**企业流控全解析—与运营商流控的需求及技术对比**

企业流控和运营商ISP流控有着很大的区别，这表现在它们的网络环境、流控前提、流控需求、流控目的都不一样，因此，面向运营商的DPI七层流控技术并不一定适合企业。目前存在部分管理员使用免费版七层运营商流控软件产品管理企业网络的情况，这一方面由于部分厂家有意、无意混淆运营商流控和企业流控产品，另一方面由于市场上少有性价比高的、可免费下载体验的企业流控软件产品，因此，企业在实际购买流控及上网行为管理产品时，还应当从多方面进行全面的了解。本文对企业流控的各个方面做了详细的分析，希望能起到明辨是非、抛砖引玉的作用。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能项** | **企业需求** | **运营商需求** | **UTMWALL混合流控** | **DPI七层流控** |
| **一、总体比较** | | | | |
| **近期网络流量变化** | 1）随着百度网盘、115网盘、网络视频网站本地化服务及本地ISP WEB缓存等新产品、新技术的出现，HTTP流量超过了P2P流量成为占用带宽最大的应用，传统基于特征识别的七层流控不在那么重要，更多的用于多WAN口的应用分流  2）企事业单位接入带宽越来越大、越来越稳定，管理越来越规范，带宽空余的情况也越来越普遍，因此也不一定非要做流量控制；于此相反，运营商逐利的本质注定其要用有限的带宽接入无限的用户，因此必须做出口应用流量控制，以节省成本 | | | |
| **1.1上级ISP对本单位流量的收费政策** | 上级ISP对本单位的流量无差别的收费 | 上级ISP对本单位的流量有差别的收费，流向外部网络的收费高，本地网络内的收费低 | <空> | <空> |
| **1.2本单位对上网用户的收费政策** | 一般都是免费上网 | 对用户收费，一般通过PPPoE拨号等认证方式避免用户逃费及充分利用带宽 | <空> | <空> |
| **1.3 WAN口数** | 1个，或者有多个，但用于连接多条相互隔离的专网 | 多个，1个ISP也可能有多条线路，上级ISP支持PPPoE多拨 | 1~无限制WAN口，内外网任何一块网卡均可以作为管理网卡 | 1~无限制WAN口，有的需要专门的管理网卡 |
| **1.4 部署方式** | 边界网关、透明网桥(多对) | 透明网桥 | 边界网关、透明网桥(多对) | 透明网桥方式，部分产品网桥数受限；很少产品同时具备边界网关方式，因为边界网关附带各种NAT、路由及上网日志等要求，不容易满足 |
| **1.5 适用单位** | 政府、企业、事业、学校、电商、专网、IDC等单位 | ISP（互联网宽带运营商、小区宽带接入商）、网吧 | 互联网或专网联网单位；使用者入门要求低，无需专业技能，看得懂汉字即可 | 二线城市（有PPPoE多拨）小区宽带接入私营业主身兼Linux、BSD等系统及网络管理员 |
| **1.6流控目的** | **1）在带宽耗尽时，优先保证与本单位业务有关的关键应用；**  **2）在带宽空余时，不要限制非关键应用的带宽；**  **3）审计、定位、剔除个别用户的恶意流量**  **4）保障服务器应用接入的QoS** | **1）在不增加带宽接入成本的前提下，尽量多地接入收费用户；**  **2）优先保证WEB浏览、网络游戏、网络聊天等交互式应用的QoS，尽量抑制去往外网的P2P流量** | <同企业需求> | <同运营商需求> |
| **1.7流控原则** | **保障关键应用，合理利用带宽** | 抑制灰色流量，合理分配应用路由 | **1）以纯七层流控为耻，以混合流控为荣，达到自主可控、长期有效的目的；**  **2)一步到位卖产品，在保障流控效果的前提下，绝不收取用户的流控特征库升级费** | 1）以四层流控为耻，以纯七层流控为荣，达到精细控制应用路由和带宽的目的  2）以维护七层流控特征库持续向用户收费为生 |
| **1.8流控技术** | <空> | <空> | **以用户为对象，6元组四层流控+80端口七层流控+0特征库的混合流控技术，白名单方式流控，不用关注各个非关键应用的带宽，只需设置其总带宽，适用于非ISP的终端联网单位使用** | 以应用为对象，基于七层特征库的流量识别、控制及多WAN口分流技术，黑名单方式流控，类似防病毒的特征匹配，适用于带宽接入商、运营商 |
| **1.9 日常维护** | **说明：**除非关键应用有变化，否则不需要经常升级系统、变更策略 | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png  **说明：**由于互联网应用软件经常变化，所以需要经常升级系统、变更策略 | 1）不需要精通Linux、BSD的管理员就可以做日常维护；  2）不依赖于流量特征库，无需将时间花在升级特征库、调整流控策略上 | 1）需要精通Linux、BSD的管理员才能做日常维护；  2）依赖于厂家提供的流量特征库，平时需要频繁升级特征库、调整流控策略，**时间成本巨大**  **说明：**如果使用者是身兼管理员的个体户或企业业主则以上也不成问题 |
| **1.10 安全性** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\disable.png  **说明：**ISP只关心网络的连通性，不关心用户的安全性 | 1）专用安全操作系统，没有安全隐患；  2）**OS通过了公安部等权威部门的功能、性能及安全性检测** | 1）通用操作系统，不能保证自身安全，有各种破解版、广告插件及第三方软件  2）没有通过权威部门的功能、性能及安全性检测  **H:\Notes\develop\icon\0\url.png安全漏洞详见最下方的参考文件。** |
| **1.11优缺点** | <空> | <空> | **优点：** 1） 100%控制非关键应用的带宽，从而100%保障关键应用的QoS； 2）后续维护不依赖于流量特征库，自主可控，长期有效，总体成本低；  3）可以在非互联网的专网内和服务器应用接入等场合发挥作用。  **缺点：** 无法按应用类型分析、控制出口流量的带宽。但仍有针对内网IP的应用审计和基于ISP IP数据库的策略路由。 | **优点：** 按照应用类型精细控制出口流量的带宽和路由。  **缺点：** 1）特征库不包含用户关键应用的特征，只能通过抑制特征库中已有应用的带宽，来间接保障用户关键应用的QoS； 2）用户没有自主性，完全依赖厂家的售后支持，需要频繁的升级特征库，随时存在流控失效的风险，而且总体费用高；  3）无法在非互联网的专网内和服务器应用接入等场合发挥作用。 |
| **二、四层流控功能比较** | | | | |
| **2.1 四层流量带宽实时分析** |  | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **1.6 qos_statusQoS状态** 查看QoS对象实时应用情况，确认限流的效果 | 一般都有 |
| **2.2 四层流量带宽趋势分析** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **1.4 network_status网络状态** 查看24小时之内各个网卡的带宽、会话数等使用趋势，并且留存至少60天的日志记录 | 一般都有，但不一定能留存60天的日志 |
| **2.3 四层ACL访问控制策略** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **5.7 firewall总控策略**  包含源IP及端口、协议、目的IP及端口、动作、网卡、方向、时间、用户认证等18个子项，既可以作为内外网的安全策略也可以作为流控策略 | 一般有简单的、非IP对象的四层ACL策略，既无法作为内外网的安全策略也无法作为流控策略，有的产品甚至直接省略 |
| **2.4 四层流量带宽控制** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **5.5 qos_objQoS对象** 与总控策略配合实现基于策略的QoS带宽控制  对于单IP限速，最好在接入交换机的端口上实现，这样做不仅效率高而且不影响网关的性能 | 一般都有，但和其它策略项关联性不强，例如没有和用户认证策略相关联 |
| **2.5 四层流量会话控制** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **5.4 session_obj会话对象** 与总控策略配合，控制单个用户各个应用的会话数及新建会话速率，可用于控制私接二级路由 | 一般只控制单个用户全部应用或全部TCP/UDP的会话数及新建会话速率，导致不能保障关键应用的QoS |
| **2.6 四层异常流量控制/抗内外网DoS攻击/动态剔除个别流量异常的会话** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\disable.png  **说明：**ISP只关心出口应用带宽分布，不关心某一具体源IP的流量明细 | **5.3 traffic_obj流量对象** 定时分析每个源IP的所有流量的会话，识别并记录持续流量和上传流量，根据设置可动态剔除这样的会话，并暂时屏蔽目的IP，并且留存至少60天的记录 | 一般都缺乏像样的技术手段，也没有相应的日志留存。 **当上传流量异常大时就成了DoS攻击流量，此时绝对不能用DPI七层应用识别的带宽或路由策略去压制或分流这样的流量，只能立刻将其丢弃，否则只会适得其反、雪上加霜，系统资源将被耗尽直至崩溃！** |
| **2.7 四层流量策略路由** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **5.1 ip_obj地址对象 5.7 firewall总控策略** 与总控策略配合，实现基于各大ISP IP数据库的出网和入网策略路由 | 一般只是出网策略路由，缺乏入网的策略路由 |
| **2.8 四层流量统计** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **1.8 traffic_stat流量统计**  对各总控策略中的源IP对象的各成员进行流量统计，即使当前无流量，仍能查看其历史流量统计 | 一般都有但和策略无关 |
| **2.9 在线主机流量明细** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\disable.png  **说明：**ISP只关心出口应用带宽分布，不关心某一具体源IP的流量明细 | **1.10 active_host在线主机**  实时查看当前流量状况，对源IP、应用以及流量明细这三种对象进行带宽、会话数、总流量等指标的排序，并且标示是否是持续流量和上传流量 | 一般都有，但细粒度不够 |
| **2.10 会话状态查询及控制** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **说明：**ISP不关心某一源IP的具体会话，更不会强制中断 | **1.11 session_status会话状态**  查询网络数据会话，包括源IP、源端口、协议、目的IP、目的端口、总控策略编号等查询条件，并可以将所查询到的会话强制中断 | 一般都有，但查询和中断功能不全 |
| **2.11 NAT包过滤日志** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **说明：**数据量太大，不易留存和查询，一般用Netflow流量日志 | **5.7 firewall总控策略**  实时记录网络数据包，包括时间、源IP、源端口、协议、目的IP、目的端口、总控策略编号及部分数据内容，是联网单位、涉密单位必配的审计手段 | 大多数都没有，或需要第三方服务器支持，安全性不佳 |
| **2.12 Netflow流量日志** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **4.5 netflowNetflow探针**  一条会话输出一条netflow数据流，与包过滤日志相比，效率更高、体积更小，更方便集中存储和查询 | 部分产品有 |
| **三、七层流控功能比较** | | | | |
| **3.1 七层应用带宽分析、应用审计/流量统计** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **1.9 specapp_state应用状态1.10 active_host在线主机** 没有按应用类别叠加的带宽趋势图，但有各源IP各七层应用关键特征流量（不是其全部流量）的带宽、会话数统计和日志，需要特殊应用特征库的支持 | 一般都有，但缺乏日志留存，或需要第三方服务器支持 |
| **3.2 七层应用带宽控制** | **说明：**能够直接定义关键应用，就能100%保障关键应用的QoS，不需要通过七层识别、控制非关键应用的带宽来间接保障 | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **5.7 firewall总控策略（QoS选项）**  系统自动分析80端口流量，并把不符合HTTP协议的目的IP放入FAKE80\_ip对象，再在总控策略里对其进行带宽、会话数等的控制；另外还可以自定义IPS策略，阻拦具有某一七层特征值的流量 | 一般都有，但策略设置繁琐，且和其它策略项关联性不强，例如没有和用户认证策略相关联 |
| **3.3 七层应用策略路由** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\disable.png **说明：**只有多WAN环境才有必要进行七层应用策略路由 | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **5.7 firewall总控策略（路由选项）** 系统自动分析80端口流量，并把不符合HTTP协议的目的IP放入FAKE80\_ip对象，再在总控策略里对其进行策略路由 | 大多数都有，例如：游戏、聊天应用走联通线路，下载应用走ADSL线路，不适用于专网或单个WAN口接入的环境 |
| **3.4 七层应用分类阻拦** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\disable.png **说明：**ISP不能阻拦用户的网络应用，只能控制网络应用的带宽 | **6.1 specapp_basic特殊应用总体设置**  **6.2 netgame特殊应用功能设置**  **7.5 idp_rulesIDP特征值规则**  对远程应用、下载存储、网络游戏、网络视频、聊天通讯、网银支付、证券交易等网络应用一键勾选阻拦；对一万多种非法攻击进行七层特征值过滤并阻拦 | 一般都没有，但可以通过控制应用带宽，间接实现阻拦应用 |
| **3.5 七层流量实时监控** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **说明：**ISP汇聚层流量太大，一般会通过交换机端口镜像的方式实时查看部分流量 | **1.12 realtime_monitor实时监控**  实时查询网络流量，可以显示数据包的7层内容，查询条件包括源IP、源端口、协议、目的IP、目的端口、总控策略编号等，不需要先记录、再下载查看 | 一般有类似的离线功能，但缺乏设置查询条件及直接监控的功能，需要先记录、再下载查看（记录文件的大小受制于存储器的大小），而且记录的流量没有对应的策略号，丧失了实时监控的意义 |
| **3.6 WEB审计日志** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | **6.3 netaudit网络审计**  包括DNS域名查询（https URL的域名）、URL、WEBPOST内容、WEB邮件正文、BBS论坛发帖内容等日志，本地留存至少60天，还可以显示URL级的实时带宽 | 一般有URL日志，有的需要第三方服务器，且缺乏日志统计和留存管理功能，缺乏URL级的实时带宽显示 |
| **3.7 WEB URL阻拦** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\disable.png **说明：**ISP不能阻拦用户的WEB请求 | **6.4 wafWEB审计过滤 6.6 dns_url_dbDNS&URL库**  对URL的各个组成部分分别进行内容匹配并阻拦 | 一般都没有，或有简单的自定义域名、URL过滤功能，缺乏大规模分类库及白名单控制 |
| **四、用户认证** | | | | |
| **4.1认证目的** | 基于用户角色的访问控制，和流控策略相关，一般不对用户收费 | 用于防止IP盗用，强制用户缴费，与流控策略无关 | 可以满足企业及运营商的需求 | 部分产品可以满足运营商的需求，但都不能满足企业的需求 |
| **4.2认证方法** | 要求PC、手机、平板等设备上都可以认证，在有三层交换机的网络环境下也可以认证 | 一般只要求PC或网关上认证，没有考虑三层交换机的网络环境 | **4.1 ipmacARP服务** 二层IP&MAC地址绑定  **4.2 mac3layerSNMP监控** 通过三层交换机的IP&MAC地址绑定  **5.7 firewall总控策略**  **8.3 usergroup用户组** WEB认证（本地、RADIUS、LDAP）  **9.3 pppoePPPOE总体设置**  PPPoE认证  **9.1 pptp_vpnPPTP总体设置**  PPTP VPN认证  **10.3 gatewayIPSEC VPN网关**  IPSEC VPN认证 | 一般有二层IP&MAC地址绑定、WEB认证、PPPoE认证功能，缺乏通过三层交换机的IP&MAC地址绑定与审计功能 |
| **4.3用户门户** | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | C:\Users\ibm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\enable.png | 提供https加密的用户自服务门户（WEB Portal），实现用户自主登录、登出，修改口令，展现可用URL，查看通知、流量、日志等功能 | 绝大部分都没有WEB Portal |
| **4.4认证效果** | <空> | <空> | 对内网和外网用户都可以实行基于用户组的访问控制策略；不同用户组成员，认证后获得不同的上网权限（可访问的目的、会话限制、带宽限制、流量限制、是否审计等） | 一般只针对内网用户进行认证；用户认证后，获得相同的上网权限，无法区分特权用户和普通用户 |

**本文链接：**

http://www.trustcomputing.com.cn/cn/index.php/support/techdocs/112-corp-tc-intro

**全文下载：**

http://www.trustcomputing.com.cn/utmwall-rom/Corp\_TC\_Intro.docx

**参考文件：**

1. 中神通UTMWALL网关管理员手册  
http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_v1.8\_Manual\_CN\_20131105.pdf

2. 企业流控实施指南—UTMWALL流控策略设置详解

http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_TC\_Setup.docx

3. 流量管理系统产品选型常见问答（FAQ）

http://www.trustcomputing.com.cn/cn/index.php/support/techdocs/98-tcfaq

4. 碧海威TMS系统用户手册20130227.pdf （85页）

http://wenku.baidu.com/view/4db443f9f90f76c661371a69.html

5. Panabit智能应用网关用户手册V2.0（72页）

http://forum.panabit.com/thread-10124-1-1.html

6. 流控大师资料导航

http://bbs.netzone.com/thread-1337-1-1.html

7. 新装爱快路由器用户使用手册

http://bbs.ikuai8.com/forum.php?mod=viewthread&tid=11994

8. 百为流控文档中心

http://doc.bytevalue.com/bvos.html

9. 流控软路由自身安全漏洞

panabit高危漏洞合集（官方后门、直接改admin密码以及系统命令执行）

http://www.wooyun.org/bugs/wooyun-2010-0114137

爱快流控路由最新版(iKuai8\_2.4.4\_Build20150604-17\_41)固件漏洞挖掘分析之一

http://www.wooyun.org/bugs/wooyun-2015-0122413