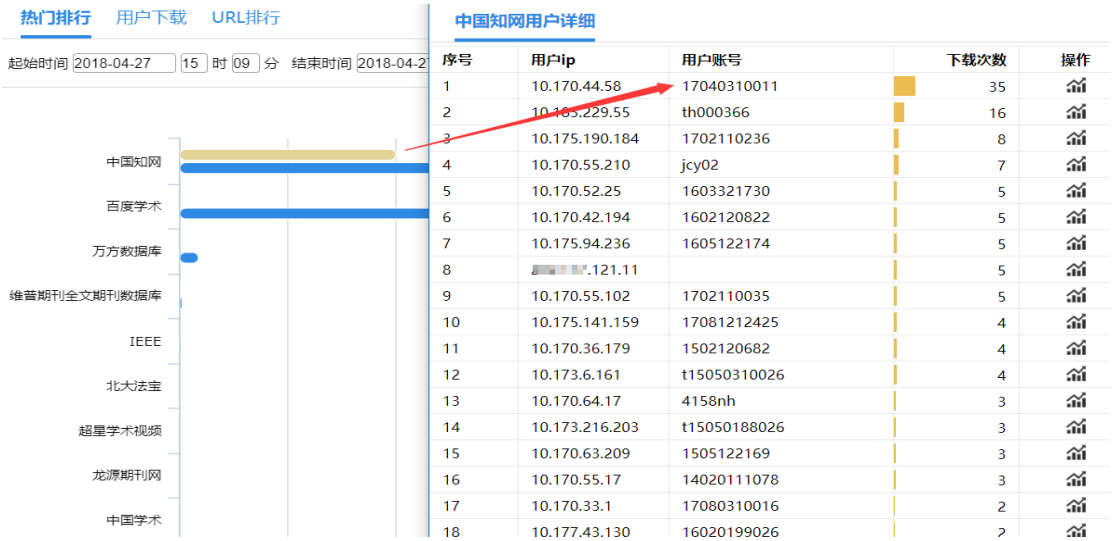
2) 应用流量引导时候，如果用户不使用你的 DNS，所有调度都会失败。

建议采取 DNS 智能管控技术，修正接入用户的 DNS 配置，降低它网解析率。对校内网站进行白名单干预，对敏感重载应用进行 DNS 重定向。与校内 DNS 服务器联动管理，

严控 DNS 解析，共同管理和优化校园网络。

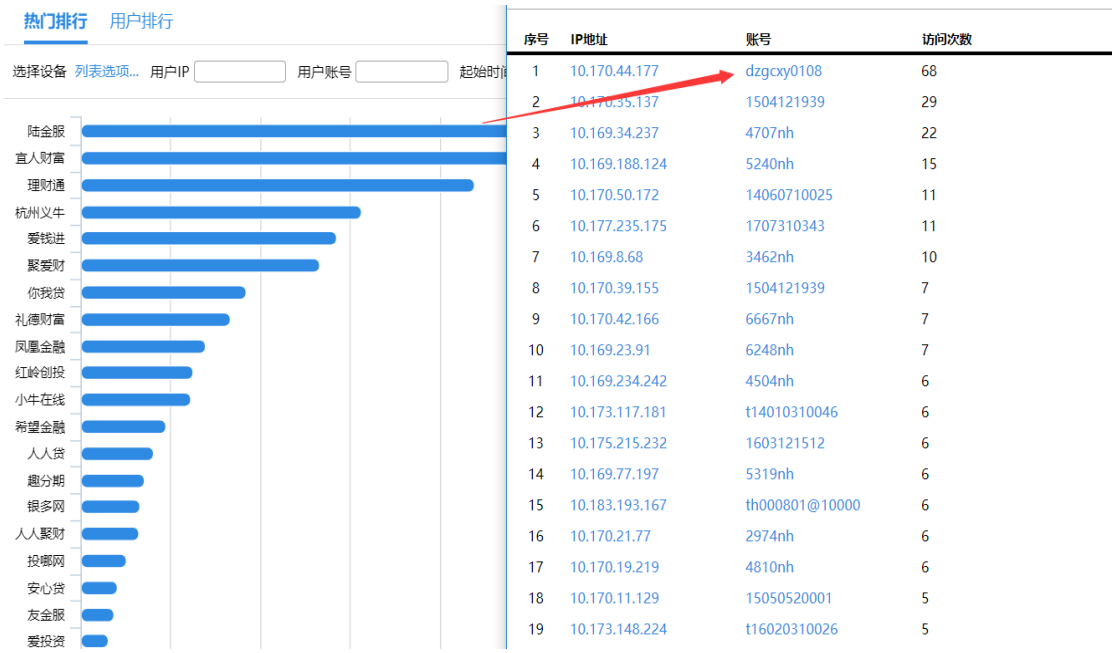
校内用户访问校外图书馆资源分析

通过 Panabit 数据分析，对校内用户访问图书馆资源进行统计，来发现那些图书馆属于热门资源，那些图书馆资源属于冷门资源，便于高校第二年购买图书馆资源参考。同时，对图书馆资源下载进行排名，通过下载次数，发现和定位恶意下载用户。



校内访问校园贷网站分析

教育部与银监会联合发布了《关于加强校园不良网络借贷风险防范和教育引导工作的通知》，明确要求各高校建立校园不良网络借贷日常监测机制和实时预警机制，同时，建立校园不良网络借贷应对处置机制。 通过 Panabit 内置校园贷特征码例如：名校贷，学生贷，云分期，我来贷，拍来贷，期乐、52 校园、趣分期、爱学贷，99 分期、优分期等，通过访问这些网站的频率排名，分析出可能产生校园贷的高危用户。



序号	IP地址	账号	访问次数
1	10.170.44.177	dzgcxy0108	68
2	10.170.35.137	1504121939	29
3	10.169.34.237	4707nh	22
4	10.169.188.124	5240nh	15
5	10.170.50.172	14060710025	11
6	10.177.235.175	1707310343	11
7	10.169.8.68	3462nh	10
8	10.170.39.155	1504121939	7
9	10.170.42.166	6667nh	7
10	10.169.23.91	6248nh	7
11	10.169.234.242	4504nh	6
12	10.173.117.181	t14010310046	6
13	10.175.215.232	1603121512	6
14	10.169.77.197	5319nh	6
15	10.183.193.167	th000801@10000	6
16	10.170.21.77	2974nh	6
17	10.170.19.219	4810nh	6
18	10.170.11.129	15050520001	5
19	10.173.148.224	t16020310026	5

校内共享用户数据分析

校园网内部总有部分人通过小路由器或者 WiFi 共享等模式进行共享上网，这对学校收费以及校内官方无线信号都造成不良影响，因此需要通过数据分析，找出共享用户并进行相关管控。

Panabit 共享检测技术是将用户上网的各类终端以及应用协议数据包中的一些特征进行分析统计和计算推断出共享终端的数量。使用方法有：IPID 轨迹检测法、时钟偏移检测法、应用协议检测、协议诱导等多种方法，达到共享检测 95%以上的准确性。

同时，配合流控策略、HTTP 管控策略、并发控制等策略，发现共享用户后进行综合管控。

策略组 网购

策略编号 3 (1~65535)

匹配条件

源接口 任意接口

VLAN 0 10或10-20,0表示忽略此条件

内网IP 任意地址

访问方法 任意

访问域名 任意域名

文件类型 任意类型

共享用户>= 1 (个, 0~255, 0表示忽略)

移动设备>= 1 (个, 0~255, 0表示忽略)

QQ用户数>= 1 (个, 0~255, 0表示忽略)

每个IP只匹配一次 否

执行动作

执行动作 信息提示

输出线路/接口 原路返回

提示信息 您的终端数已超出限制，请与网管联系。