**企业流控实施指南—UTMWALL流控策略设置详解**

**目录**

[第一部分 标准流控策略 2](#_Toc405201675)

[1.1流控目标及策略 2](#_Toc405201676)

[1.2 实施步骤 2](#_Toc405201677)

[1.2.1初始设置 2](#_Toc405201678)

[1.2.2总控策略 3](#_Toc405201679)

[第二部分 异常流量控制 7](#_Toc405201680)

[2.1流控目标及策略 7](#_Toc405201681)

[2.2 实施步骤 7](#_Toc405201682)

[第三部分 QoS带宽控制 9](#_Toc405201683)

[3.1流控目标及策略 9](#_Toc405201684)

[3.2 实施步骤 9](#_Toc405201685)

一台UTMWALL设备安装好后，其G2网卡IP为*192.168.10.1*，管理员PC的IP设置为*192.168.10.2*，在WEB浏览器中输入***https://192.168.10.1:8443***，回车后忽略安全警告，在认证窗口中输入用户名***adm***，口令***adm@12345***，一切正确即可登陆WEBAdmin管理界面。

1、执行quickset初始设置，快速设置nic网卡IP及firewall标准流控策略

2、根据本单位关键应用的实际情况，新建、修改firewall总控策略

3、启用非关键应用traffic_obj流量对象的阻拦动作，调整各阈值

**图1 UTMWALL流控策略设置流程图**

3、针对非关键应用，启用qos_objQoS功能，调整qos_objQoS对象的带宽值

4、查看qos_statusQoS状态及network_status网络状态，确认流控效果是否有效

3、调整firewall总控策略中各session_obj会话对象的会话数等阈值

# 第一部分 标准流控策略

## 1.1流控目标及策略

确保各源IP的ping检测（ICMP）、DNS查询、WEB浏览、POP3收信、SMTP发信、FTP下载等关键应用的会话数充足，其余非关键应用的会话数均受到限制，使得带宽、会话不会被非关键应用的流量所占满。

## 1.2 实施步骤

### 1.2.1初始设置

1）点击左边主菜单的“dashboard系统管理>dashboard系统管理>quickset初始设置”菜单项，或者点击右上角quickset “设置”的快捷链接，出现quickset “初始设置”界面，如下图2所示。

****

**图2 “初始设置”界面**

2）根据实际网络环境设置运行方式、外网、内网、上网管理等参数，确保

“总控策略”项为“***标准流控策略***”

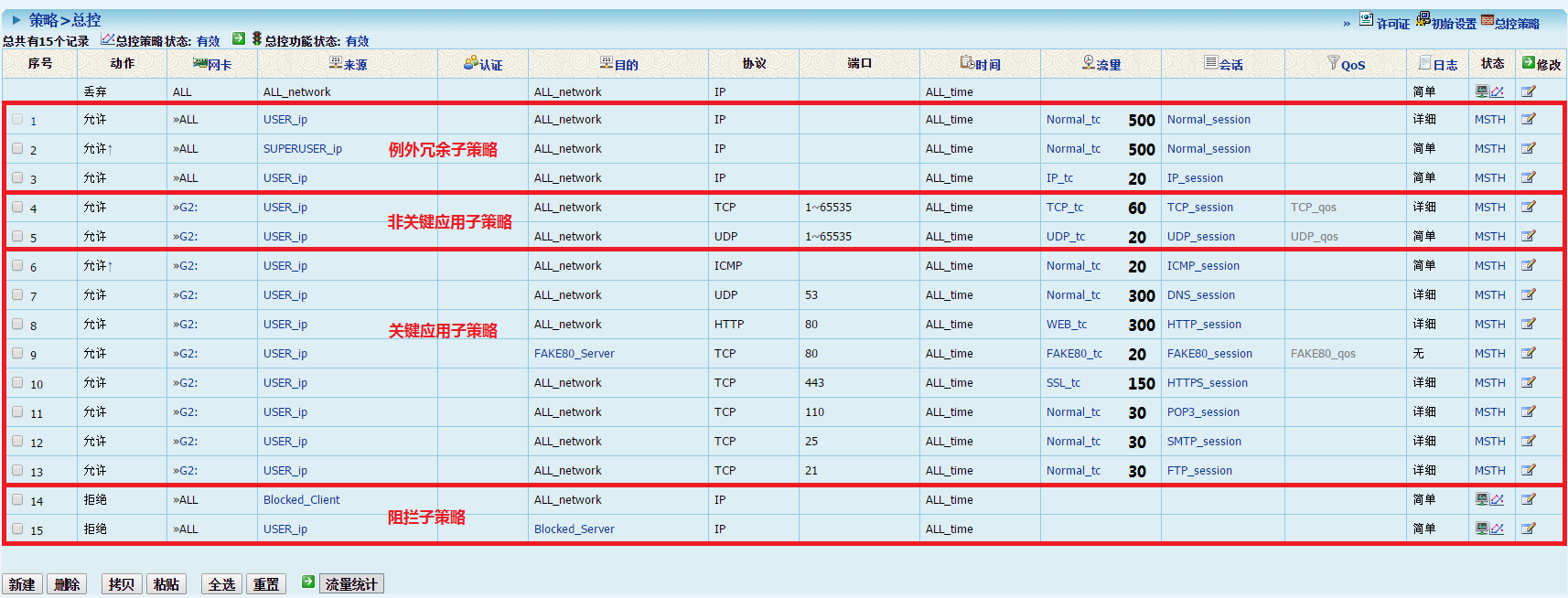


“网络审计”项为“***启用***”



再点击“确定”按钮，系统将自动生成nic网卡、firewall总控策略等十几种配置，可进一步查看并做修改。再将外网网线连接G1网卡，内网网线连接G2网卡，即可上线做转发及流控，管理员还可通过G2网卡在内网中继续管理设备。

### 1.2.2总控策略

在quickset “初始设置”界面中点击“规则数：xx”链接，或者点击左边主菜单的“防火墙>总控策略”菜单项，出现“总控策略”界面，如下图3所示为标准流控策略，可以以此基础新建适合本单位关键应用的总控策略。

**图3 “总控策略”界面**

#### 1.2.2.1 标准流控策略说明

流量控制功能主要由session_obj “会话”对象、traffic_obj “流量”对象和qos_obj “QoS”带宽对象构成，它们在quickset“初始设置”后的标准流控策略中的具体内容为：

**traffic_obj 流量对象**：只是记录持续和上传流量，没有阻拦动作。

**会话对象**：限制各源IP各应用的会话数，具体数值如图3中黑字所示。



qos_obj **QoS对象**：非关键应用的子策略中有，但需要启用QoS功能才能生效。

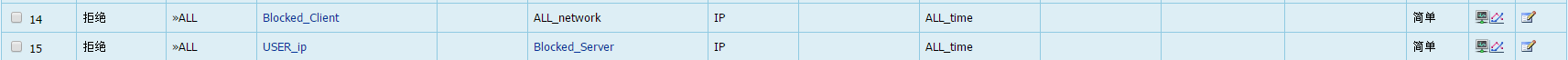
下面详细讲解图3中标准流控策略中的各个子策略的作用，由于firewall总控策略是按最后匹配的子策略优先执行的顺序，因此需要从下往上讲解。

**1）阻拦子策略**

* 第一行没有序号的策略为系统内置的缺省阻拦策略
* 序号15的子策略用于阻拦某些服务器IP
* 序号14的子策略用于阻拦某些来源IP

**策略说明：**如果没有任何总控策略，则除了8443、6443端口的管理流量，所有流量均被阻拦，因此一开始只需新建通过策略；当已有通过策略，又想再阻拦某些源IP或目的IP，则可以通过在最后的、序号14和15的子策略来实现。

**操作提示：**点击/右击ip_obj“来源”列“Blocked\_Client”或ip_obj “目的”列“Blocked\_Server” IP对象链接，再输入需要阻拦的IP并确定即可自定义需要阻拦的IP。



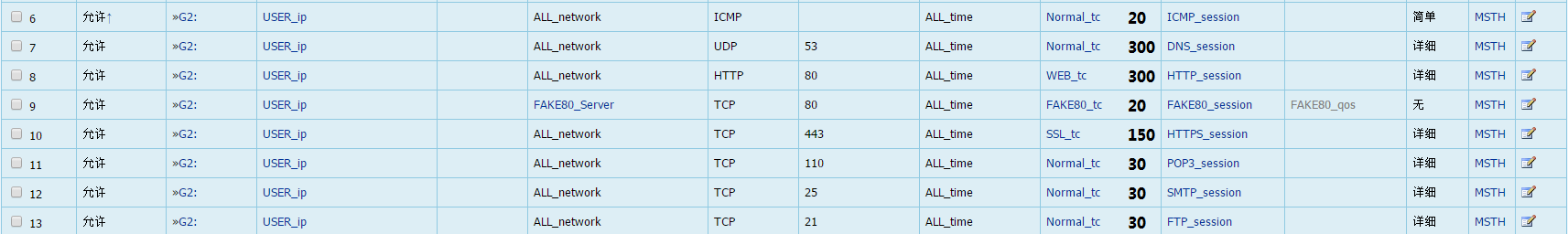
**图4 阻拦子策略**

**2）关键应用子策略**

* 序号13的子策略为FTP文件传输应用，单个源IP最大会话数为30。
* 序号12的子策略为SMTP发信应用，单个源IP最大会话数为30。
* 序号11的子策略为POP3收信应用，单个源IP最大会话数为30。
* 序号10的子策略为HTTPS加密浏览应用，单个源IP最大会话数为150。
* 序号8的子策略为WEB浏览应用，单个源IP最大会话数为300。
* 序号7的子策略为DNS域名查询应用，单个源IP最大会话数为300。
* 序号6的子策略为ping检测应用，单个源IP最大会话数为20。

**策略说明：**在此列出的关键应用是互联网的基础应用，用户可以修改或新建自己的关键应用。如果specapp_basic “特殊应用”项设置为通过，则该应用也是关键应用。

**操作提示：**点击/右击session_obj “会话”列“xx\_session”链接，再输入新值并确定即可自定义会话对象。



**图5 关键应用子策略**

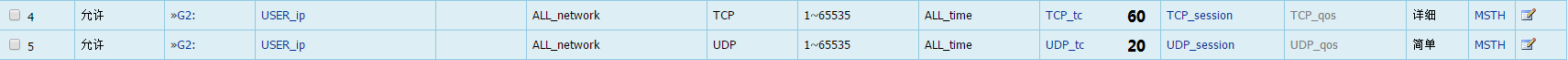
**3）非关键应用子策略**

* 序号9的子策略为伪80端口应用，单个源IP最大会话数为20。
* 序号5的子策略为其它UDP协议应用，单个源IP最大会话数为20。
* 序号4的子策略为其它TCP协议应用，单个源IP最大会话数为60。

**策略说明：**系统通过netaudit网络审计功能对WEB浏览应用的80等端口进行七层内容分析，将不符合HTTP协议的目的IP地址自动放到ip_objFAKE80\_ip IP对象中，这样可以在总控策略中对其进行流量控制。

**操作提示：**点击/右击session_obj “会话”列“xx\_session”链接，再输入新值并确定即可自定义会话对象。





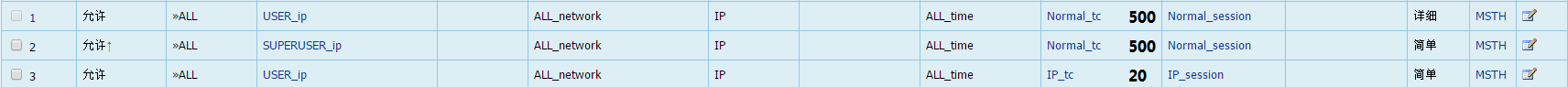
**图6 非关键应用子策略**

**4）例外冗余子策略**

* 序号3的子策略为其它IP协议应用，单个源IP最大会话数为20。
* 序号2的子策略为超级用户的应用，单个源IP最大会话数为500。
* 序号1的子策略为其它IP协议应用，单个源IP最大会话数为500。

**策略说明：**IP协议包括TCP、UDP、ICMP协议，系统将匹配后续的TCP、UDP、ICMP协议子策略执行，故序号1、3的子策略一般没有对应的流量。

**操作提示：**点击/右击ip_obj“来源”列“SUPERUSER\_ip” IP对象链接，再输入IP并确定即可自定义超级用户的IP，超级用户的流量将立即生效，而不会继续匹配下面的子策略。



**图7 例外冗余子策略**

#### 1.2.2.2 总控策略使用说明

1）总控策略匹配顺序由源IP、源端口、协议、目的IP、目的端口5元组及“规则匹配”选项决定，系统按从上到下的顺序进行匹配，在数据流的5元组与总控策略匹配的前提下，如果是“马上生效”，则按此策略实行，并会在列表界面的“动作”列中显示“允许↑”，如果是“继续检查”则即使当前策略匹配仍往下查找，并按最后一条匹配的总控策略实行。

2）总控策略内置的第一条策略是“拒绝所有”的策略，管理员一般只要在其后定义通过的关键应用的策略即可，即遵循“除非允许，否则拒绝”的原则。

3）“方向”一般选择“流入网卡”，此时的“网卡”是最靠近来源IP对象的网卡。

4）由于新建、修改总控策略会导致其序号发生变化，所以要在完成全部编辑操作后终止现有的会话。

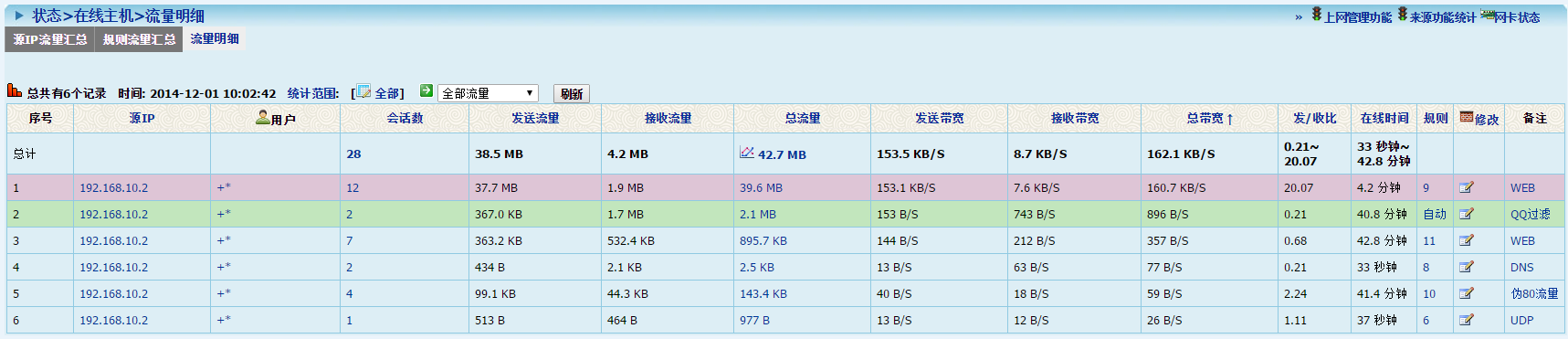
5）“日志”选项是“简单”则只记录通过数据流的第一个数据包，“详细”则记录全部数据包，这些记录的数据包可以在“实时监控”、“网络审计”、“IDP规则”功能中实时显示、记录、检查。

# 第二部分 异常流量控制

## 2.1流控目标及策略

对非关键应用的traffic_obj “流量对象”进行设置，当其“持续流量”和“上传流量”超出设定的阈值时，系统删除会话并封堵服务器IP一段时间，这样可以确保带宽不会被非关键应用的流量所占满。

可以通过点击右上角“状态”快捷链接，显示当前active_host在线主机的流量明细，其中绿色背景的为“持续流量”，红色背景的是“上传流量”。



**图8 “在线主机”界面**

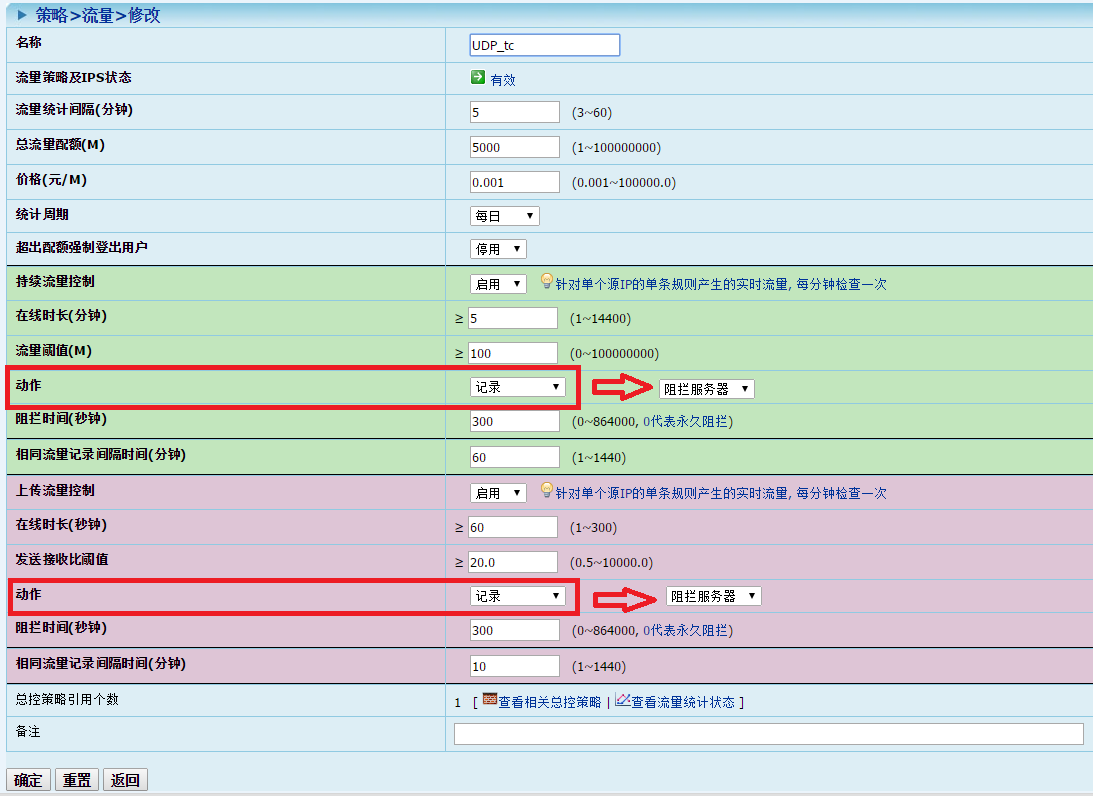
## 2.2 实施步骤

1）点击左边主菜单的“firewall防火墙>ip_obj对象设置>traffic_obj流量对象”菜单项，出现traffic_obj**“**流量对象**”**界面，如下图9所示。



**图9 “流量对象”列表界面**

2）点击**“**UDP\_tc**”**行修改按钮，或者直接在firewall **“**总控策略**”**的界面中，点击**“**UDP\_tc**”**链接，出现**“**UDP\_tc**”**流量对象的编辑界面，如下图10所示。



**图10 “流量对象”编辑界面**

**策略说明：**quickset**“**初始设置**”**后的标准流控策略中的**“**UDP\_tc**”**流量对象其“持续流量”和“上传流量”项的动作均为“记录”。系统每隔1分钟做一次流量统计，并根据对应的设置，对超出阈值的流量进行记录或阻拦。

**操作提示：**修改动作项为“阻拦服务器”，同时调整各阈值，即可对非关键应用中的UDP流量进行异常流量控制，之后再对**“**TCP\_tc**”**和**“**FAKE80\_tc**”**流量对象做类似的调整。被阻拦的IP可以在ips_status **“**IPS状态**”**中查看并手工删除。

# 第三部分 QoS带宽控制

## 3.1流控目标及策略

对非关键应用的qos_obj “QoS对象”进行设置，作用对象是firewall“总控策略”中ip_obj“来源”IP对象整体，通过限制其非关键应用的带宽，可以确保带宽不会被非关键应用的流量所占满。

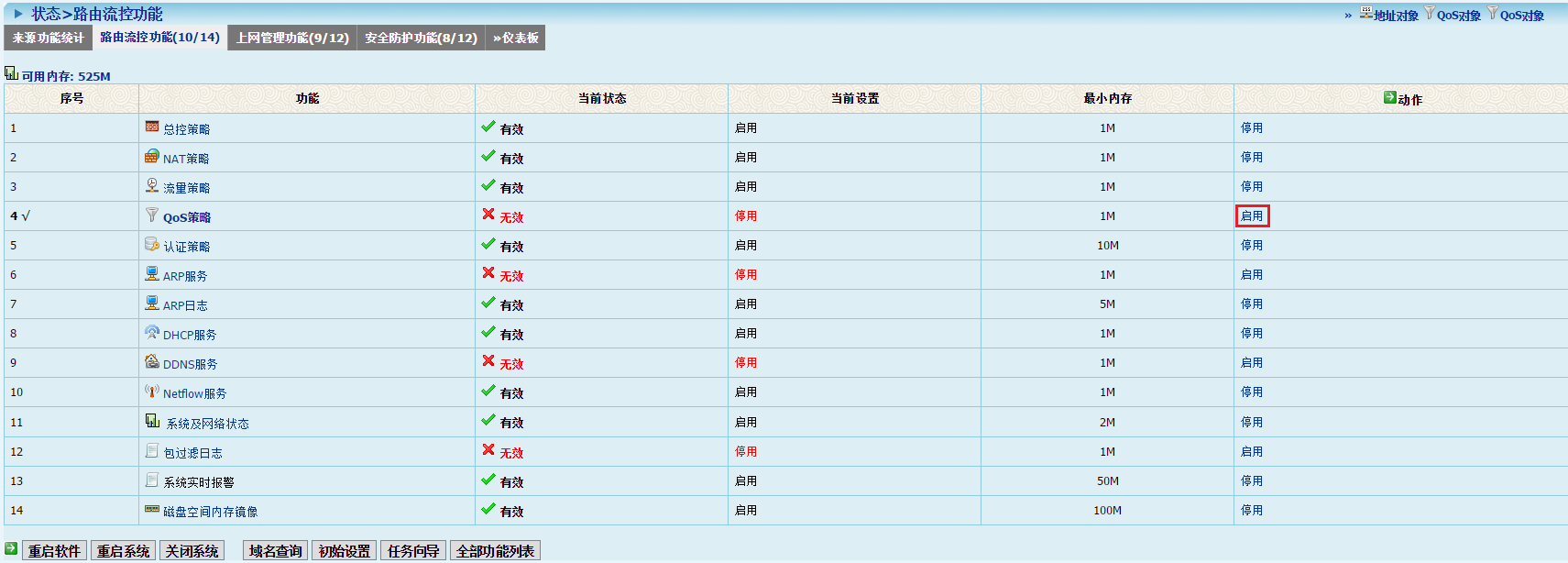
## 3.2 实施步骤

1）点击左边主菜单的“firewall防火墙>ip_obj对象设置>qos_objQoS对象”菜单项，出现qos_obj “QoS对象”界面，如下图11所示。



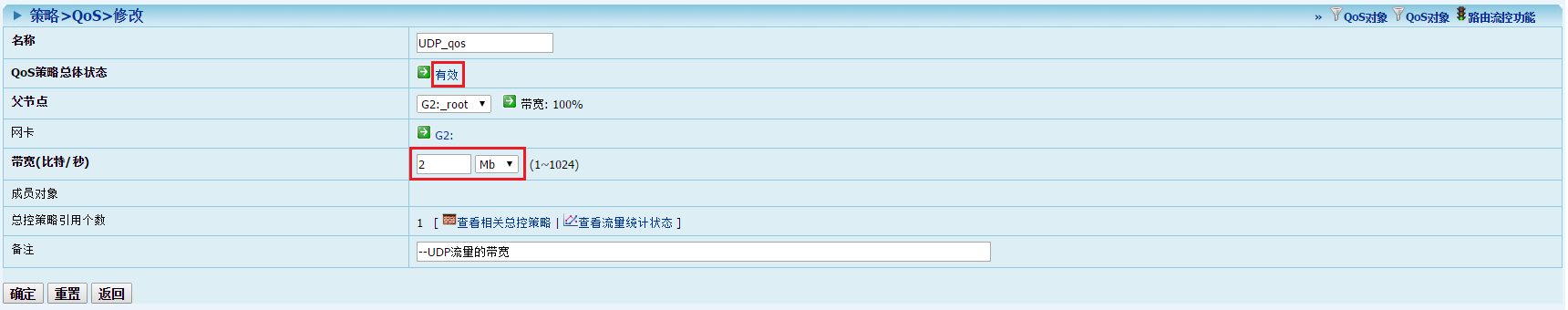
**图11 “QoS对象”列表界面**

2）系统缺省没有启用QoS功能，如果“QoS功能状态”为“无效”，则点击该链接，进入路由流控功能界面，如下图12所示，再点击qos_objQoS策略行最右边的“启用”链接，并确定，使其QoS功能生效。



**图12 “路由流控功能”界面**

3）返回qos_obj “QoS对象”界面，点击“UDP\_qos”行修改按钮，或者直接在firewall“总控策略”的界面中，点击“UDP\_qos”链接，出现“UDP\_qos”对象的编辑界面，如下图13所示。



**图13 “QoS对象”编辑界面**

**策略说明：**QoS对象的设置内容主要是带宽值，其作用的对象是引用其的firewall“总控策略”中ip_obj来源IP对象整体，当后者对应的流量的带宽超出设定值时，系统丢弃后续的封包以确保带宽不被突破。

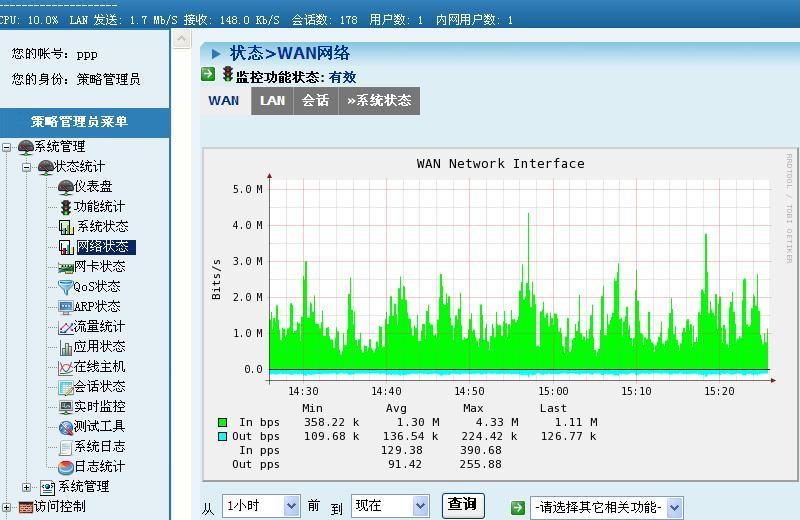
**操作提示：**修改“带宽”项的数值和计量单位，1Mb(its)=1/8MB(ytes)；再观察QoS状态及网络吞吐量暨带宽趋势图，并继续调整优化。

4）在QoS列表界面之下，点击“QoS状态”按钮，可以查看当前QoS策略实施的情况，如下图14所示，如果“丢弃封包”、 “丢弃字节”列有数值，则表明QoS对象在起限制作用。



**图14 “QoS状态”界面**

点击QoS状态界面之下“网络状态”按钮，可以查看各网卡的网络吞吐量暨带宽趋势图，如下图15所示，如果带宽由原来的被全部占满变成了有稍许余量的状态，则说明以上三种流量控制措施起到了作用。



**图15 “网络状态”界面**

**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. UTMWALL网关初始设置指南

http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_Quickset.doc

3. 企业流控全解析—与运营商流控的需求及技术对比

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