华御上网行为管理系统

操作使用说明书

北京华御科技有限公司

2017 年 6 月

目　录

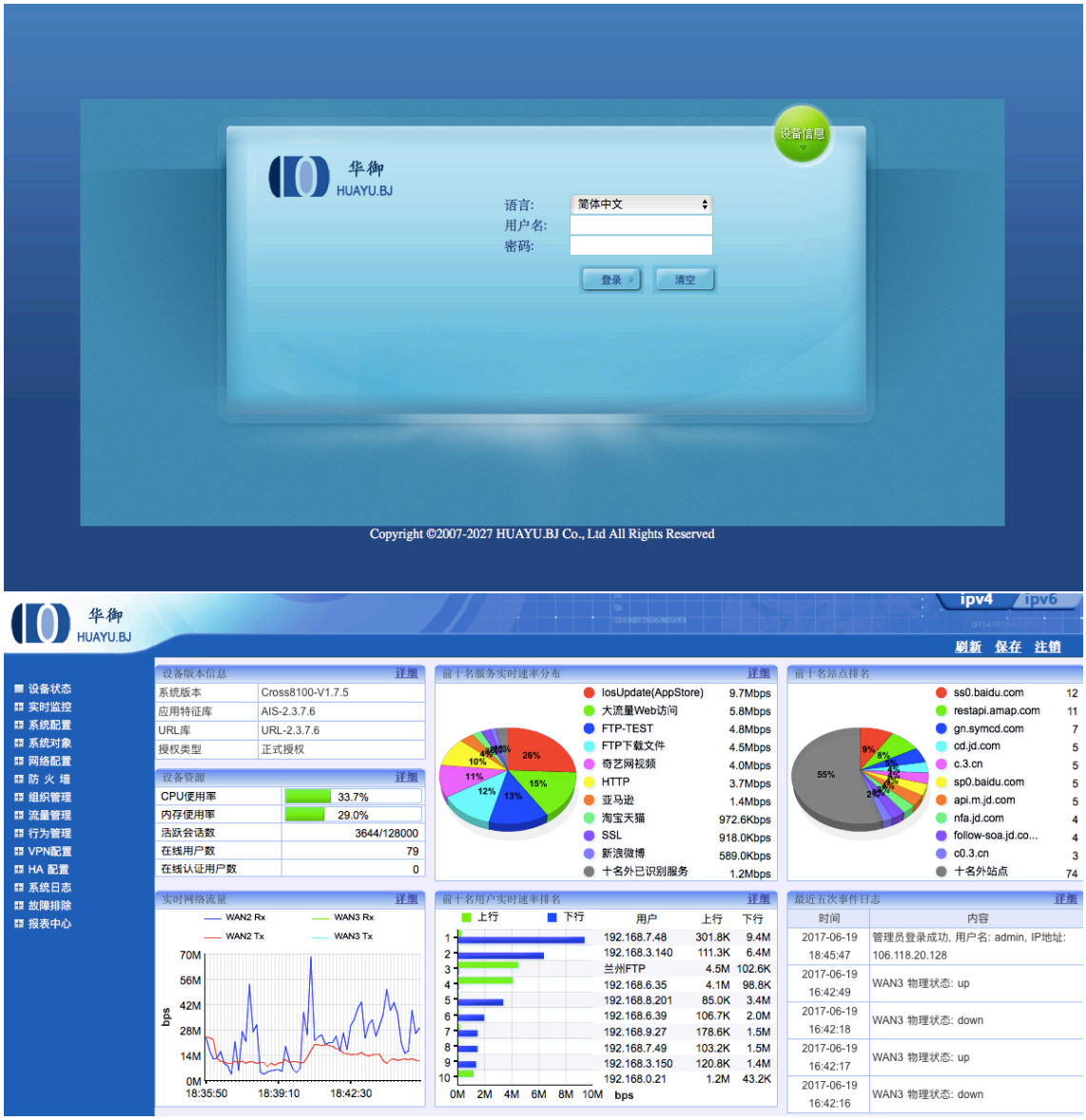
第1部分　系统初始化配置

1.1　设备登录

1、系统出厂默认是网桥模式 LAN1 和 WAN1 为网桥 1，地址为 192.168.0.1/24

2、通过网线将电脑的网口与设备的 LAN1 口相连接，电脑 IP 地址配置未：192.168.0.2/24

3、登录设备，打开浏览器输入 **https://192.168.0.1:9090**，默认用户名:admin 密码:bjhuayu,

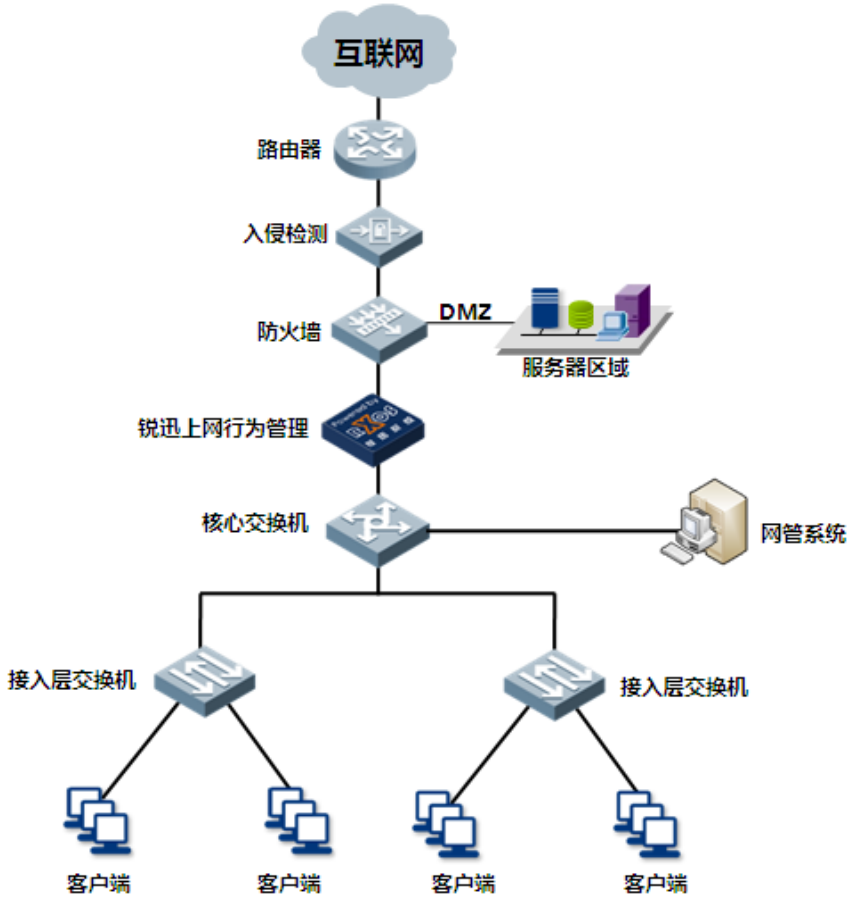


1.2 设备部署

设备支持网桥模式、路由模式、旁路模式三种部署模式。

1.2.1 网桥模式部署

设备不需要进行 NAT 网络地址转换时，通常采用网桥模式部署，网桥模式无需改变现有网络拓扑接口，“设备”视为一条带过滤功能的网线使用，把“设备”接在原有网关及内网用户之间，通常部署在配置 NAT 设备的下方。如下图所示：



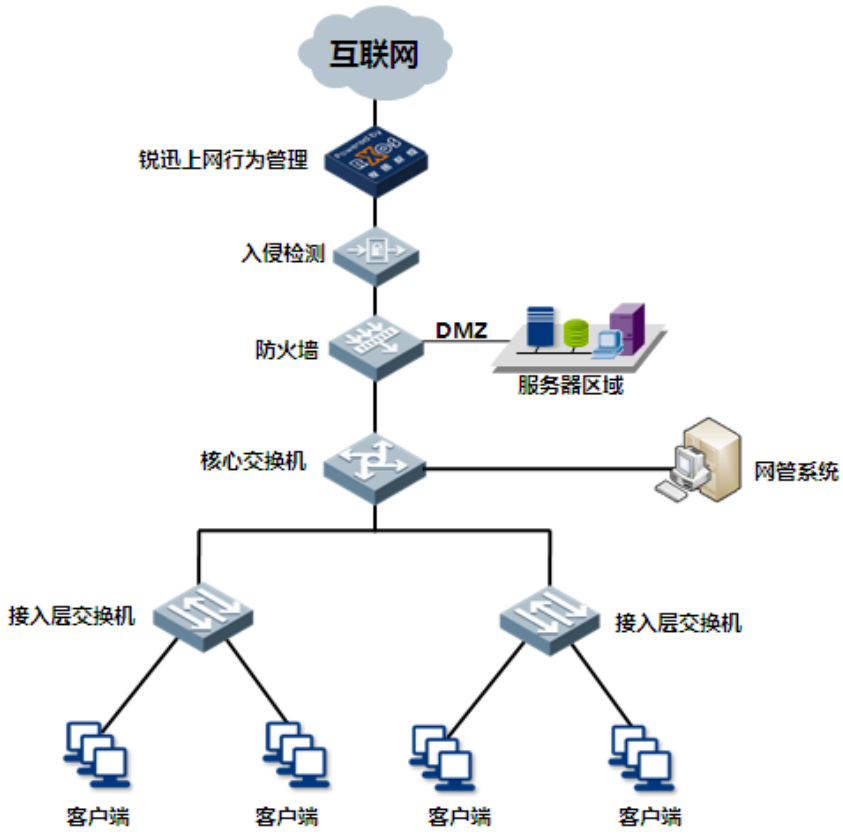
1、设备处于网桥模式时，所有数据流经过设备的流量将透明转发，设备可进行上网策略配置及审计，默认无任何策略，用户可以正常上网，所有经过的流量将进行审计。

2、配置网桥 IP 和网关，主要用于管理 Cross 设备，WEB 认证用、自动升级特征库和 URL 库等，

可在”系统配置-工作模式“中配置，如下图所示：

1.2.2 路由模式部署

Cross 设备具备防火墙的功能，可以直接作为 Internet 出口网关，进行 NAT 地址、端口映射等。此时需要将设备配置为路由模式部署，LAN1 口连接下行交换机，WAN1 口连接运营商提供的线缆，可以是光口或电口，如下图所示：

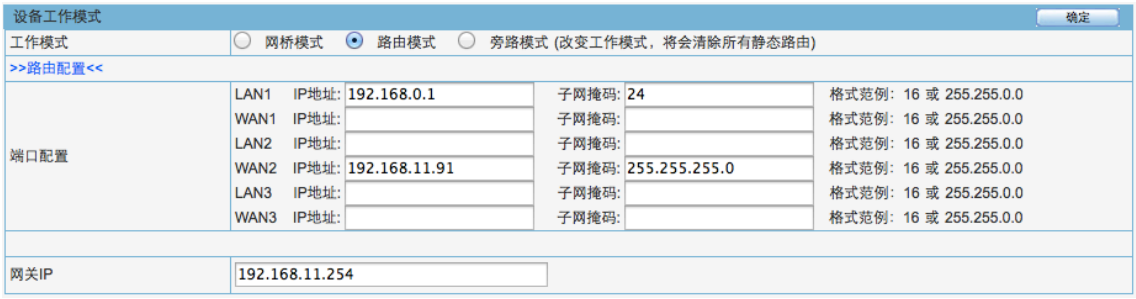


在路由模式下，需要根据实际的上网方式进行不同的配置，通常互联网接入包括：拨号上网、分配固定地址上网两种方式，下面分别介绍如何进行两种上网方式的配置

1.2.2.1 拨号上网配置

当采用拨号上网时，可通过如下方法进行配置：

1、首先在”系统配置-工作模式”页面,配置好 LAN 接口的 IP 地址，然后点击确定，如下图所示：



2、在“网络配置-接口配置-PPPOE”页面,选择外网接口(对应 Cross 设备的 WAN1 或者其他 WAN 口)，配置好拨号账号和密码，点击确定。

3、在“网络配置-路由配置-静态路由”页面,新增一条默认路由,下一跳指向 pppoe 接口。

如果内网是跨三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,可跳过第(4)步骤。

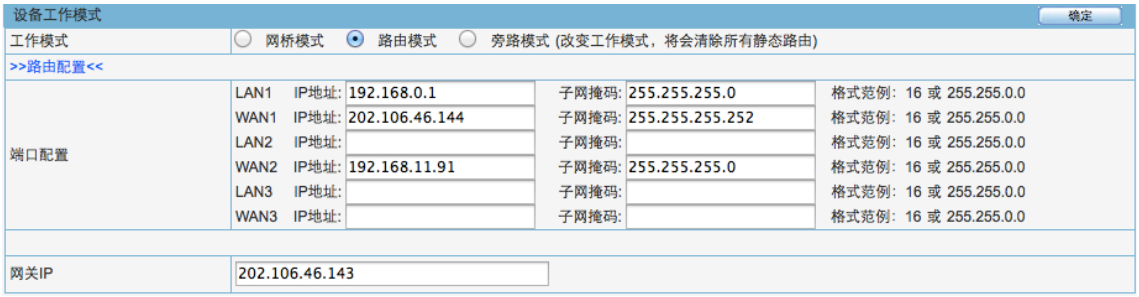
4、在“网络配置-路由配置-静态路由”页面,新增回程路由,目的 IP，输入内网中的网段，下一跳指向三层交换机上联 Cross 设备接口（LAN1 口）的地址。

5、在“防火墙-NAT 规则-内网代理”新增规则，流量方向必须选 LAN 口-PPPOE 拨号的接口，如刚创建的 PPPOE 接口名称为 adsl，其他默认。

1.2.2.2 固定地址上网配置

1、首先在”系统配置-工作模式”页面，配置好 LAN 和 WAN(运营商提供的固定 IP)接口的 IP 地

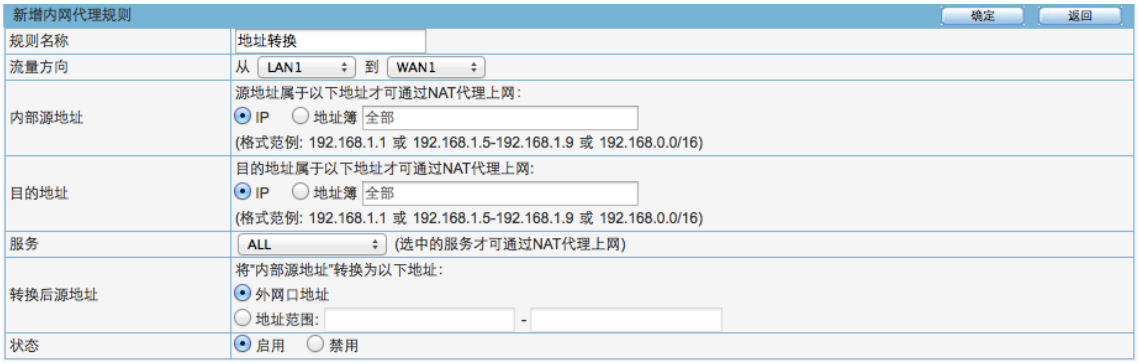
址,网关 IP 地址,如下图,点击确定



如果内网是跨三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,那么第(2)步骤可以跳过。

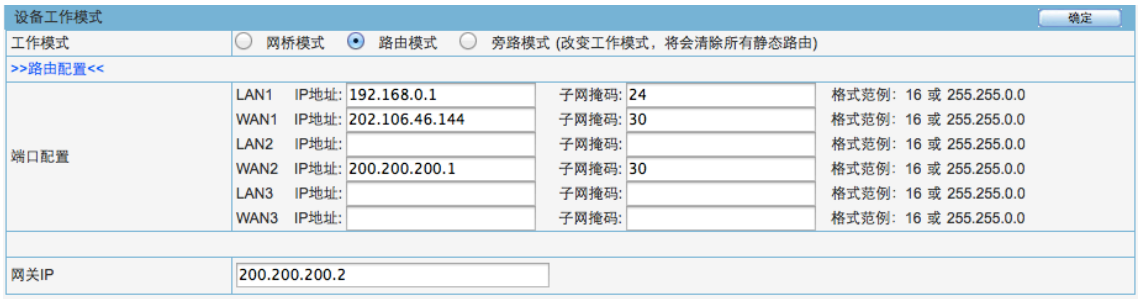
2、在“网络配置-路由配置-静态路由”页面,新增回程路由,目的 IP，输入内网中的网段，下一跳指向三层交换机上联 Cross 设备接口（LAN1 口）的地址。

3、在“防火墙-NAT 规则-内网代理”新增一条规则,流量方向必须选 LAN1 口-WAN1 的接口,有多个公网 IP，转换后源地址选地址范围。



1.2.3 多互联网出口负载均衡配置

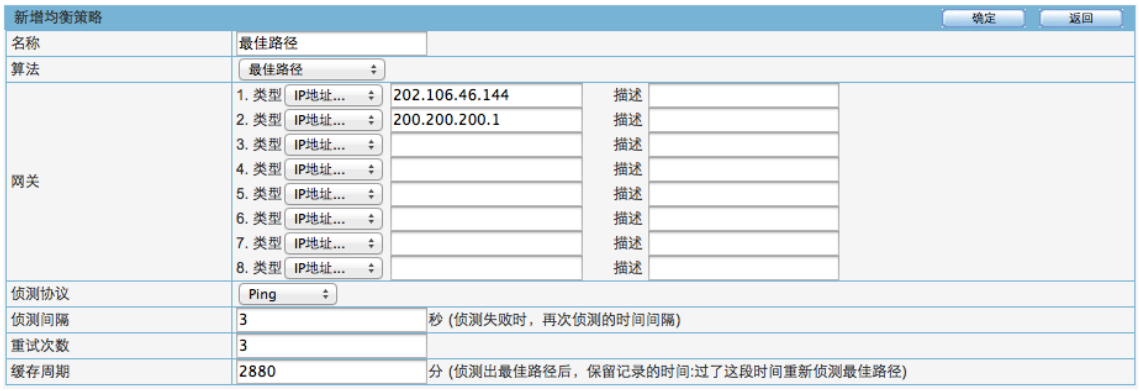
1、首先在”系统配置-工作模式”页面，配置好 LAN1、WAN1 和 WAN2 接口的 IP 地址,网关 IP 地址,如下图

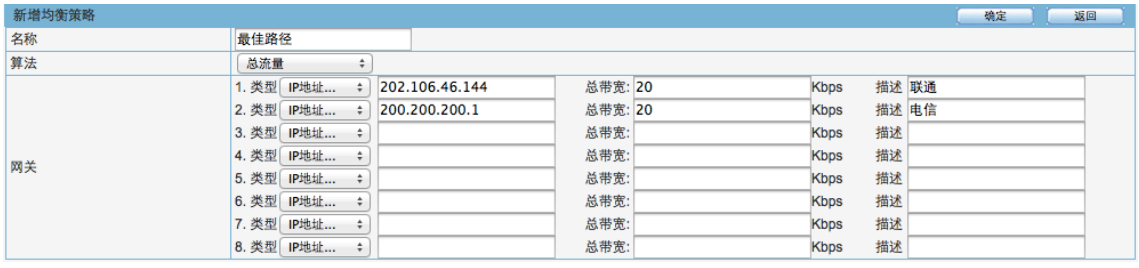


如果内网是三层交换机,有多个内网网段的情况下,还需要配置回程路由,如果内网无三层交换机,那么第(2)步骤可以跳过。

2、在“网络配置-路由配置-静态路由”页面,新增回程路由,下一跳指向三层交换机上联接口的地址。

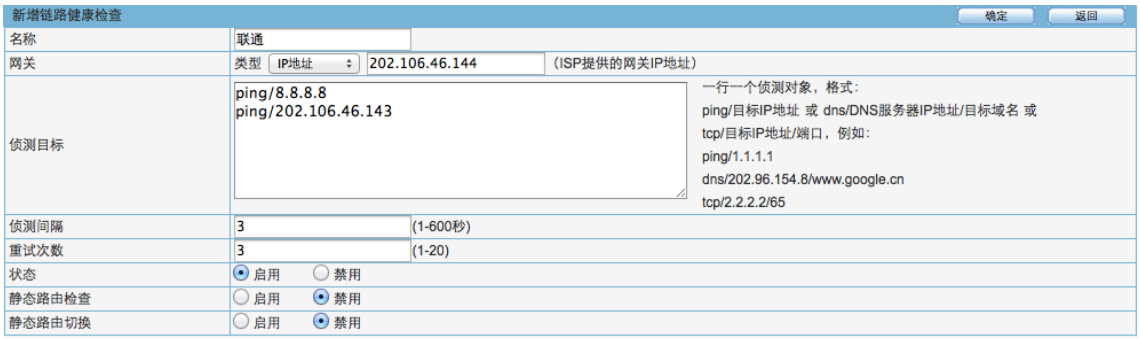
3、在“网络配置-路由配置-均衡策略”页面，新增策略，如果是 1 条电信，1 条网通的线路，建议选择最佳路径算法，如果 2 条都是电信，建议选择总流量算法。





4、如果 2 条链路,1 条失效立马切换到另 1 条线路,必须配置链路健康检查,在“网络配置-路由配

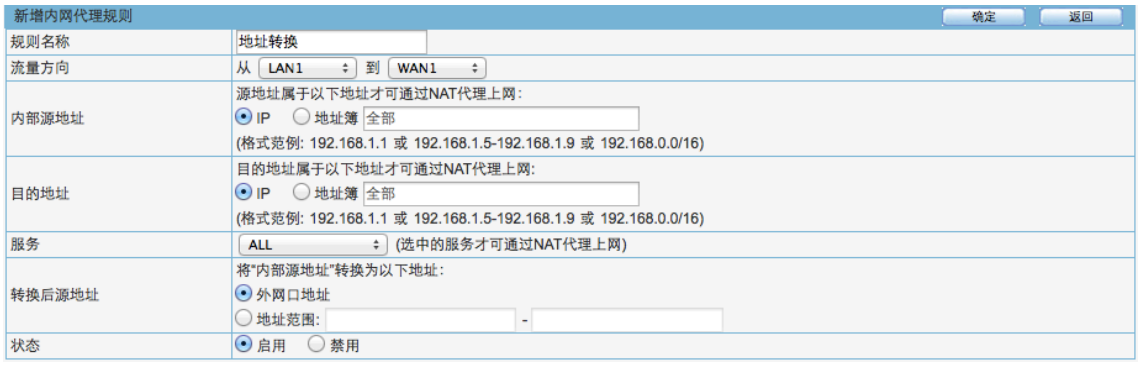
置-链路健康检查”页面,新增策略,建好 2 条线路的侦测。



5、在“网络配置-路由配置-策略路由”页面,新增策略,引用刚创建的均衡策略。

注:均衡策略算法根据实际环境配置,如果 2 条都是电信线路,可以选择总流量或者下行流量进行负载,如果 1 条电信、 1 条网通都是相同带宽,可以选择最佳路径,也可以实现一部分用户走 1 条线路,另一些用户走第 2 条线路,根据实际需要进行配置。

6、在“防火墙-NAT 规则-内网代理”新增二条规则,流量方向必须选 LAN1 口-WAN1、LAN1-WAN2,有多个公网 IP,转换后源地址选地址范围。



第2部分 用户管理

Cross 设备的用户管理，可以采用默认的 IP 地址管理，也可在设备中建立实际的、清晰的组织架构,方便管理人员管理，根据不同的部门或者用户下发不同的流控策略、上网行为策略。

2.1 组织结构

选择组织管理->组织结构,如下图所示：

2.1.1 新增子组(部门)

此部分说明，如何建立用户的分组，也可理解为部门，点击新增子组按钮,增加部门,如图:

配置说明:

1、组名:新建的部门名称,如财务部等,如果需要建立多个部门,需要一行一个组名称(部门名称)

2、所属组:新建的组增加到哪个部门下面,如 root 组。

3、上网策略，此处时针对组设定上网行为的策略，可以继承父组的策略，也可选择“使用自己的配置”指定上网策略，此处需要提前在“策略管理” - “行为策略” - “上网策略对象”中提前配置好。

4、黑名单控制:新建组用户所执行的黑名单策略名称,如果选择”继承父组配置”,将执行上级组(所属组)的黑名单策略,如 root 组;如果选择使用自己的配置,将执行所选择的黑名单策略。

5、准入规则:主要用在当用户需要监控及时通讯(QQ)记录需求时,需要用户安装插件的情况；当选择”继承父组配置”时，继承上级组准入规则；如果当前组不需要继承上级组的准入规则,请选择“使用自己的配置”。

6、离线用户自动删除:当离线用户超过设定的时间后,自动删除该用户。

2.1.2 新增普通用户

下面说明如何在组织结构中建立用户，通过用户的建立可以将每个用户进行区分，加以标示，使得管理人员能够直观在设备中看到上网人员。用户分为普通用户与认证用户，认证用户需要通过认证后方可上网，本节说明如何新增普通用户，具体操作为：点击“组织管理”->“组织结构”->“新增用户”,如下图所示:

1、用户名:上网行为设备内唯一合法的标识名称

2、显示名:主要用于报表统计时直观看到的名称

3、描述:对该用户的简单说明

4、所属组:该用户属于哪一个部门

5、用户类型:普通用户:在符合相关条件下,不需要输入用户名和密码可以直接上网；认证用户:在符合相关条件下,需要输入用户名和密码才可以上网。

6、绑定检查:检查该用户名的绑定条件;绑定 ip:该用户名绑定指定的 ip 地址后才可以上网,如需要绑定多个 ip 地址,需要一行一个 ip 地址,如 192.168.0.131；绑定 MAC 地址:该用户名绑定指定的 MAC 地址后才可以上网,如需要绑定多个 MAC 地址,需要一行一个 MAC 地址,如 00:24:8C:51:24:23;同时绑定 MAC 和 ip:该用 户名绑定指定的 MAC 地址和 ip 后才可以上网,如需要绑定多个 MAC 和 ip 地址,需 要一行一个 MAC 和 ip 地址,如 192.168.0.131(00:24:8C:51:24:23);绑定 VLAN: 该用户名绑定指定的 VLANID 后才可以上网,如需要绑定多个 VLANID,需要一行 一个 VLANID 地址,如 123

7、上网策略:新建用户所执行的上网策略名称,如果选择”继承父组配置”,将执行上级组(所属组)

的上网策略,如 root 组;如果选择使用自己的配置,将执行所 选择的上网策略对象。

8、准入规则:主要用在当用户需要监控及时通讯(QQ)记录需求时,需要用户安装插件的情况;当选择"继承父组配置"时,继承上级组准入规则;如果当前组不需要 继承上级组的准入规则,请选择"使用自己的配置"。

9、用户状态：该用户的使用情况；"正常"：该用户能够正常使用；"冻结"：该用户处于冻结状态。

2.1.3 新增认证用户

认证用户在符合特定条件下还需要用户名和密码才能够正常上网,其他操作和新增普通用户一样,在"用户类型"那里选择"认证用户",如图:

说明:

1、认证方式:选择认证服务器;"本地认证"：上网行为流控设备本身作为认证服务器,当认证用

户输入的用户名和密码与设备数据库里面的用户名和密码匹配时通过认证；“到外部服务器认证”：选择用户的 AD 域服务器、POP3 服务器、RADIUS 服务器、LADP 服务器等,具体配置请参考“上网行为”->“认证策略”配置。

2、公用帐户:设定该帐户允许多少个用户同时使用。

3、有效期:设定该帐户的使用期限。

2.1.4 组织架构导出

在配置好用户后，可以通过组织架构导出来备份组织结构，便于管理人员后期管理。选择“组织管理”->“组织架构”->“导出按钮”,选择需要导出的用户或者用户组,如图:

选择“导出”按钮,选择文件保存位置即可。

2.1.5 移动用户或组

当需要调整用户或者组的隶属关系，可以通过移动用户或组的功能进行调整，点击“组织管理”->“组织结构”,选择需要移动的用户或者组,点击“移动”按钮，在“目的组”处选择需要移动的最终隶属组,点击“选择”按钮,如下图所示:

2.1.6 批量导入

如果用户较多，可以通过批量导入的方式进行导入，避免管理员逐个建立用户的麻烦。点击“组织管理”->“批量导入”,如下图所示:

第3部分 认证配置

这部分主要说明如何进行：认证策略配置、用户上网行为策略、配置认证服务器及参数、设置黑白名单及管理等操作。

3.1 认证策略

认证策略包括几种不同的类型，首先需要定义认证的条件、认证方式及认证服务器等操作，如下图所示：

配置说明:

1、名称：认证策略的名称可以根据实际情况命名,如财务部认证策略、访客认证策略等。

2、IP 地址：匹配认证条件的内网地址。可以是指定的 ip 地址、也可以是一段 ip 或通过地址簿来选择。

3、认证方式:判断新增加用户以哪种方式来作为用户名称,有五种方式:

1）“新用户以 IP 地址作为用户名”:新增加的用户名为 IP 地址名称。内网用户不需要密码认证,并且当该用户不在组织结构中时,自动以用户的 IP 地址为用户名。

2）“新用户以 MAC 地址作为用户名”:新增加的用户名为 MAC 地址名称。内网用户不 需

要密码认证,并且当该用户不在组织结构中时,自动以用户的 MAC 地址为用户名。

3）“新用户以主机名作为用户名”:新增加的用户名为用户主机名称。内网用户不需要密码认证,并且当该用户不在组织结构中时,自动以用户的主机名称为用户名。

4）“新用户以 VLANID 作为用户名”:新增加的用户名用户 VLANID 名称。内网用户不需要密码认证,并且当该用户不在组织结构中时,自动以用户的 VLANID 为用户名。

5）“到服务器去认证”:新增加的用户需要到指定的服务器做认证。只有用户输入和指定服务器相匹配的用户名和密码只有,才能通过认证。

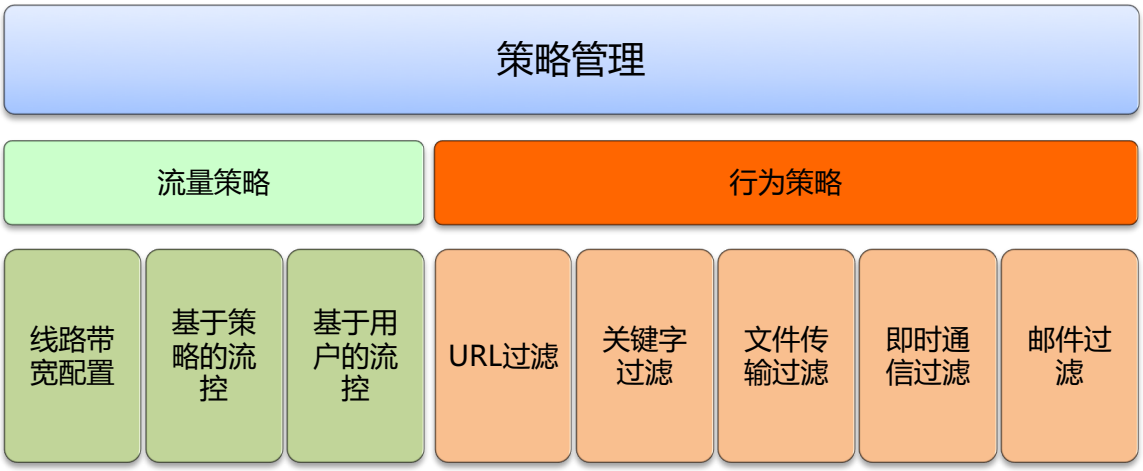
4、自动添加到组织结构:认证成功后的用户自动添加到指定的组中,点击“选择”按 钮,为新增加的用户选择所属组;根据不同的认证方式,所选择的自动绑定条件也不近相同。

5、状态:启用或禁用本策略,默认启用

第4部分 上网策略配置

策略管理通常包括以下两部分内容：

- 流量策略：基于协议、每用户带宽、会话数进行控制
- 行为策略：基于关键字、文件后缀、URL 等进行控制



4.1 流量策略

流量管理可以用于：

1、精确识别各种互联网应用，包括各种对带宽占用较大的主流 P2P 软件与在线视频软件；

2、基于应用或用户对流量进行管理，对指定类型的流量进行限速，避免占用过多网络带宽；

3、对关键业务提供带宽资源保障，保留足够可用带宽，保障服务质量；

4.1.1 线路带宽配置

用于配置互联网出口带宽，根据运营商实际给定的带宽值填写，此处配置好之后，在设定策略的时候可以通过百分比来分配带宽。

线路带宽配置 确定

名称	上行带宽(Kbps)	下行带宽(Kbps)
WAN1	1000000	1000000
WAN2	1000000	1000000
WAN3	1000000	1000000

根据线路的带宽值来配置

4.1.2 基于策略的流控

用于全局的基于用户与对应七层应用的流控策略控制，配置完立即生效，策略规则匹配原则是按顺序从前往后匹配，从上往下顺序匹配，遇到第一匹配的条目就停止，所以同一组策略中，序号小的优先执行，可以通过插入、移动来调整顺序，此处如果使用 URL 阻断策略时，需要防止到最下方。

策略流控规则 新增通道 修改状态 删除所有 计数清零

规则名称	内网地址	外网地址	服务/URL/文件类型	带宽(Kbps)	生效时间	生效线路	匹配计数	状态	操作
阻断P2P	全部	全部	HTTP应用 :3种 WEB视频 :全部 P2P下载 :全部 流媒体 :全部 网络游戏 :全部 其他服务 :2种	阻断流量	全天	WAN1	311416	☑	新增 修改 插入 移动 删除
VIP通道	特殊用户	全部	所有	最大: ↑1500, ↓1500	工作时间	WAN1	212016	☑	新增子通道 修改 插入 移动 删除
访问北京服务器	全部	北京服务...	所有	最大: ↑4096, ↓4096 保障: ↑3072, ↓3072	全天	WAN1	21863	☑	新增子通道 修改 插入 移动 删除
特殊协议保障	全部	全部	常用服务 :5种 网上银行 :全部	最大: ↑4096, ↓4096 保障: ↑2048, ↓2048	全天	WAN1	2131881	☑	新增子通道 修改 插入 移动 删除
URL阻断	全部	全部	内置URL库 :4种	阻断流量	全天	WAN1	344	☑	新增 修改 插入 移动 删除

提示: 不同线路的通道策略互相独立，没有优先顺序。同一线路的同级通道策略，按从前往后的顺序匹配，可通过<插入>或<移动>来改变策略的先后顺序。匹配到父通道策略之后，再进一步匹配子通道策略。

配置说明

生效线路：流控规则的生效线路

内网地址：可输入IP地址、选择地址簿或用户组。地址簿需要在【系统对象>地址簿】中预先配置好，用户组在【组织管理>组织结构】中预先配置后在此处可选择。

外网地址：可输入目的IP地址、选择地址簿或用户组，通常无需配置；

服务 / URL / 文件类型：可以选择七层应用或应用组、URL分类或自定义URL、文件类型；

流控行为：包括“阻断流量”、“限制通道”、“保障通道”，其中详细配置选项包括，

优先级：保障带宽时，优先级较高的报文优先传送。可将核心业务应用、重要人物的流量配置为高优先级；同时将P2P、网络电视、WEB视频等非核心的、占用带宽资源较多的应用配置为低优先级。

最大带宽：为某些用户或特定应用指定最大带宽，百分比为占用本线路带宽值的比例。

保障带宽 :结合最大带宽和优先级 ,根据需要为某些关键应用或者 VIP 客户保障一定带宽。

当网络繁忙时，这些关键应用或者 VIP 客户至少可以得到设定的保障带宽，并还可以租借空闲的或低优先级流量的带宽；当网络空闲时，低优先级的流量亦可使用当前空闲带宽。从而保证了带宽的合理、高效的使用。百分比为占用本线路带宽值的比例。

预留带宽：为某种特定应用或某些重点客户预留一定带宽，以保证在不同时间段、不同的网络使用环境中某种流量都能得到同样的带宽。预留带宽不能被其他数据流使用，百分比为占用本线路带宽值的比例。

生效时间：本规则的有效时间段，细化至分钟，可在“时间计划”中预先定义好。

4.1.3 基于用户的流控

网络中 80%的带宽被 20%的人占用，为了防止这一情况出现，体现网络公平，可以对全网中每个主机进行带宽、会话控制、分类服务进行限制以及分时段管理。策略规则匹配的原则是从上往下匹配，如下图所示：

4.1.4 配置策略常见注意事项

1、如果需要阻断 URL ,建议在行为管理策略中配置 ,流控对 URL 阻断会现实无法访问此网站；

2、如果在基于策略的流控中选择对 URL 阻断或者流控，那么所有服务（如 P2P、Web 视频）都会匹配这一条 ,而且默认的服务是允许的 ,因此阻断服务如 Web 视频或者 P2P 下载的服务，必须配置在 URL 流控的上方才可生效；

3、有阻断的策略，建议开启阻断记录，方便排查问题；

4、配置完成后，发现策略无效果，查看匹配计数，无匹配计数请检查生效线路，IP、服务、URL 以及生效时间有无配置错误，策略是否启用。如果是某一项应用没有祈祷控制效果，请把该应用的名称、版本号上报，方便及时对该应用进行更新。

5、应用服务中对某些 P2P 下载的阻断和流控需要选择多种服务才能起作用 ,比如迅雷等下载，迅雷有自己的私有协议还有加密协议，对此种协议的阻断需要阻断如下集中应用：P2P 下载中的迅雷、BT、HTTP 应用的多线程下载和伪 IE 下载阻断，这样能阻断和控制大部分迅雷和 BT，但是有一些极端环境中，迅雷还是会走我们没有识别到的部分加密协议，那么需要把“其他服务 - 其他 TCP 协议”也阻断掉，这个阻断可能会引发一些没有识别到重要的 TCP 应用也无法访问，阻断视情况而定。如果基于策略流控和基于用户流控都对某个 IP 的带宽限制，那么带宽限制小的生效；

6、对于限制单个用户的会话数也非常有必要，用户中毒、木马或者使用扫描工具会产生大量的上行会话，P2P 下载也会产生大量上下行会话，特别在教育行业，会话必须进行限制，建议值为 400-500，值太小会导致正常应用访问不了，太大达不到应有的效果，对于服务器不能限制会话数。

4.1.5 配置流控策略的步骤

1、清楚网络出口实际带宽大小；

2、设备上架后先分析用户网络流量的状况，在“设备状态页面”查看实时网络流量大小，前 10 名服务和前 10 名用户流量；

3、观察一段时间流量后，开始配置策略流控，配置的步骤为：

1）先配置好实际的线路带宽大小；

2）针对重要 IP、重要服务和服务器做保障带宽，保障的带宽值视带宽；

3）针对 P2P 下载、WEB 视频以及流媒体做带宽限制或阻断；

4）对“其他服务 - 其他 UDP”做一定的带宽限制（但不能过小，可能会影响部分游戏）

5）最后配置一条默认策略，IP 和服务都是全部，带宽限制为总带宽的 80% - 100%（必须，要想保障带宽起到很好的作用，必须最后配置这条）

6)对于某些用户占用带宽资源比较大时 ,在基于用户流控对每个用户限制一个带宽值(1-2M)，除非带宽很充裕可以适当调整，对于服务器的 IP 通常不做限制。

提示：所有策略保障带宽的和加起来不能大于总的线路带宽。

4.2 行为策略设置

在配置好用户之后，可以针对用户进行上网行为策略的配置，包括 URL 过滤、关键字过滤、文件传输过滤、即时通讯过滤、邮件过滤。

重要提示：上网策略设置必须先设置“认证策略”，然后在“组织结构”对应组中，选择组应的上网策略。

4.2.1 URL 过滤

该功能主要用于 URL 的禁止和允许的配置 ,点击“行为管理”->“上网策略对象”,点击“新增”按钮,如图:

配置说明:

1、名称:配置上网策略对象名称,方便管理员标示。

2、描述:对该策略的简要概述

3、URL 过滤:内置 URL 库->内置 URL 库共分为 40 多个类型,1500 多万条 URL 记录,选择相应的类，在“动作”选择“拒绝”或者“允许”,生效时间选择“全天”或者自定义时间任务计划。自定义 URL 库->系统向用户开放自定义 URL 接口,用户可根据自己实际需求自定义 URL 内容。

4.2.2 关键字过滤

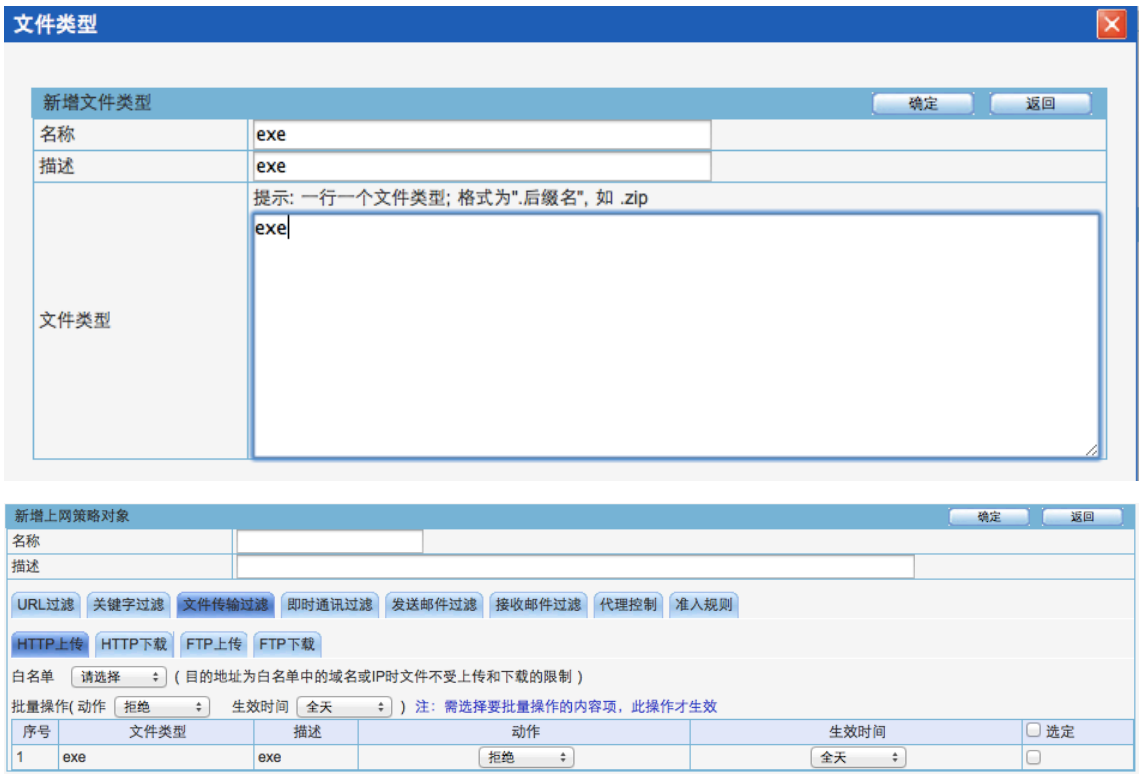
关键字过滤用于对论坛中的发帖内容、搜索引擎中搜索的关键字进行过滤，即阻止某些关键字，如下图所示：

选择“关键字过滤>搜索引擎”,配置“生效时间”,勾选需要过滤的关键字条目的“阻断”复选框，“未勾选”的条目表示不过滤。

4.2.3 文件传输过滤

文件传输过滤用于过滤 HTTP/FTP 指定文件类型的文件上传和下载，首先建立文件类型，然后

在文件传输过滤中选择，如下图所示：



勾选后，如动作选择“拒绝”，那么指定类型的文件无法通过 HTTP / FTP 进行上传和下载。

4.2.4 即使通讯过滤

用于过滤即时通讯工具如 QQ、MSN 等工具的登录、聊天内容、文件传输等，其中 QQ 内容记录需要安装插件，如下图所示：

如果过滤内容选择“登录”，相应的即时通讯工具将无法登录；如果勾选“文字聊天”，相应即时通讯将无法聊天；“语音聊天”和“文件传输”功能类似；QQ 只能过滤“登录”。

4.2.5 邮件过滤

用于对网内用户使用邮件客户端、Web 邮件收发邮件进行过滤，能够对邮件地址、邮件主题、邮件内容及附件进行检查，对符合邮件过滤条件的邮件进行过滤，如下图所示

注：上网策略对象制作好之后是无法生效的，需要在“组织结构”中应用，点击需要引用的部门或用户，在“上网策略”中选择“使用自己的配置”选择相应的策略即可，如果是部门，可以通过勾选“强制继承”，让该部门所有用户都继承所选的上网策略，如下图所示：

4.2.6 白名单管理

白名单包括：用户白名单、URL 白名单、即时通讯白名单、网页上传白名单

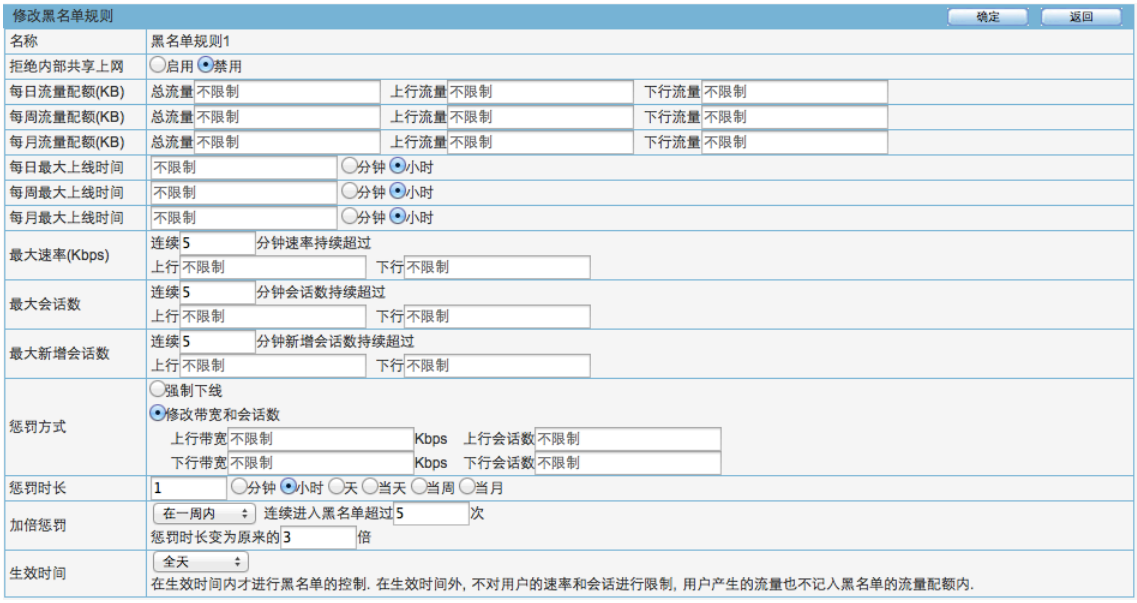
用户白名单：IP 白名单策略包含的流量全部放行，不受任何策略的控制，也不被审计。

URL 白名单：URL 白名单包含的流量全部放行，不受任何策略的控制，也不被审计。

即时通讯白名单：只有在‘即时通讯白名单’策略里的账号才能登录和使用，但其通讯记录是否被审计由【报表中心>内容记录配置】页面的配置来决定。

4.2.7 黑名单管理

通过黑名单可以提前定义好规则，当用户的上网行为符合相应的规则后，将自动加入黑名单，予以控制，规则包括流量、带宽、会话等。



黑名单规则设置后默认不生效，需要在组织结构中引用，操作方法为：

点击“组织管理”-“组织结构”，点击需要引用的部门或用户，在黑名单控制中选择“使用自己的配置”，选择相应的策略即可，如果是部门，还可以勾选“强制继承”，让该部门所有用户都继承选择的黑名单规则，如下图所示：

4.3 跨三层交换机绑定 MAC 地址实施

设备部署到三层交换机的上方后，数据经过三层交换机后，终端的 MAC 地址都将变成交换机的 MAC 地址，这样将无法还原真是的 MAC 地址，绑定 MAC 地址将失效，通过下面方法配置将实现跨三层绑定 MAC 地址。

1、开启三层交换机的 SNMP 协议，获取三层交换机的 community 值，交换机必须支持 SNMPV2 及以上的版本，下面给出 H3C、华为、思科交换机的配置

H3C 交换机配置

[Sysname]snmp-agent sys-info version v1v2c

[Sysname]snmp-agent community read public

华为交换机配置

snmp-agent community read public

snmp-agent sys-info version all

思科交换机配置

snmp-server community public ro

通过上面的配置，设置只读 community 名为 public；

2、配置 Cross 中认证选型中的 SNMP，如下图所示

如果内网有 3 台三层交换机，其中一台为核心交换机，另外两台分别为连接到核心交换机的三层交换机 A 和 B。

则三台交换机的 IP/MAC/Oid/Community 都必须填入到 SNMP 服务器列表中。

核心交换机不要求一定能支持 SNMP，但是设置 SNMP 选项时必须要把核心交换机的 IP、MAC 填写进去，在不支持 SNMP 时，oid 和 community 可以随便设置。

例如 192.168.2.1/00:01:03:0A:EF:03/.1.3.6.1.2.1.4.22.1.2/public

其中 192.168.2.1 为三层交换的 IP 地址，00:01:03:0A:EF:03 为三层交换的 MAC 地址，IP 和 MAC 为三层交换机离设备最近的接口 IP 和 MAC 地址。

.1.3.6.1.2.1.4.22.1.2 为固定的；

public 为三层交换的 community 名称；

3、配置认证方式为 MAC 认证，并绑定 MAC 地址。

4.4 主备配置

如果您的网络是冗余网络拓扑接口，可以在网络中部署 2 台 Cross 上网行为管理设备，实现冗余备份，下面介绍以网桥模式 HA 配置，部署拓扑分下面两种;

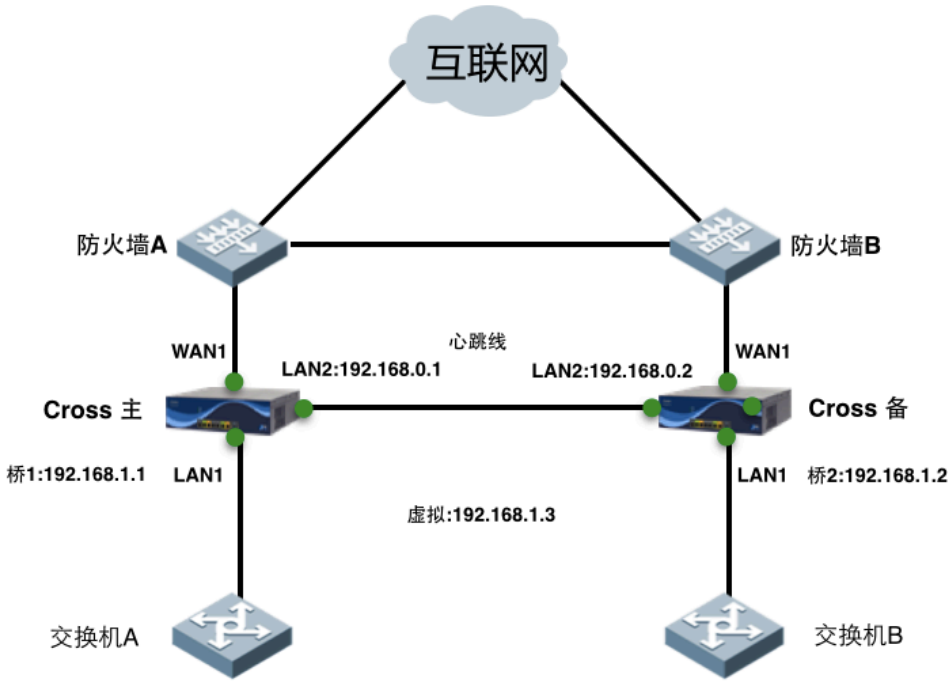


图 1

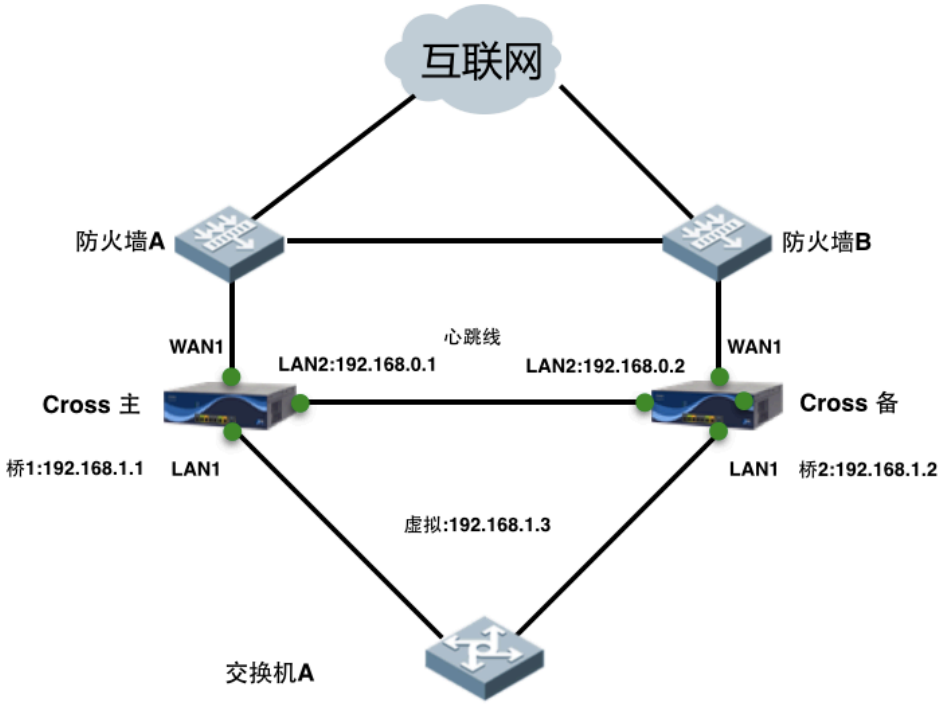


图 2

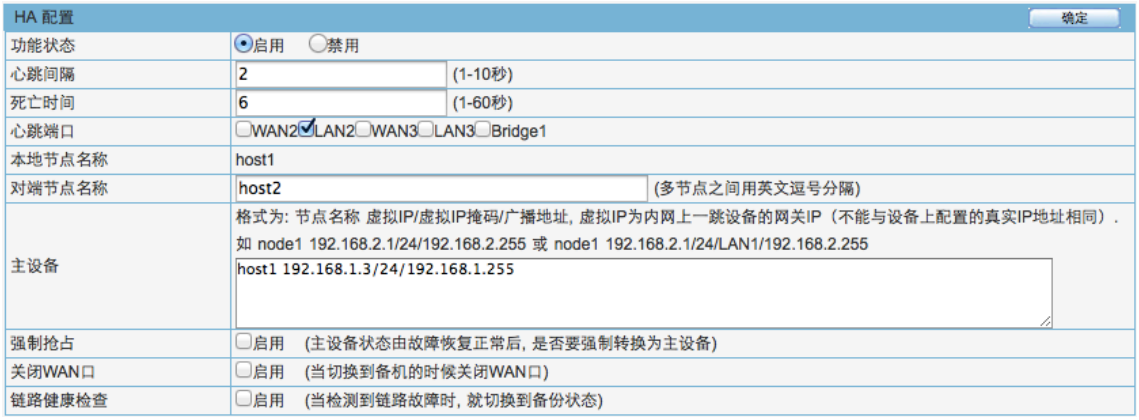
第一步:配置主备设备的 IP 地址，主网桥 1：IP 地址 192.168.1.1/24；备网桥 1：IP 地址 192.168.1.2/24，虚拟 IP 地址定义为：192.168.1.3

第二步：配置心跳线 LAN2 地址，主设备配置成 192.168.0.1/24，备设备配置为 192.168.0.2/24

第三步：配置主备设备的节点名称,在”系统配置-系统信息”里修改主设备配置为 host1，备设备配置为 host2

第四步 配置 HA ,启用主设备“自动同步”,“同步 IP”填备机 LAN2 接口的 IP 地址 :192.168.0.2(主设备保存配置的时候将自动把配置同步到备机)

第五步:在主设备上配置心跳间隔 2s，死亡时间 6s，心跳端口选 LAN2.，对端节点名称写备份的节点 host2,主设备一栏写 host1192.168.1.3/24/192.168.1.255.强制抢占和链路健康检查视情况而定(注意,主设备一栏节点名称需要写要协商成主设备的节点名称,虚拟 IP 必须和 Bridge1IP 相同网段,但是不能和内网地址有冲突)。备份设备除了对端节点名写 hostname001,其他的和主设备一样.



第 6 步:配置完后,先启用备份设备的 HA 功能,然后在立即开启主设备的 HA 功能,过几秒种 host1 这台就协商成主设备,host2 协商成备份设备,备份设备不转发数据,主设备可以有按钮一键切换到备份设备。

注意事项:(针对图一)

1.第一次 HA 上线的时候，先连接心跳线，并配置心跳线，然后登陆上去，把 pc 接到主设备

LAN1，WAN1 连接备机的 WAN1 口，登陆主机和备机，备机先开启 HA，然后主机开启 HA，协商好后,就可以插线了。

2.Cross 主备 LAN1 口都接在一个交换机上时，在协商好之前，备机不能插线，协商成一主一备后，备机插上线，以防协商过程中出现的短暂环路。

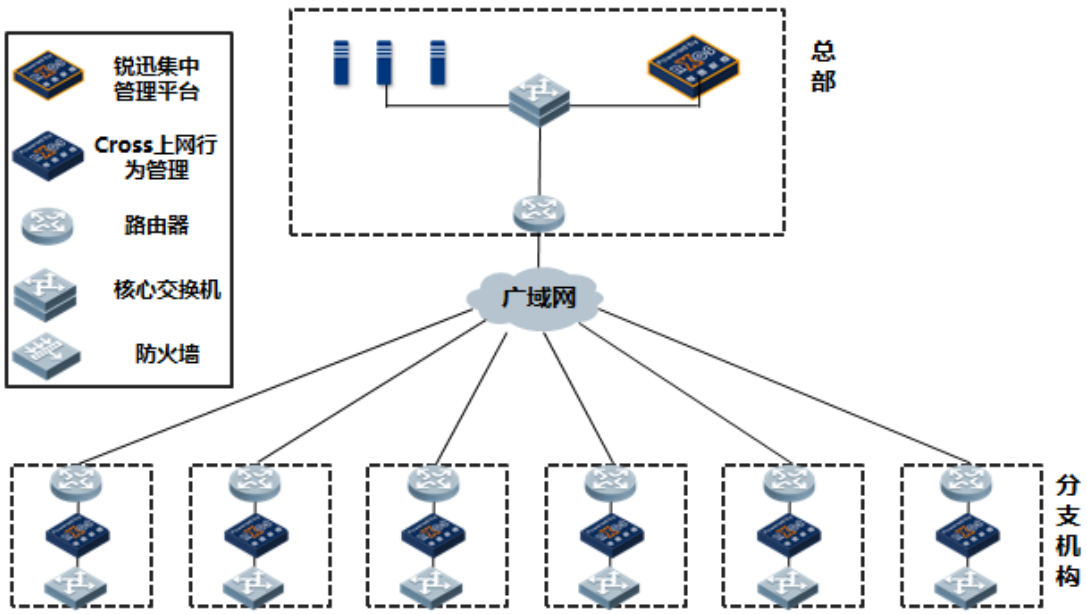
3.备机设备断电的情况下需要把接口线拔了,以防断电 bypass 出现的环路。

4.心跳线出现问题的情况下，2 台设备都会变成主的,需要把原来备机的线拔掉。

4.5 集中管控配置

华御集中管控可以对企业全网行为管理设备统一进行策略下发、定时备份配置文件、上网行为、流量行为、日志记录、全网设备状态操控等数据，同时还支持分支机构自行设置个性化管理策略，实现“个性化管理”与“集中管理”完美结合。

在管理员分级管理方面，通过将全网流量管理、行为管理设备划入到不同“区域”中，将不同“分支”的管理权限分配给不同级别的管理员，使管理职责更清晰，总部和分支的管理员协作更加高效，能有效降低管理成本和沟通成本。



对于部署了上网行为管理平台的网络环境，华御集中管理平台，将进一步提升企业网络的统一管理，更加规范企业城域网权限、策略分配的合理性。

配置说明：公司总部在深圳,假设有 10 个分支机构,总部和每个分支机构在网络出口，都部署一台上网行为管理设备。现在总部部署一台集中管理平台(中心端设备),用于集中管理这 11 台上网行为管理设备(受控端:网点设备)。[防火墙策略]、[流量管理策略]和[上网行为策略对象]由总部统一下发。其中北方有 8 个网点设备,南方有 3 个网点设备,北方和南方的管理策略稍不同。在此将建立两个子区域:南方区和北方区,两个区域引用不同的配置模版。

上例的配置步骤如下:

网点设备配置:

(1) 配置每台网点设备的基本功能,如 IP 地址、路由等。前面已经体现,此处不做详细描述。

(2) 在每台网点设备上启用集中管理功能。

每台网点设备启用[集中管理]和[集中配置模板]的配置方法类似,这里以其中一台(深圳 SF)为例,进行详细说明

配置步骤

(1)进入网点设备的【系统配置>集中管理】页面,启用集中管理功能,并配置相关参数。如下图:

(2)[流量管理>基于策略的流控]、[流量管理>基于用户的流控]和[上网行为策略对象],这四个功能启用[集中配置模板]的配置方法类似,这里以[流量管理>基于策略的流控]为例。

进入网点设备的【流量管理>基于策略的流控】页面,在[使用集中配置模版,该页面的配置将与集中配置模版一致]处,选择[启用],并点击右上角的<确定>按钮。

如下图:

中心端设备配置过程:

(1)配置中心端设备的基本功能,如 IP 地址、路由等。

(2)配置全局参数,配置[虚拟网络 IP 地址池]和[通讯端口],顺丰使用默认值即可。

(3)新建两个模版:统一模版 1 和特殊模版,然后分配置两个模版的策略。

(4)建立两个区域:统一模板区和特殊模板区,[统一模板区]引用[统一模版 1],[特殊模版区]引用[特殊模版模版]。

(5)将各网点设备分别加入统一模板区和特殊模板区。

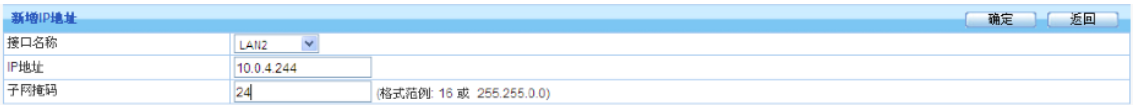
(6)将模版配置下发到各个网点设备。

(7)通过中心端连接到每台网点设备或网点设备的报表中心,对每台网点设备进行单独的配置和管理。

详细配置如下:

(1)配置中心端 IP 地址和静态路由:主要是为了让深圳总部和各地分部的上网行为设备能够连通集中管控设备

第一:进入【网络配置】>【配置 IP 地址】页面,配置集中管控地址为 10.0.4.244 如下图所示:



第二:进入【网络配置】>【静态路由】页面,配置一条缺省路由,使集中管控设备能 ping 通外网,假设网关地址为 10.0.4.1,如下图所示

(2)第 2 步配置使用默认值即可

(3)配置模板,在模板上制定相应策略,进行各个分支的统一策略下发,根据顺丰实际情况,建立 1 个统一的模板和一个特殊的模板,大多数网点执行统一模板,少数根据需求引用特殊的模板,所有策略配置都在总部集中管控配置,分支无权配置设备,只能查看设备。

第一:定义好南北区域的模板,进入【集中管理>模版配置】页面,配置策略模版:统一模版 1、特殊模版。

模版添加完成后,如下:

全局配置模板 新增

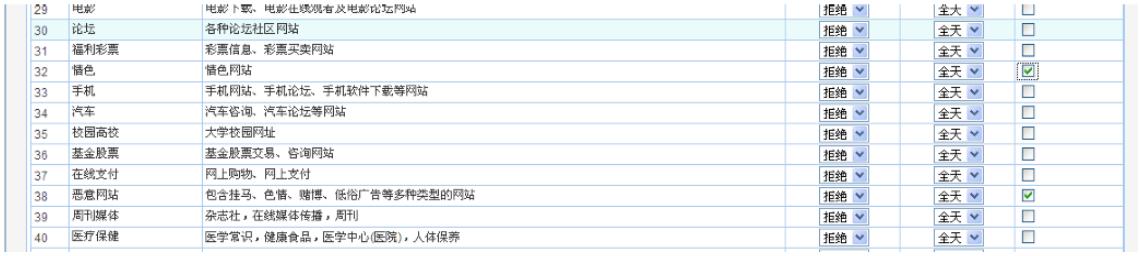
序号	模板名称	描述	操作
1	统一模版1	大多数设备的策略模版	配置 修改 删除
2	特殊模版	特殊设备的策略模版	配置 修改 删除

点击操作栏的<配置>按钮,弹出模版配置页面,即可设置该模版相关的策略。由于顺丰总部和分部都是与 AD 域结合做认证和相应的策略,所有的策略都根据 AD 域定义好的进行配置,那么需要总部和分部的 AD 域的安全策略组名必要配置一样的名称,以便于统一下发的时候策略对应,假设总部和分部 AD 定义的安全组策略有如下几个 webvideo-deny、 p2p-deny 以及 URL-deny 这 3 个组,在所有网点设备的 AD 域导入这 3 个组,然后在集中管控的模板下发基于策略流控引用这 web-deny、 p2p-deny 这 2 个组,行为管理定义需要过滤的 url,然后在 URL-deny 里引用此组,AD 域导入已经详细说明,集中管控模板下发配置如下:

第一:进入模板配置页面的【流量管理>基于策略的流控】页面,配置 p2p-deny 策略,如下图:

配置 webvideo-deny 策略,如下图

第二:进入模板配置页面的【行为管理>上网策略对象】页面,配置 URL-deny 策略,比如禁止色情和病毒类的网页,如下图:



29	电影	电影下载、电影在线观看及电影论坛网站	拒绝	全天	
30	论坛	各种论坛社区网站	拒绝	全天	
31	福利彩票	彩票信息、彩票买卖网站	拒绝	全天	
32	情色	情色网站	拒绝	全天	☑
33	手机	手机网站、手机论坛、手机软件下载等网站	拒绝	全天	
34	汽车	汽车咨询、汽车论坛等网站	拒绝	全天	
35	校园高校	大学校园网址	拒绝	全天	
36	基金股票	基金股票交易、咨询网站	拒绝	全天	
37	在线支付	网上购物、网上支付	拒绝	全天	
38	恶意网站	包含挂马、色情、赌博、低俗广告等多种类型的网站	拒绝	全天	☑
39	周刊媒体	杂志社，在线媒体传播，周刊	拒绝	全天	
40	医疗保健	医学常识，健康食品，医学中心(医院)，人体保养	拒绝	全天	

配置好策略后,在每个网点的组织结构对应的 URL-deny 组里引用该上网策略对象即可设置完模版后,需要保存模版的配置。点击模版配置页面右上角的<保存>按钮,保存模版相关的配置

(4)配置区域进入【集中管理>网点管理】页面,在根区域(Root)之下添加两个区域:统一模版 1 和特殊模版。这里以新增[统一模板 1]为例。点击<新增区域>按钮,增加区域,如下图:

(5)配置网点和引用模板

新增每台网点设备的配置方法类似,这里以其中一台(深圳 SF)为例。进入【集中管理>网点管理】页面,在左边的树形结构上,定位到[统一模板 1]。然后点击<新增网点>按钮,增加网点[深圳 SF],如下图:

(6)通过中心端连接到每台网点设备或网点设备的报表中心,对每台网点设备进行单独的配置和

管理。

操作说明:

点击<配置>按钮,即连接到该网点设备的配置页面,可对网点设备进行单独的配置和管理。

点击<报表中心>按钮,即连接到该网点设备的报表中心系统的页面,可对网点设备的报表中心进行单独的管理。

点击<模版下发>按钮,即将该网点设备引用的策略模版里包含的配置下发到网点设备。以网点设备[深圳 SF]为例。模版下发后,在对应的策略页面可以看到已下发的策略。

如在【防火墙>安全策略】页面,查看已下发的配置。如下图:

图 1.配置网点

规则名称为红色,表明这些规则是通过集中配置模版下发的,不是在该设备上单独配置的。点击操作栏的<查看>按钮,可以查看该规则的详细配置。