BiGuard 50G

用户手册

V1.10（FW2.05）

目录

1. 前言

随着 Internet 的爆炸性增长，IP 业务的蓬勃发展，网络应用成指数级增长，同时网络安全的需求也越来越大，传统路由器的安全性已满足不了企业成长的需求，新一代的 BiGuard 50G 企业级防火墙路由器提供了强大的数据安全性和极高的可靠性、可用性，满足了当前市场的需求，适应了未来的技术发展趋势。
本手册着重介绍了 BiGuard 50G 企业级防火墙路由器的技术特点、性能指标、配置细节，为广大用户和网络技术人员深入掌握产品提供帮助。

2. 概述

随着 Internet 业务量呈指数级增长，IP 已成为全球新一代网络基础设施的首选传输方式
，基于 IP 协议的业务已经完全主宰服务供应商的网络，通信网络正处于深刻的变革之中。这一变革，为企业提供了数据、语音和视频等多业务的宽带网络，企业在应用这些业务的同时，也带来了诸如数据传输不安全、企业网络受攻击、语音质量不高等网络问题。企业迫切需要一种解决方案来改善这种状况，为此我们推出了这款集防火墙、路由器、IPQoS 、IPsec VPN 于一体的企业级安全网关设备——BiGuarad 50G。

2.1. 主要特性

2.1.1. 全面支持虚拟专用网络

BiGuard 50G 支持全面的 IPsec VPN 协议，强大的数据加密和数据完整性校验为企业在多个站点之间通信的时候提供安全的隧道，保证数据传输的安全性，即使站点在 NAT 设备后面，隧道也能够透明的穿越过去，并且创新实现了 VPN 中转，即站点只需和中心站点建立隧道连接，即可与其他站点进行通信。

2.1.2. 高级防火墙

高级的防火墙保护企业内部不受外来攻击，能有效防止七类二十多种 DoS 攻击；通过状态检测机制来限制对企业内部网络的访问，以及控制企业内部员工数据外发，包括代理过滤、域名过滤、智能内容过滤等多种策略，而且在内部网络有问题的时候可以用邮件来通知管理人员。

2.1.3. 智能带宽管理

BiGuard 50G 具有粒度细致、方便灵活的带宽管理功能。采用 IPQoS 来提供可靠的带宽服务，特别是语音业务，视频业务，需要较高的时实传输性能，即使在负载很高的情况

下，系统能够智能的决定为这些服务提供转发优先级和可用带宽，以保证服务质量。

2.1.4. 负载均衡和失效切换

BiGuard 50G 提供了两个 WAN 接口，使得企业宽带接入更具灵活性，并且专门为企业网络做了负载均衡和失效切换的解决方案，大大提供了企业网络的可用性和可靠性。

2.1.5. 多样化的工作模式

BiGuard 50G 支持路由模式、透明网桥模式、混合模式三种模式，以适应不同复杂情况的网络拓扑结构。透明网桥模式无须改变网络拓扑，就可以让 BiGuard 50G 和带 VLAN 功能的交换机互联；混合模式则提供透明网关的功能；

2.1.6. 高级 NAT 功能

BiGuard 50G 提供了 4K 容量的 NAT 表，对于各种报文能够智能的应用地址转换还是端口转换，不仅支持多对一的映射，还支持多对多的映射，诸如不同子网对应不同的出口地址映射。

2.1.7. SIP 电话和 IPTV 的支持

BiGuard 50G 支持 SIP 电话的穿透以及 IPTV、VOD 等组播业务；

3. 详细功能描述

3.1. 面板描述

3.1.1. 面板指示灯功能表

指示灯	功能
电源灯	设备上电后，电源灯保持长亮，显示绿色；
状态灯	设备上电后，系统未启动完毕时显示橙黄色，启用完毕后状态灯熄灭；
LAN 1-4 端口	10/100M：端口工作在 100Mbps 时，显示绿色，工作在 10Mbps 时，指示灯不亮； Link/Act：端口连接后，显示长亮；有流量经过时绿灯闪烁；
WAN1	10/100M：端口工作在 100Mbps 时，显示绿色，工作在 10Mbps 时，指示灯不亮； Link/Act：端口连接后，显示长亮；有流量经过时绿灯闪烁；
WAN2	10/100M：端口工作在 100Mbps 时，显示绿色，工作在 10Mbps 时，指示灯不亮； Link/Act：端口连接后，显示长亮；有流量经过时绿灯闪烁；
无线天线	一个可以拆卸的 2.4GHz 5dbi SMA 天线

3.1.2. RESET 按钮设置

面板上的 RESET 按钮，在设备上电的情况下，按住持续 10 秒，设备能够恢复到出厂默认设置；

3.2. 功能描述

3.2.1. 状态

状态信息记录了一些系统参数列表以及统计信息、日志信息等。

3.2.1.1. 设备信息

设备信息界面显示了设备的基本信息，分为三个部分：

第一部分为设备的基本信息：包括设备名称、系统启动时间、失效切换状态、私有 LAN MAC 地址、公有 WAN1 MAC 地址、公有 WAN2 MAC 地址、版本信息、Home URL；
第二部分为 LAN 的基本信息：包括 IP 地址、网络掩码、DHCP 服务器；
第三部分为 WAN1 和 WAN2 的基本信息：包括 WAN 连接方式、IP 地址、网络掩码、网关、DNS 服务器、启动时间；

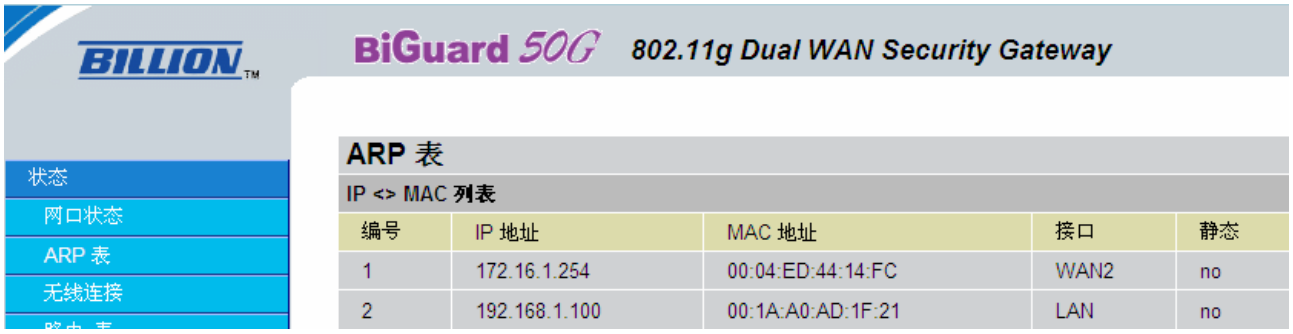
3.2.1.2. 网口状态

网口状态显示了设备当前 WAN1 、WAN2 和 LAN1-4 端口的连接状态。

端口：显示对应的端口号。
状态：显示与端口号对应的端口的状态。断开或者连接。点击**断开**或**连接**查看详细信息。

3.2.1.3. ARP 表

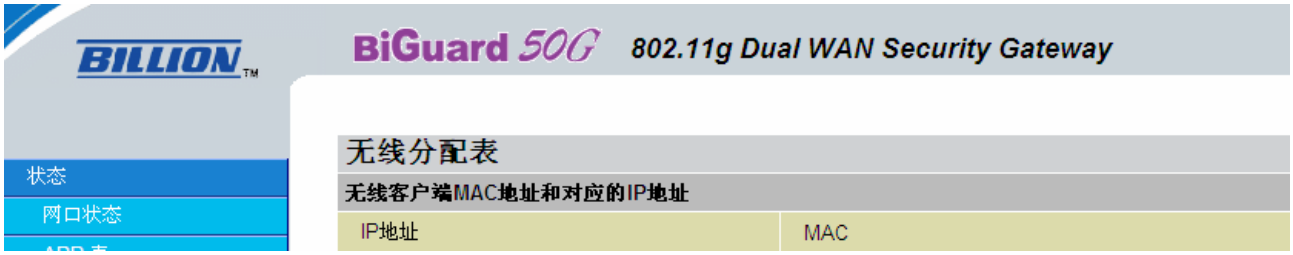
ARP 表显示了设备缓存中的 ARP 记录，也就是 IP 地址与 MAC 地址的对应关系。



静态：IP 地址与 MAC 地址的对应关系有静态的，也有动态的，“**yes**”表明是静态的对应关系，“**no**”表示是动态的对应关系。静态的对应关系能有效防止 ARP 欺骗攻击。动态对应关系系统能够自己获得。

3.2.1.4. 无线分配表

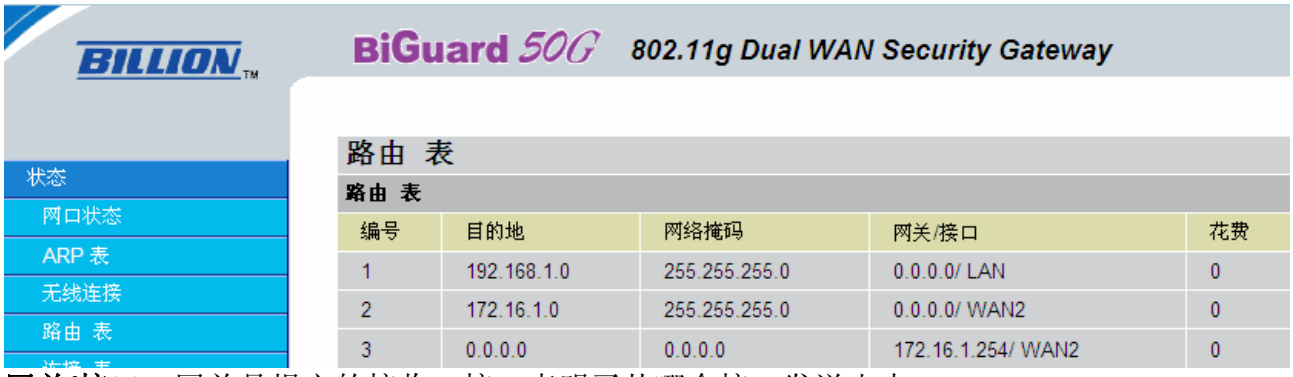
也就是无线网络中的 IP 地址与 MAC 地址的对应表。



IP 地址：无线网络中设备的 IP 地址；
MAC：无线网络中设备的 MAC 地址；

3.2.1.5. 路由表

下图显示了路由表条目，路由表显示出报文如何被转发的。



编号	目的地	网络掩码	网关/接口	花费
1	192.168.1.0	255.255.255.0	0.0.0.0/ LAN	0
2	172.16.1.0	255.255.255.0	0.0.0.0/ WAN2	0
3	0.0.0.0	0.0.0.0	172.16.1.254/ WAN2	0

网关/接口：网关是报文的接收，接口表明了从哪个接口发送出去；
花费：路由好坏的一个度量指标，路由器能智能的根据开销来选择路由；

3.2.1.6. 连接表

连接表，显示了当前设备上面存在的所有连接。

编号	协议	源IP	源端口	目的IP	目的端口
1	TCP	192.168.1.100	1671	220.180.211.11	80
2	TCP	192.168.1.100	1536	207.46.124.221	1863
3	TCP	192.168.1.100	1669	220.180.211.11	80
4	UDP	192.168.1.100	13217	202.104.241.3	8000
5	TCP	192.168.1.100	1875	192.168.1.254	80
6	TCP	192.168.1.100	1873	192.168.1.254	80
7	UDP	192.168.1.100	4000	58.60.14.48	8000

3.2.1.7. DHCP 表

动态主机配置列表，从这张表中可以找到哪些主机被分配了哪些 IP 地址。

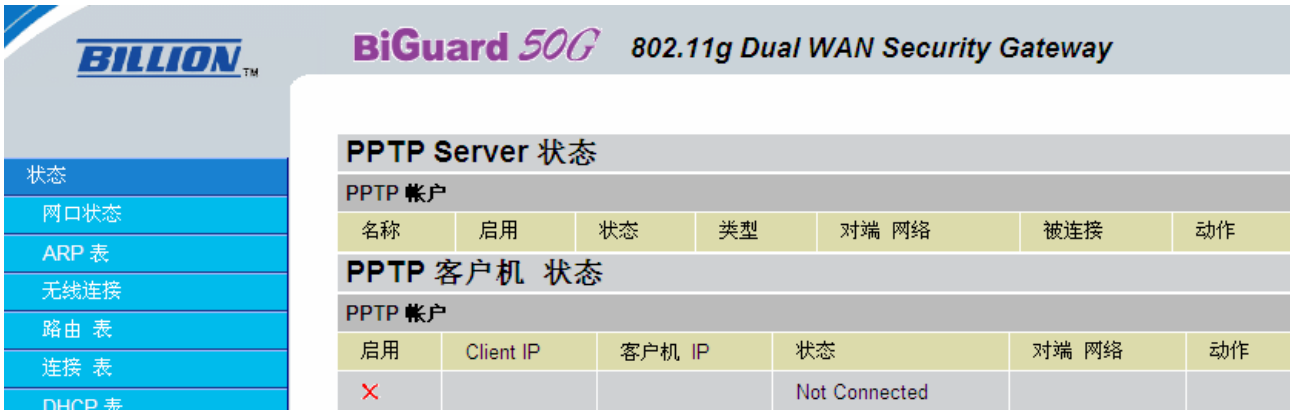
3.2.1.8. IPsec 状态

IPsec 的通道状态显示，当在设备上面建立了 IPsec VPN 后，可以在这个界面查看建立的通道以及通道的状态。

启用：该通道是否被启用；
状态：当处于启用状态时显示为“**激活**”，否则显示“**未激活**”；
SA：通道连接成功时显示“**Phase 1 建立、Phase 2 建立**”，未成功不显示；
动作：对于该通道连接可以做的两个动作，一个是断开连接，一个是发起连接；

3.2.1.9. PPTP 状态

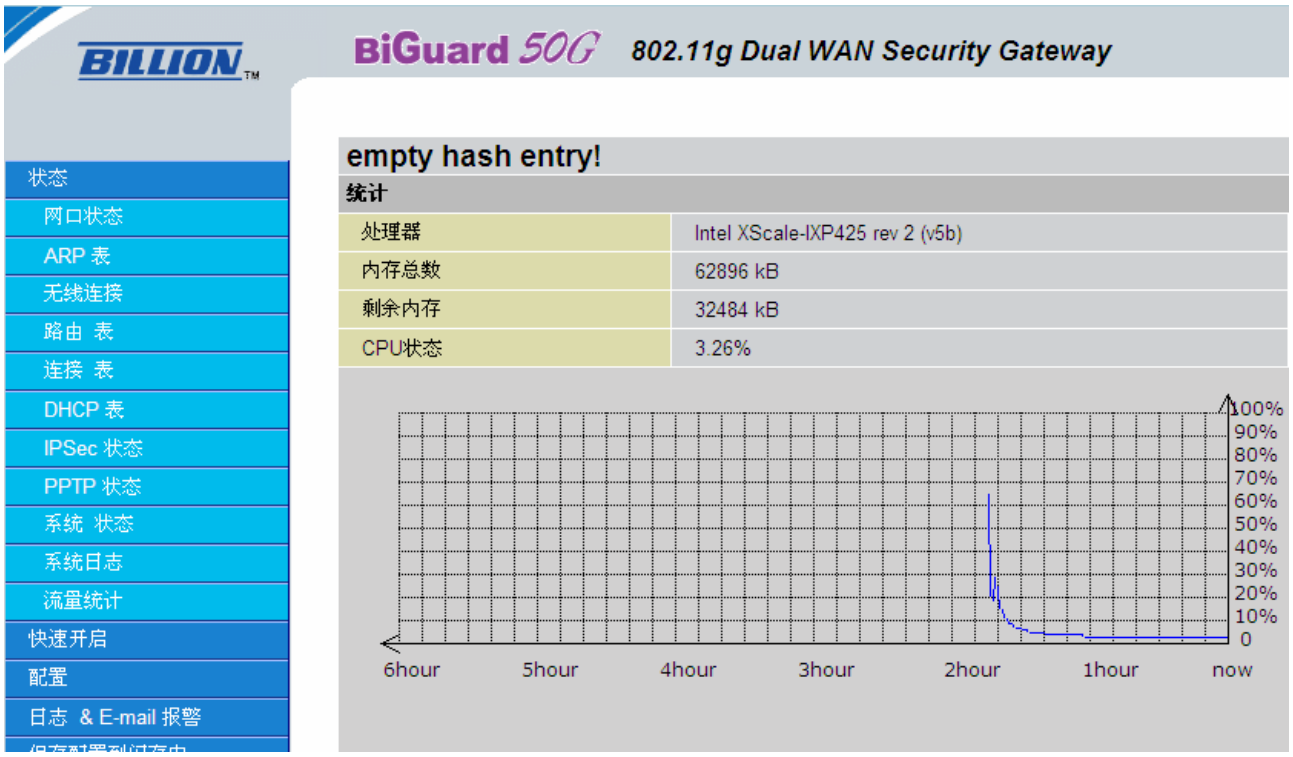
PPTP 状态显示了远程用户拨入的情况；最大支持 4 个远程用户同时拨入；



名称：PPTP 帐号的连接名称，在配置 PPTP 帐号的时候会要求输入一个连接名称来标识该帐号；
启用：帐号是否有效；
状态：使用该帐号拨入成功后，显示“**激活**”，否则显示“**未激活**”；
类型：用户类型，主要有两种：远程访问用户和 LAN to LAN，前者不对拨入用户的网络做限制，后者会受到限制；
对端网络：只有用户类型为 **LAN to LAN** 的时候才会显示拨入用户的网络；
被连接：远程用户拨入时建立连接使用的 IP 地址；
动作：PPTP 服务器可以断开远程用户拨入的连接；

3.2.1.10. 系统状态

系统状态显示了 BiGuard 50G 的硬件系统状态。



处理器：显示了 BiGuard 50G 的处理器芯片型号；

内存总数：显示了 BiGuard 50G 的内存总数；
剩余内存：显示了 BiGuard 50G 的剩余内存；
虚拟硬盘：显示了 BiGuard 50G 的虚拟硬盘总数；
CPU 状态：显示了 BiGuard 50G 的处理器使用率；

3.2.1.11. 系统日志

系统日志显示了设备在运行过程中产生的事件，包括受到外来攻击的事件。

可以通过选择“**显示**”下拉列表的事件种类来显示关心的内容，可供选择的事件种类有以下 11 种：

1. 所有日志：同时显示所有种类的事件；
2. 系统维护事件：需要在日志&E-mail 报警->日志配置里面启用记录该事件；
3. 系统错误事件：同样需要在日志&E-mail 报警->日志配置里面启用记录该事件；
4. 访问控制事件：该事件包含了防火墙所有事件，同样需要在日志&E-mail 报警->日志配置里面启用记录该事件；
5. 包过滤事件：需要在防火墙->包过滤和日志&E-mail 报警->日志配置里面同时启用记录该事件；
6. LAN MAC 过滤事件：需要在防火墙->LAN MAC 过滤和日志&E-mail 报警->日志配置里面同时启用记录该事件；
7. 入侵侦测事件：需要在防火墙->入侵侦测和日志&E-mail 报警->日志配置里面同时启用记录该事件；
8. 调用数据记录事件；
9. 点对点连接事件：包括 PPPoe 和 PPTP 连接事件，需要日志&E-mail 报警->日志配置里面启用记录该事件；
10. 远程访问事件：需要日志&E-mail 报警->日志配置里面启用记录该事件；

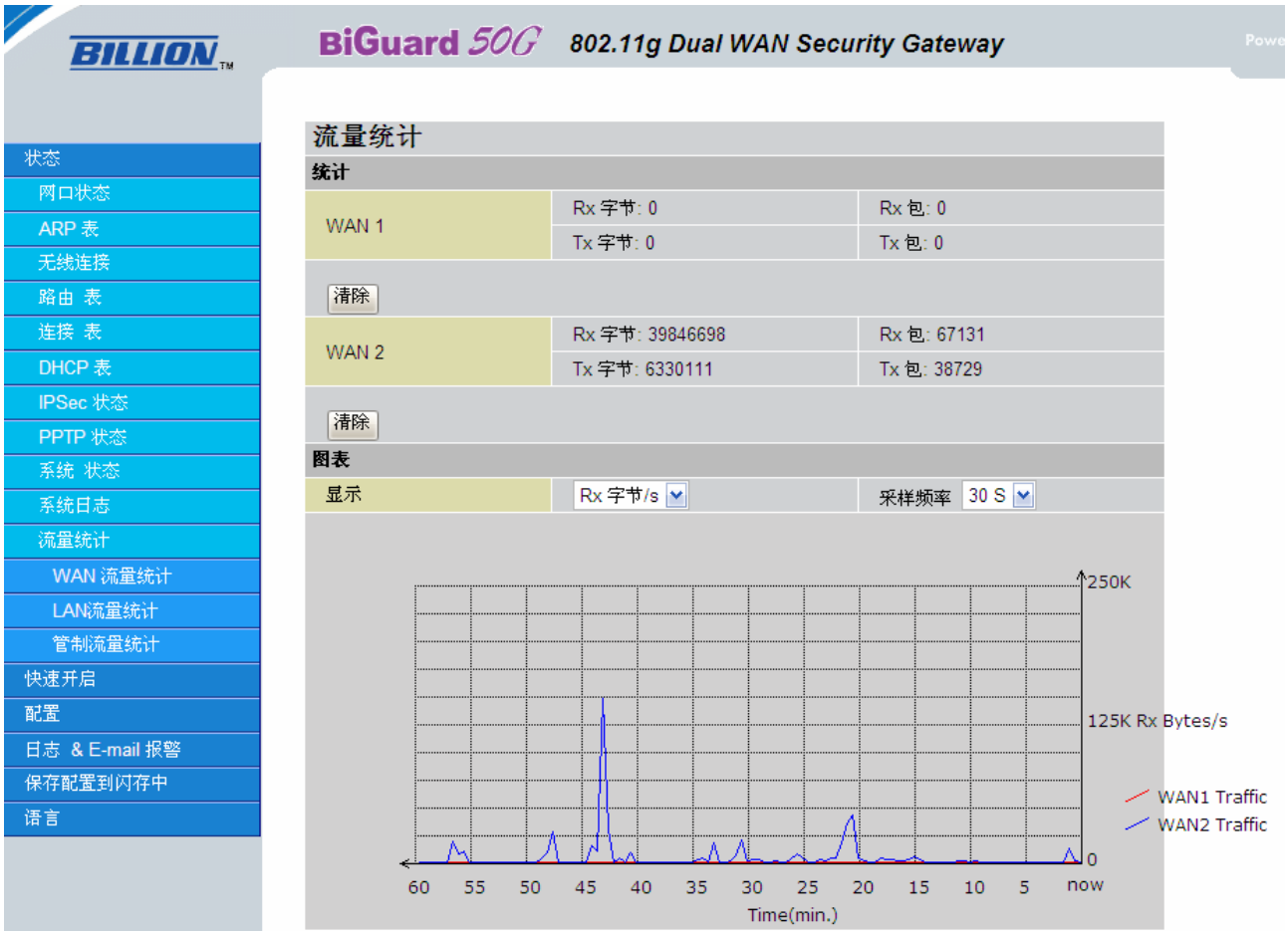
11. IPsec VPN 事件：需要日志&E-mail 报警->日志配置里面启用记录该事件；
12. IM： 需要日志&E-mail 报警->日志配置里面启用记录该事件；
13. P2P：需要日志&E-mail 报警->日志配置里面启用记录该事件；

同时提供三个按钮来处理日志记录：
“刷新”、“清除日志”、“发送日志”；

3.2.1.12. 流量统计

流量统计包括了 WAN 流量统计，LAN 流量统计和管制流量统计，并且配以图表显示时实流量变化；

WAN 流量统计



在 WAN1 和 WAN2 接口上面做如下统计：
Rx 字节：接收字节总数；
Rx 包：接收报文总数；
Tx 字节：发送字节总数；
Tx 包：发送报文总数；
可以通过选择以上四个统计参数，查看以图表形式展现的时实流量变化；

LAN 流量统计

连接限制：当用户在 LAN 流量统计中发现问题时可以点击入侵侦测进行策略调整。
IP 阻塞：当用户在 LAN 流量统计中发现问题时可以点击包过滤进行策略调整。
IP 地址：内部主机的 IP 地址。
字节/秒：数据流量的大小。
%：显示每个连接的数据流量的百分比。

1.点击**入侵检测**，配置入侵检测

入侵检测系统 (IDS) 用来检测来自 Internet 的黑客攻击和入侵行为。如果已启用防火墙的 IDS 功能，将对所有入站数据包进行过滤，并根据是否被检测为可能的黑客攻击、入侵行

为或其他路由器认为可疑的连接进行阻塞。

2.点击**包过滤**配置包过滤

ID：显示包过滤条目的 ID。
方向：显示包的流动方向，出战或者入站。
源 IP:显示包的源 IP 地址。
目的 IP：显示包的目的 IP 地址。

点击**创建**，增加包过滤规则

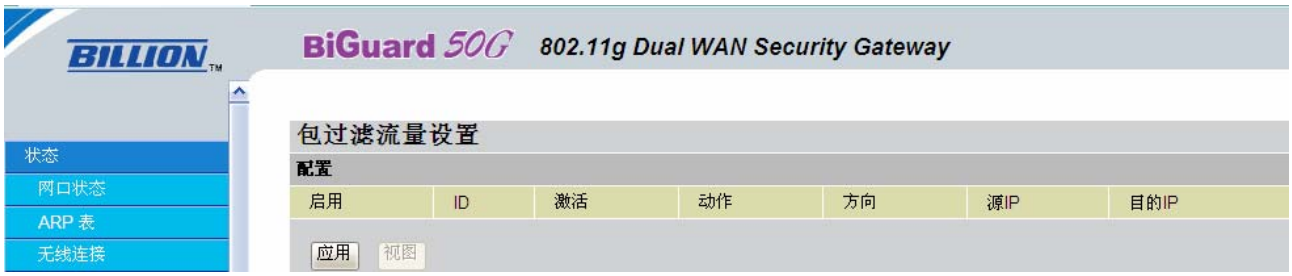
源地址/目的地址：用来允许或阻塞发送/接收来自特定 IP 地址的流量的地址过滤。选择您想要允许或阻塞的 IP 地址的子网掩码；将 IP 地址和子网掩码设置为 **0.0.0.0**，以禁用地址过滤规则。

协议：应用使用的包协议类型，可以选择 TCP 或 UDP，也可两者都选。

源端口范围：定义允许被远程/WAN 用来连接到应用程序的端口或端口范围。默认设置范围是：**0 ~ 65535。**建议高级用户配置此项。

目的地端口范围：定义应用的端口或端口范围。

管制流量统计



ID：显示包过滤条目的 ID。
方向：显示包的流动方向，出战或者入站。
源 IP:显示包的源 IP 地址。
目的 IP：显示包的目的 IP 地址。

3.2.2. 快速开启

快速开启旨在指导用户进行简单的配置，即可融入用户网络；

3.2.2.1. 快速开启 WAN1

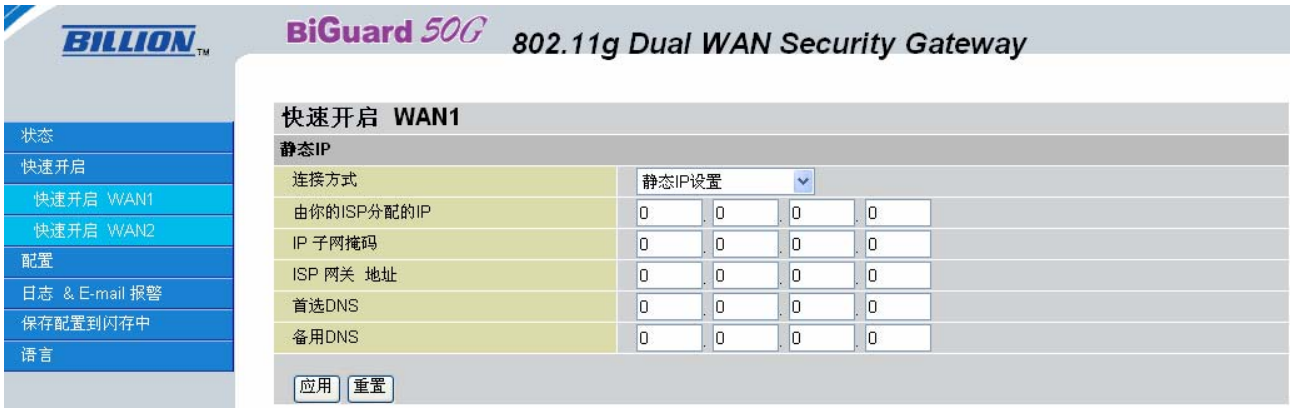
快速开启 WAN1 的配置，能够迅速完成与用户现有网络的融合；

WAN1 接口的连接方式有以下 5 种：

1. **自动获得一个 IP 地址；**
2. **静态 IP 设置；**
3. **PPPoE 设置；**
4. **PPTP 设置；**
5. **Big Pond 设置；**

3.2.2.1.1. 自动获得一个 IP 地址

3.2.2.1.2. 静态 IP 设置

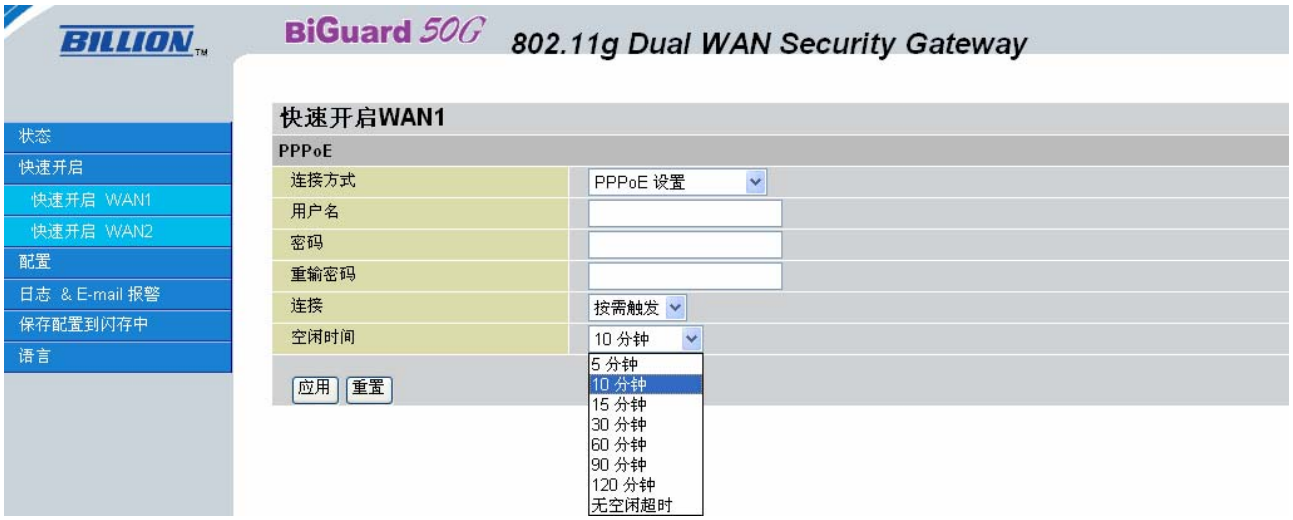


3.2.2.1.3. PPPoE 设置

连接的两种方式：

1. **总是连接：**一旦 PPPoE 连接建立后，连接总是存在，当“**连接**”选择该种方式时，“**空闲时间**”无需配置；
2. **按需触发：**连接并不总是存在，但可以由用户流量来触发连接的重建，此时需要配置“**空闲时间**”；

空闲时间：表示连接空闲一段时间后自动断开连接，可以通过下拉列表来选择空闲的时间；



3.2.2.1.4. PPTP 设置

PPTP 客户 IP：PPTP 客户端 IP 地址，主要是为了能够与 PPTP 服务器建立连接；
PPTP 客户 IP 网络掩码：子网掩码；

PPTP 客户 IP 网关：PPTP 客户端网关；

PPTP 服务器 IP：ISP 提供的 PPTP 服务器的 IP 地址；
连接的两种方式：

3. **总是连接**：一旦 PPTP 连接建立后，连接总是存在，当“**连接**”选择该种方式时，“**空闲时间**”无需配置；
4. **按需触发**：连接并不总是存在，但可以由用户流量来触发连接的重建，此时需要配置“**空闲时间**”；

空闲时间：表示连接空闲一段时间后自动断开连接，可以通过下拉列表来选择空闲的时间；

3.2.2.1.5. Big Pond 设置

连接方式：连接方式选择“**Big Pond Settings**”，该种方式目前只有澳大利亚的 ISP 支持；

3.2.2.2. 快速开启 WAN2

对 WAN2 接口进行配置，请参考快速开始 WAN1 配置；

3.2.3. 配置

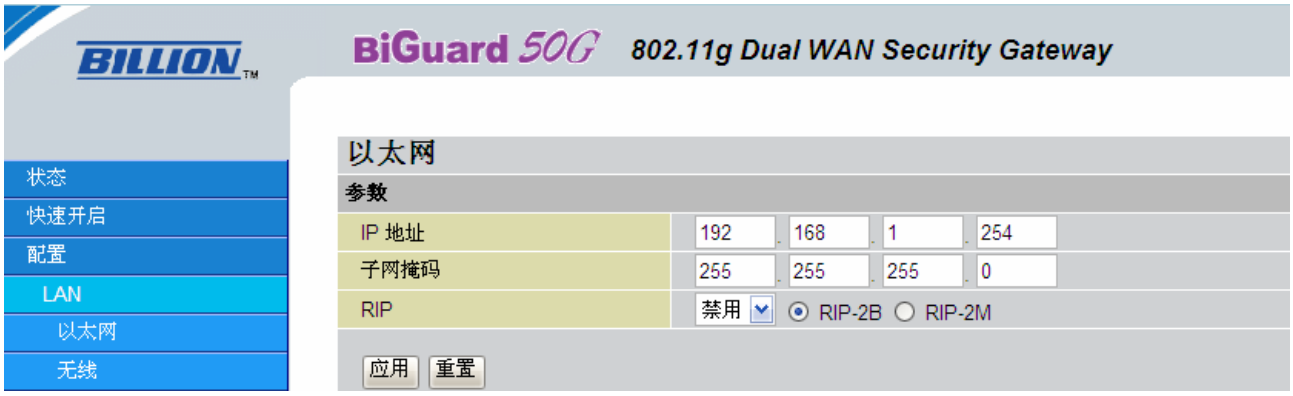
BiGuard 50G 包含了相当丰富的功能，有宽带接入、无线接入、负载均衡、链路备份、策略路由、防火墙、服务质量保证、IPsec VPN、PPTP VPN、DDNS 等等非常强大的功能，以满足用户各种应用，下面就这些功能做详细的配置说明。

3.2.3.1. LAN

LAN 配置主要为 LAN 侧主机提供网关服务以及动态地址分配。

3.2.3.1.1. 以太网

默认的 LAN 网段为 192.168.1.0/24，但可以通过**配置->LAN->LAN 地址映射**章节的配置说明来增加其他网段。



IP 地址：LAN 侧 IP 地址，通常被 LAN 侧主机设置为它的网关；
子网掩码：与 IP 地址一起作用来决定 LAN 侧所属的网段；
RIP：路由信息协议，一种动态路由选择协议，LAN 侧接口如果连接一台路由器，那么

1. **禁用：**不发送路由更新信息，丢弃接收到路由器发出的更新信息；
2. **发送：**只发送路由更新信息，丢弃接收的路由更新信息；
3. **接收：**只接收路由更新信息，不发送路由更新信息；
4. **兼有：**接收同时发送路由更新信息；
5. **RIP-2B：**RIP-2 指示采用路由信息协议第二个版本，并以广播方式发送路由更新信息；
6. **RIP-2M：**以组播方式发送路由更新信息；

3.2.3.1.2. 无线

此表显示无线网络的配置参数。

由静态 IP 设置连接：启用和**禁用**；

无线的模式：有三种，一般默认是 802.11b+g，如果不是很清楚无线的模式，选择默认的；

1. **802.11b；**
2. **802.11g；**
3. **802.11b+g；**

ESSID：无线网络的名称，区别于其他无线接入的名称，无线网络名称的设置不能超过 32 个字符；无线接入的客户端与设备必须有相同的无线网络的名称，才能确保连通性；

隐藏 ESSID：启用和禁用；是否允许任何人连接设备还是允许与设备相同的无线网络名称的客户端连接设备；

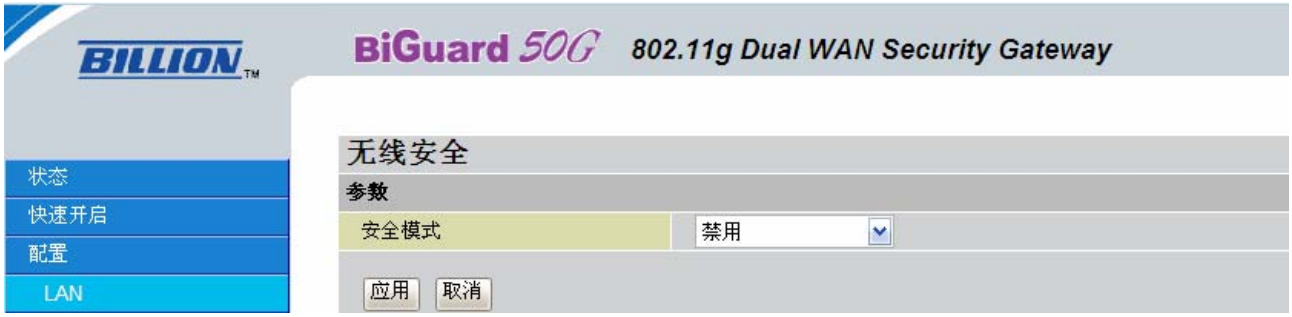
无线区域：有 7 个无线区域，选择无线区域的不同，信道的设置也不相同；

WDS 服务：启用和禁用；

对等的 WDS MAC 地址：与无线接入点的 MAC 地址有关系，无线接入点必须包括对端的 MAC 地址，这样才能够连接互相通信；

3.2.3.1.3. 无线安全

此项显示无线安全三种模式下的配置。



无线安全的模式一共有 4 种：

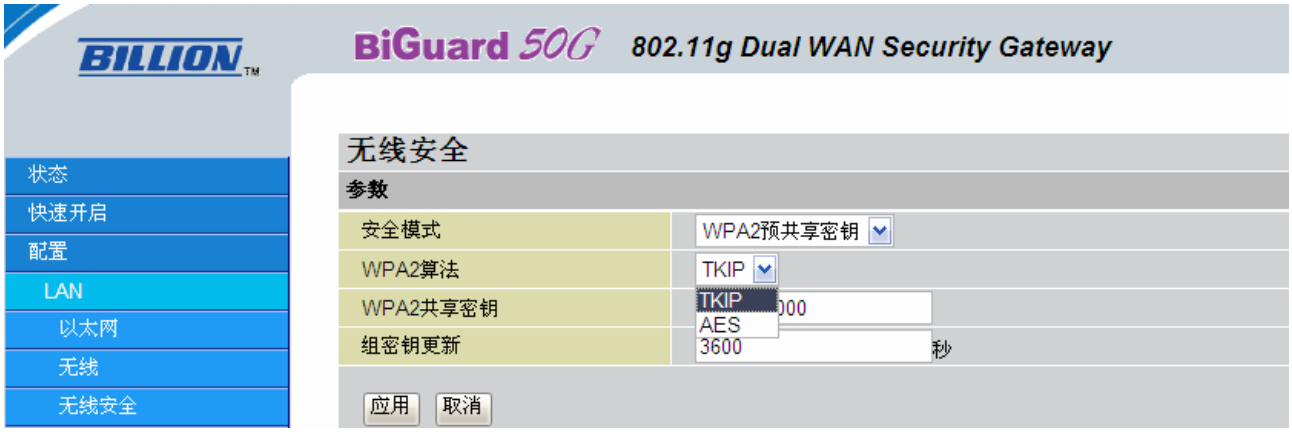
1. **禁用：**不启用无线安全；
2. **WPA 预共享密钥；**
3. **WEP；**
4. **WPA2 预共享密钥；**

当安全模式是 WPA 预共享密钥，WPA 的算法有 2 种：**TKIP** 和 **AES**。
WPA 共享密钥：是为网络鉴定提供的，是以字符的形式表示出来，并且最小 8 个字符，最大 63 个字符；
组密钥更新：在无线客户端和接入点间间隔时间自动更新的安全密码；

WEP 鉴定：有 3 种模式：

1. **开放系统；**
2. **共享密钥；**
3. **兼有；**

当密钥产生作用是无需输入密钥 1、密钥 2、密钥 3、密钥 4。密钥的作用是加密无线数据，增加无线数据传输的安全性；



WPA2 算法有 2 种：**TKIP** 和 **AES**。WPA2 共享密钥与组密钥更新（请参考 WPA1 预共享密钥）

3.2.3.1.4. DHCP 服务器

DHCP 服务器主要为 LAN 侧主机分配动态 IP 地址。

3.2.3.1.4.1. DHCP 服务器参数

IP 池范围开始：规定一个 IP 地址范围用于分配给 LAN 侧主机使用，该参数指定起始 IP 地址；

IP 池范围结束：该参数指定 IP 地址范围的结束 IP 地址；

3.2.3.1.4.2. 主机绑定

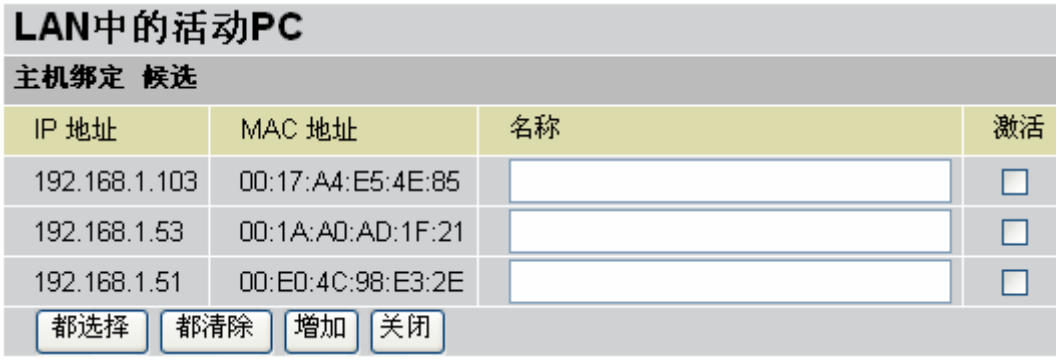
通过建立主机 MAC 地址和 IP 地址的对应关系，来指派给主机固定的 IP 地址，下图是关系表：

建立一个主机 MAC 地址和 IP 地址的对应关系，这样的对应关系在 ARP 表里面显示为静态关系。

名称：该对应关系的名称；
激活：该对应关系是否处于有效状态；

1. **启用：**启用该对应关系；
2. **禁用：**禁用该对应关系；

IP 地址：指派 IP 地址给主机；
MAC 地址：主机的 MAC 地址；
增加：把该对应关系添加到下面列表框内；
取消：取消输入的字符；
侯选：提供了主机 MAC 地址和 IP 地址的对应关系，如果该侯选表中存在某个主机的 MAC 地址和 IP 地址的对应关系，可以直接选择来应用，无需手工输入 IP 地址和 MAC 地址；侯选表的形式如下图：



3.2.3.1.5. LAN 地址映射

LAN 地址映射，主要有两个应用目的：

① 在 LAN 侧添加新的子网，只要是除了 192.168.1.0/24 网段的子网都可以添加；

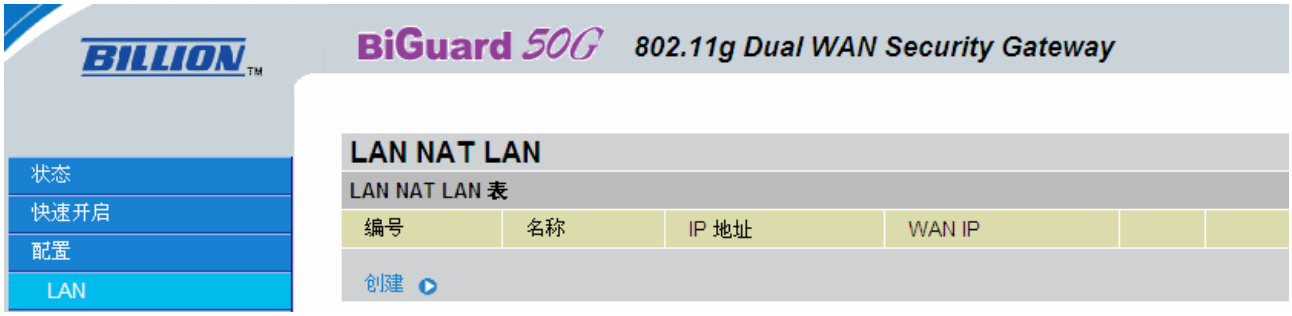
② 为新的子网指派报文的 WAN 侧出接口，可以是 WAN1 接口，也可以是 WAN2 接口；

IP 地址：必须是子网的网关地址，该地址是被配置在系统上的；
WAN IP：被指派的 WAN 侧出接口；
点击后面的“**创建**”，进入规则配置界面：

名称：该规则的名称，或者说新增子网的名称；
IP 地址：必须是子网的网关地址，与下面的子网掩码相结合在系统上产生一个新的网段，LAN 侧主机需要把该地址配置为它的网关地址；
WAN IP 地址：WAN1 接口或者 WAN2 接口的 IP 地址，只能通过“**候选**”来选择，如下图所示，图中的“**名称**”和“**IP 地址**”由 WAN IP 别名配置而来，具体配置请参照**配置->WAN->WAN IP 别名**章节的配置说明；

3.2.3.1.6. LAN NAT LAN

通过 NAT 功能，指定 LAN 口的某个特定 IP 的设备以指定 WAN IP 去访问网络。



名称：子网的名称。
IP 地址：子网的 IP 地址。
WAN IP 地址：WAN 端的 IP 地址。

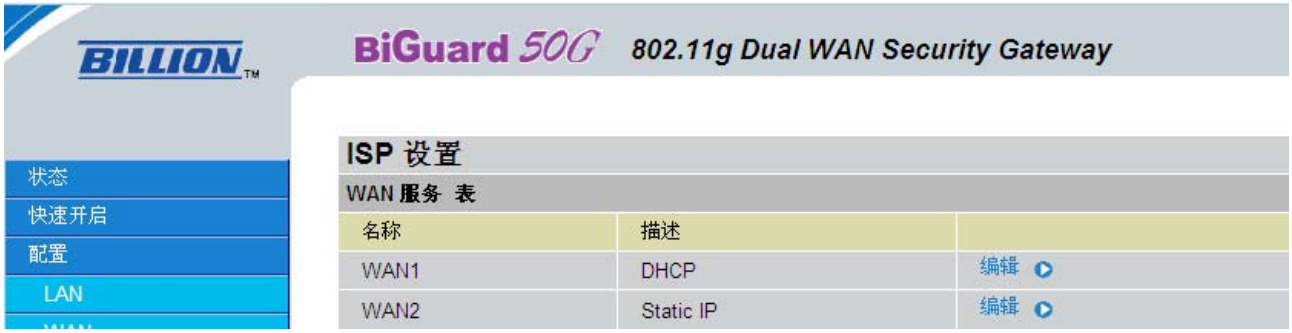
3.2.3.1.7. High Availability

VRRP：启用或禁用虚拟路由冗余协议（VRRP）。
VRID：VRRP 路由器唯一的标识。
Priority：优先权。
Preempt mode:真或假。

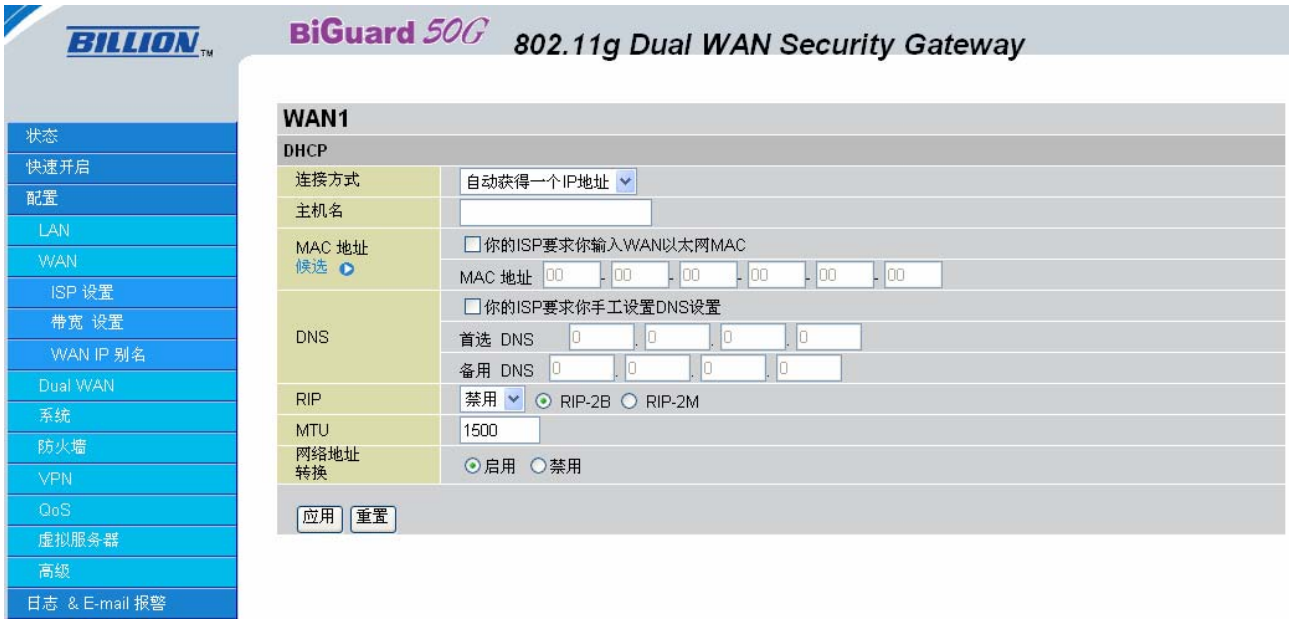
3.2.3.2. WAN

WAN 配置包含 ISP 参数配置和接口带宽配置。

3.2.3.2.1. ISP 设置



WAN 服务表：显示了 WAN 接口的与 ISP 网络的连接方式，比如 DHCP、PPPoE、静态 IP 等；
编辑：进入 WAN 接口的连接方式的配置界面；
如下图显示了 WAN1 接口的配置界面：



连接方式：可选项有：

1. **自动获得一个 IP 地址，也就是 DHCP 方式；**
2. **静态 IP 地址；**
3. **PPPoE 设置；**
4. **PPTP 设置；**
5. **Big Pond 设置；**

3.2.3.2.1.1. 自动获得一个 IP 地址

主机名：用来标识 WAN 接口，对应于 DHCP 协议里面的一个选项参数；

MAC 地址：通常在 ISP 要求锁定 MAC 的时候使用，目的是 ISP 分配给用户的 IP 地址与 WAN1 接口的 MAC 地址绑定，该 MAC 地址也可以通过**“候选”**来获得；

DNS：ISP 提供的域名服务器的 IP 地址，一般会在获得 IP 地址的同时获得域名服务器的 IP 地址，或者手工输入 ISP 提供的两个域名服务器的 IP 地址，一个作为首选，另一个为备用；

RIP：路由信息协议，一种动态路由选择协议，LAN 侧接口如果连接一路由器，那么

1. **禁用：**不发送路由更新信息，丢弃接收到路由器发出的更新信息；
2. **发送：**只发送路由更新信息，丢弃接收的路由更新信息；
3. **接收：**只接收路由更新信息，不发送路由更新信息；
4. **兼有：**接收同时发送路由更新信息；
5. **RIP-2B：**RIP-2 是指采用路由信息协议第二个版本，并以广播方式发送路由更新信息；
6. **RIP-2M：**以组播方式发送路由更新信息；

MTU：接口的最大传输单元，单位是字节，以太网接口的默认 MTU 是 1500，一般为了避免报文分片带来的问题，MTU 的值要求不能大于默认值 1500；

网络地址转换：报文从 WAN1 接口发送出去之前，对报文源 IP 地址和源端口号的处理；

1. **启用：**启用该功能；
2. **禁用：**禁用该功能；

3.2.3.2.1.2. 静态 IP 设置

IP 子网掩码：ISP 提供的子网掩码，与 IP 地址联合使用；

ISP 网关地址：ISP 提供的网关 IP 地址；

MAC 地址：通常在 ISP 要求锁定 MAC 的时候使用，目的是 ISP 分配给用户的 IP 地址与 WAN1 接口的 MAC 地址绑定，该 MAC 地址也可以通过“**候选**”来获得；

首选 DNS：首选域名服务器的 IP 地址，由 ISP 提供；

备用 DNS：备用域名服务器的 IP 地址，由 ISP 提供 ；

RIP：路由信息协议，一种动态路由选择协议，LAN 侧接口如果连接一路由器，那么

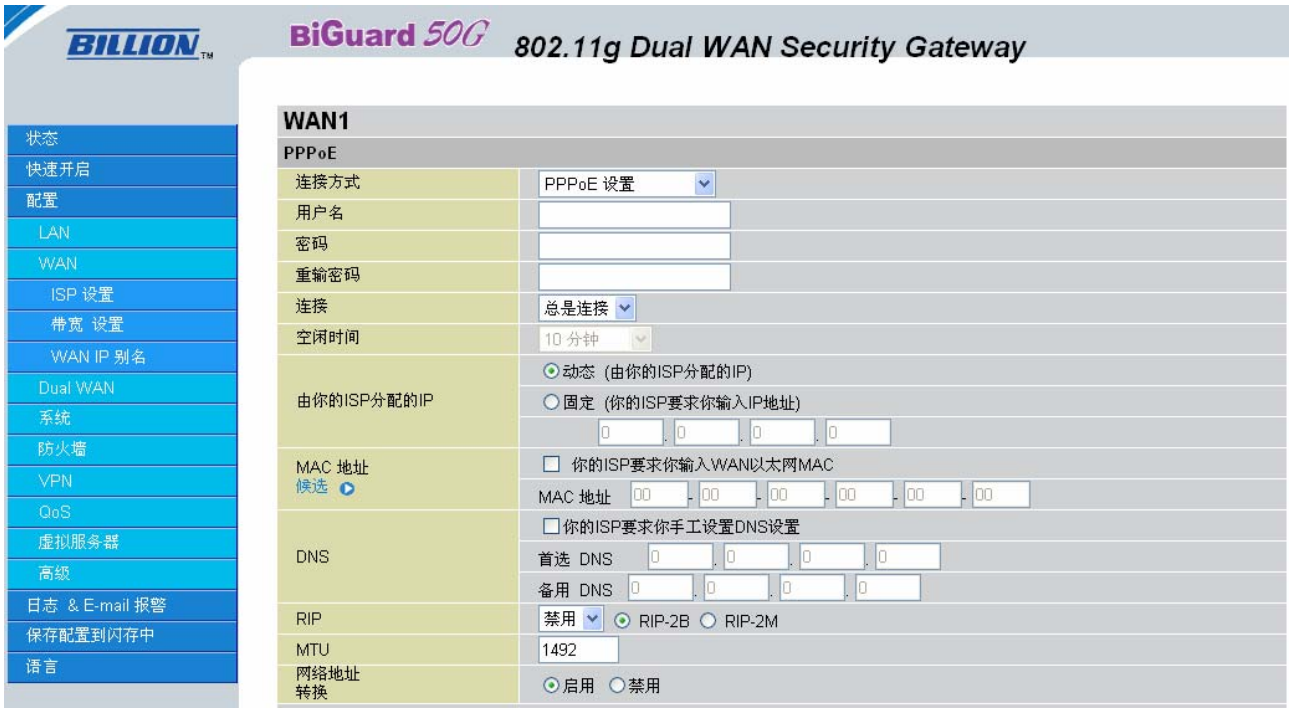
1. **禁用**：不发送路由更新信息，丢弃接收到路由器发出的更新信息；
2. **发送**：只发送路由更新信息，丢弃接收的路由更新信息；
3. **接收**：只接收路由更新信息，不发送路由更新信息；
4. **兼有**：接收同时发送路由更新信息；
5. **RIP-2B**：RIP-2 是指采用路由信息协议第二个版本，并以广播方式发送路由更新信息；
6. **RIP-2M**：以组播方式发送路由更新信息；

MTU：接口的最大传输单元，单位是字节，以太网接口的默认 MTU 是 1500，一般为了避免报文分片带来的问题，MTU 的值要求不能大于默认值 1500；

网络地址转换：报文从 WAN1 接口发送出去之前，对报文源 IP 地址和源端口号的处理；

1. **启用**：启用该功能；
2. **禁用**：禁用该功能；

3.2.3.2.1.3. PPPoE 设置



用户名：在申请 PPPoE 宽带服务时由 ISP 提供；

连接：PPPoE 的连接存在两种方式：

1. 总是连接：一旦 PPPoE 拨号成功，PPP 连接一直处于激活状态；

2. 按需触发：PPPoE 拨号成功后，如果 LAN 侧到 WAN 侧没有数据流过设备，那么在“**空闲时间**”指定的时间后，PPP 连接断开，当重新有数据流过时，PPPoE 重新拨号；

PPPoE 拨号有两种方式来获得 IP 地址：

动态：动态方式获得 IP 地址；

静态：ISP 提供的一个固定 IP 地址；

MAC 地址：通常在 ISP 要求锁定 MAC 的时候使用，目的是 ISP 分配给用户的 IP 地址与 WAN1 接口的 MAC 地址绑定，该 MAC 地址也可以通过“**候选**”来获得；

DNS：ISP 提供的域名服务器的 IP 地址，一般会在获得 IP 地址的同时获得域名服务器的 IP 地址，或者手工输入 ISP 提供的两个域名服务器的 IP 地址，一个作为首选，另一个为备用；

RIP：路由信息协议，一种动态路由选择协议，LAN 侧接口如果连接一路由器，那么

1. **禁用：**不发送路由更新信息，丢弃接收到路由器发出的更新信息；
2. **发送：**只发送路由更新信息，丢弃接收的路由更新信息；
3. **接收：**只接收路由更新信息，不发送路由更新信息；
4. **兼有：**接收同时发送路由更新信息；
5. **RIP-2B：**RIP-2 是指采用路由信息协议第二个版本，并以广播方式发送路由更新信

息；

6. RIP-2M：以组播方式发送路由更新信息；

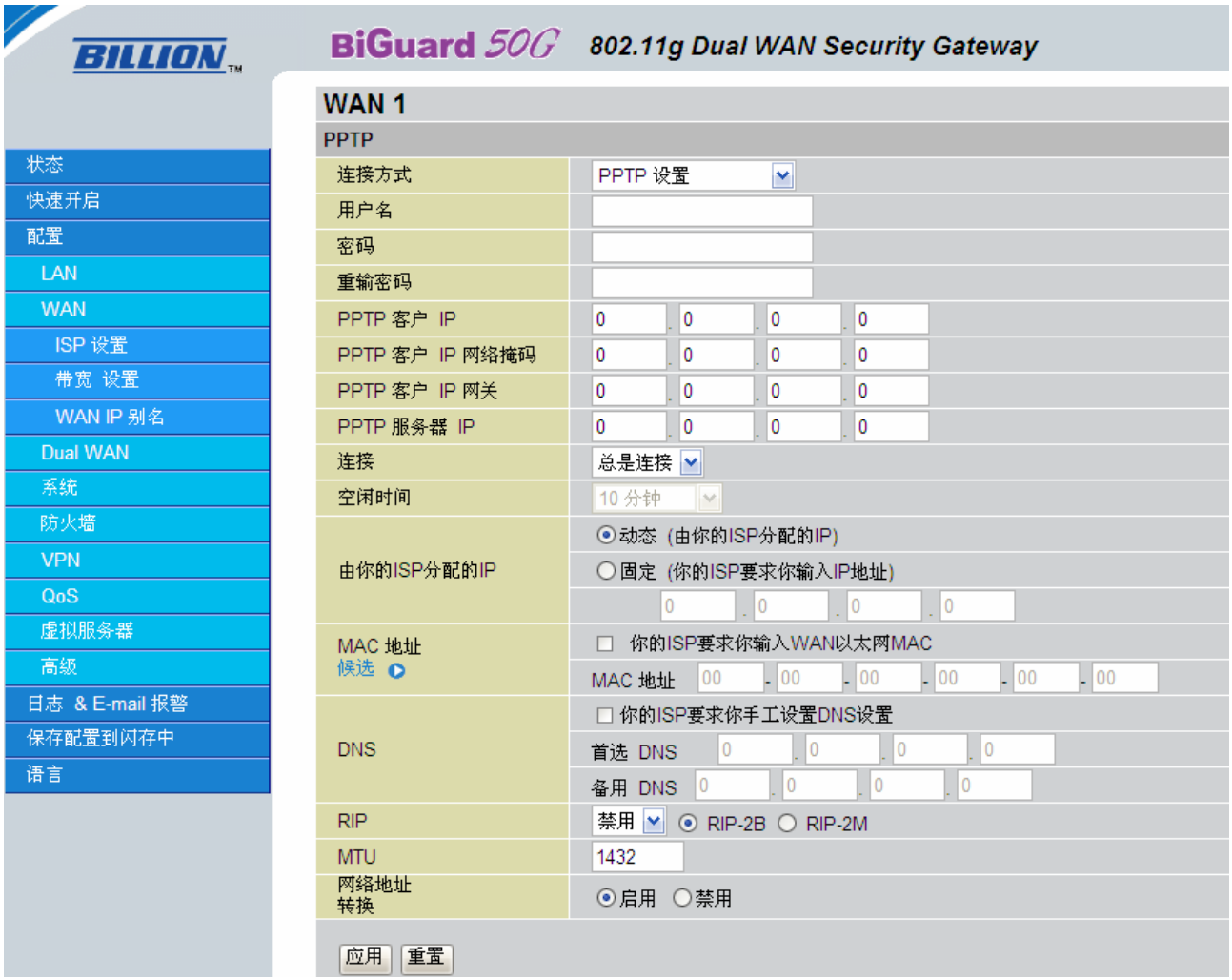
MTU：接口的最大传输单元，单位是字节，以太网接口的默认 MTU 是 1500，一般为了避免报文分片带来的问题，MTU 的值要求不能大于默认值 1500；

网络地址转换：报文从 WAN1 接口发送出去之前，对报文源 IP 地址和源端口号的处理；

1. 启用：启用该功能；

2. 禁用：禁用该功能；

3.2.3.2.1.4. PPTP 设置



用户名：在申请 PPTP 宽带服务时由 ISP 提供；

密码：一般由电话号码组成，也有其他情况；

PPTP 客户 IP：预先配置的 IP 地址，主要是为了能够连接 PPTP 服务器；

PPTP 客户 IP 网关：用于 PPTP 拨号请求的选路路径；

PPTP 服务器 IP：ISP 提供的 PPTP 服务器的 IP 地址；

PPTP 的连接存在两种方式：

1. **总是连接：**一旦 PPTP 拨号成功，PPP 连接一直处于激活状态，LAN 和 WAN 一直处于连通状态；
2. **按需触发：**PPTP 拨号成功后，如果 LAN 侧到 WAN 侧没有数据流过设备，那么在“**空闲时间**”指定的时间过后，PPP 连接断开，当重新有数据流过时，PPTP 重新拨号；

PPTP 拨号需要一个 IP 地址来与服务器建立连接，然后进行拨号建立 PPP 链路，有两种方式来获得 IP 地址：

1. **动态：**动态方式获得 IP 地址，；
2. **静态：**ISP 提供的一个固定 IP 地址；

MAC 地址：通常在 ISP 要求锁定 MAC 的时候使用，目的是 ISP 分配给用户的 IP 地址与 WAN1 接口的 MAC 地址绑定，该 MAC 地址也可以通过“**候选**”来获得；

DNS：ISP 提供的域名服务器的 IP 地址，一般会在获得 IP 地址的同时获得域名服务器的 IP 地址，或者手工输入 ISP 提供的两个域名服务器的 IP 地址，一个作为首选，另一个为备用；

RIP：路由信息协议，一种动态路由选择协议，LAN 侧接口如果连接一路由器，那么

1. **禁用：**不发送路由更新信息，丢弃接收到路由器发出的更新信息；
2. **发送：**只发送路由更新信息，丢弃接收的路由更新信息；
3. **接收：**只接收路由更新信息，不发送路由更新信息；
4. **兼有：**接收同时发送路由更新信息；
5. **RIP-2B：**RIP-2 是指采用路由信息协议第二个版本，并以广播方式发送路由更新信息；
6. **RIP-2M：**以组播方式发送路由更新信息；

MTU：接口的最大传输单元，单位是字节，以太网接口的默认 MTU 是 1500，一般为了避免报文分片带来的问题，MTU 的值要求不能大于默认值 1500；

网络地址转换：报文从 WAN1 接口发送出去之前，对报文源 IP 地址和源端口号的处理；

1. **启用：**启用该功能；
2. **禁用：**禁用该功能；

3.2.3.2.1.5. Big Pond 设置

Big Pond 拨号方式是澳大利亚特有的拨号方式。

用户名：在申请 PPPoE 宽带服务时由 ISP 提供；

密码：一般由电话号码组成，也有其他情况；

登录服务器：ISP 提供的登录服务器；

MAC 地址：通常在 ISP 要求锁定 MAC 的时候使用，目的是 ISP 分配给用户的 IP 地址与 WAN1 接口的 MAC 地址绑定，该 MAC 地址也可以通过“**候选**”来获得；

DNS：ISP 提供的域名服务器的 IP 地址，一般会在获得 IP 地址的同时获得域名服务器的 IP 地址，或者手工输入 ISP 提供的两个域名服务器的 IP 地址，一个作为首选，另一个为备用；

RIP：路由信息协议，一种动态路由选择协议，LAN 侧接口如果连接一路由器，那么

1. **禁用：**不发送路由更新信息，丢弃接收到路由器发出的更新信息；
2. **发送：**只发送路由更新信息，丢弃接收的路由更新信息；
3. **接收：**只接收路由更新信息，不发送路由更新信息；
4. **兼有：**接收同时发送路由更新信息；
5. **RIP-2B：**RIP-2 是指采用路由信息协议第二个版本，并以广播方式发送路由更新信息；
6. **RIP-2M：**以组播方式发送路由更新信息；

MTU：接口的最大传输单元，单位是字节，以太网接口的默认 MTU 是 1500，一般为了避免报文分片带来的问题，MTU 的值要求不能大于默认值 1500；

网络地址转换：报文从 WAN1 接口发送出去之前，对报文源 IP 地址和源端口号的处理；

1. **启用：**启用该功能；
2. **禁用：**禁用该功能；

3.2.3.2.2. 带宽设置

WAN1：WAN1 接口，百兆以太网接口，带宽配置如下：

1. 出站带宽：数据从 WAN1 接口出去时的总带宽，一般称为上行带宽；
2. 入站带宽：数据从 WAN1 接口进来时的总带宽，一般称为下行带宽；

WAN2：WAN2 接口，百兆以太网接口，带宽配置如下：

1. 出站带宽：数据从 WAN1 接口出去时的总带宽，一般称为上行带宽；
2. 入站带宽：数据从 WAN1 接口进来时的总带宽，一般称为下行带宽；

配置接口总带宽的时候要注意：

1. **QoS 的各队列带宽之和由上行或者下行总带宽决定；**
2. **负载均衡的吞吐量要受上行或者下行总带宽限制；**

3.2.3.2.3. WAN IP 别名

WAN IP 别名配置为 WAN1 接口和 WAN2 接口提供好记的名称。

名称：WAN1 接口或者 WAN2 接口的别名；
IP 地址：WAN1 接口或者 WAN2 接口 IP 地址；
接口：指定该 IP 地址是 WAN1 接口的还是 WAN2 接口的；

3.2.3.3. Dual WAN

这个部分的配置前提是 WAN1 和 WAN2 接口都已经配置好连接，都能够把 LAN 侧的数据转发出去，那么可以对 WAN1 和 WAN2 做**负载均衡**、**失效切换（链路备份）**，以及**协议绑定（策略路由）**的一些配置。

3.2.3.3.1. 一般设置

基本配置决定了 WAN1 和 WAN2 是应用于**负载均衡**还是**失效切换**。

WAN 接口启用**负载均衡**或者**失效切换**时，会需要进行一些配置，来检测 WAN1 和 WAN2 是否是有效的出接口；

两种模式：

1. **负载均衡**：对于从 WAN1 和 WAN2 接口发送出去的数据做流量分配；
2. **失效切换**：又称为**链路备份**，当 WAN1 接口失效后，报文被切换到从 WAN2 接口出去；

服务侦测：WAN 接口有效性检测，可以提前获得数据链路的状态，以此来避免报文的丢弃；当模式选择为**失效切换**的时候，有效性检测总是开启；只有在模式选择**负载均衡**的时候才会出现下面的配置：

1. **启用：**检测两个 WAN 接口的有效性；
2. **禁用：**不检测两个 WAN 接口的有效性；

有效性检测是通过配置连接性决策和检测周期来协同工作的：

连接决策：通过设置连接尝试的次数来决定 WAN 接口的状态，以便做 WAN1 和 WAN2 的切换；

探测周期：每个周期都会进行连接尝试；

探测 WAN1：检测 WAN1 接口的数据链路状态，连接性检测的方式是通过设备内置的 ping 服务来进行的；

1. 网关：通过 ping WAN1 接口的网关来做连接性检测；
2. 主机：通过 ping WAN1 接口侧的某个主机来做连接性检测；

探测 WAN2：检测 WAN2 接口的数据链路状态，连接性检测的方式是通过设备内置的 ping 服务来进行的；

1. **网关**：通过 ping WAN2 接口的网关来做连接性检测；
2. **主机**：通过 ping WAN2 接口侧的某个主机来做连接性检测；

回切到 WAN1：这个参数只有在 WAN 模式为**失效切换**时才有效；

1. **启用**：当 WAN1 接口恢复到有效状态后，报文被切换到从 WAN1 接口发送出去；
2. **禁用**：当 WAN1 接口恢复到有效状态后，报文依然从 WAN2 接口发送出去；

3.2.3.3.2. 出站负载均衡

对从 WAN1 和 WAN2 接口出去的数据做负载均衡，主要是利用路由器多路径的优点，在可以利用的路径上发送报文，常用的负载均衡方式是：**基于连接**和**基于 IP 地址**；

基于连接机制：通常会用一个四元组来表示一个连接[源 IP、源端口、目的 IP、目的端口]，具体分为下面五种策略；

1. **由连接平衡（交替策略）**：从 WAN1 和 WAN2 接口交替的出去连接，并且连接数基本持平，如果 WAN2 接口出去的连接较少，后续的连接会从 WAN2 出去，以维持平衡状态；
2. **由连接平衡（链路容量权重）**：受 WAN 接口设定的带宽所限制，比如说 WAN1 接口带宽设置为 102400Kbps，WAN2 接口带宽设置为 51200Kbps，那么从 WAN1 和 WAN2 发送出去的连接数为维持在 1：2，也就是说从前一个连

接的报文从 WAN1 发送出去，后面的两个连接的报文从 WAN2 发送出去；

3. **比重分配策略：**设置从 WAN1 和 WAN2 出去的连接的百分比；
4. **由流量平衡（链路容量权重）：**这种策略也会受 WAN 接口设定的带宽所限制，假定 WAN1 和 WAN2 的带宽设置一样，某个时刻 WAN1 和 WAN2 的连接数比为 3：1，那么后续的连接都会从 WAN2 出去，直到 WAN1 和 WANA2 的连接数接近相同；
5. **由流量权重平衡：**这种策略可以由用户指定 WAN1 和 WAN2 的连接数比例，假定用户指定 WAN1 和 WAN2 的比重分配为 2：3，那么在 WAN1 和 WAN2 出去的连接数比就为 2：3；

基于 IP 地址散列机制：这种机制使用一个二元组[源 IP、目的 IP]来标识连接双方，可以看出这种机制比基于连接的机制要粗放；

1. **由链接容量权重平衡：**这种策略会受 WAN 接口设定的带宽所限制，假定 WAN1 和 WAN2 的带宽设置一样，某个时刻 WAN1 和 WAN2 的去往目的网络的流量比 3：1，那么后续的流量都会从 WAN2 出去，直到 WAN1 和 WAN2 的流量接近相同；
2. **由权重平衡：**这种策略可以由用户指定 WAN1 和 WAN2 的流量比例，假定用户指定 WAN1 和 WAN2 的比重分配为 2：3，那么在 WAN1 和 WAN2 出去的流量比就为 2：3；

3.2.3.3.3. 入站负载均衡

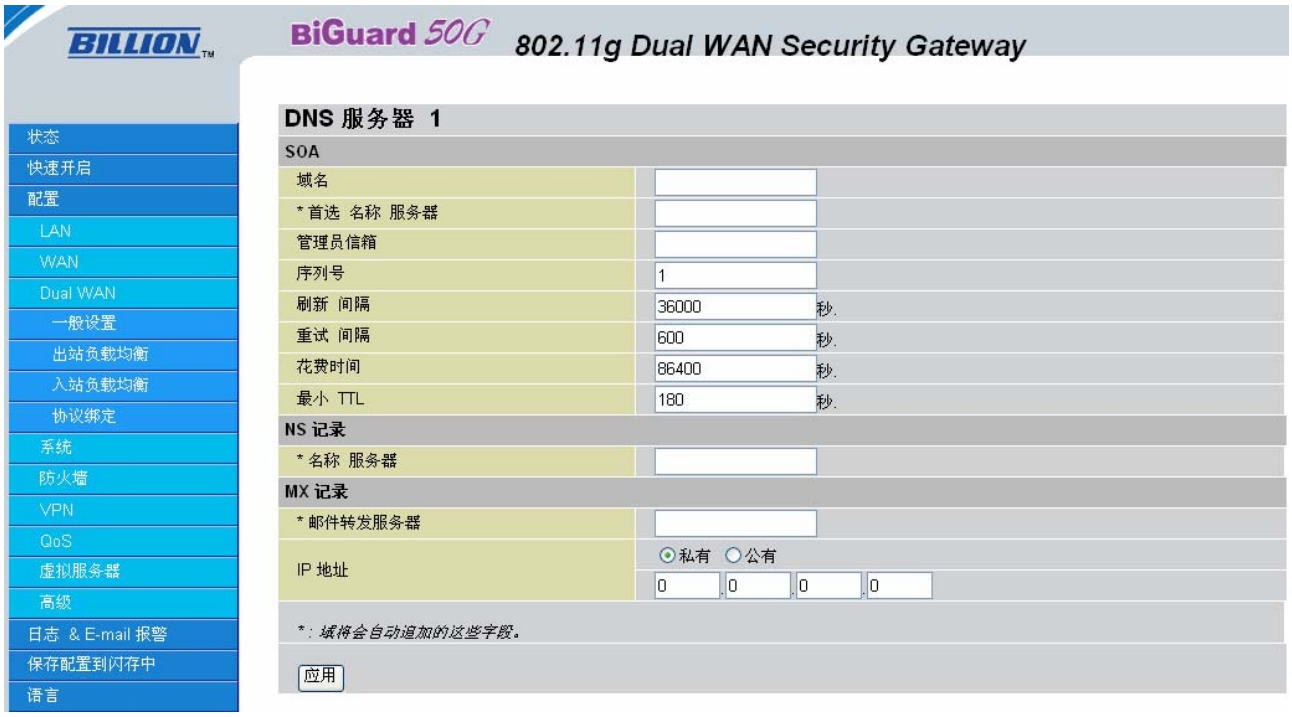
当企业在内部搭建一些服务器，例如 Web 服务器、FTP 服务器等等，提供给 Internet 用户访问。Internet 用户可以通过访问某个域名来访问这些服务器，那这个部分的配置可以让一部分服务器的流量从 WAN1 出去，其他一部分服务器流量可以去 WAN2 出去，实现流量分流；

3.2.3.3.3.1. DNS 服务器

DNS 服务器主要用来为企业内部服务器做域名解析。

服务器设置：每个 DNS 服务器都会建立一个授权资源记录，在这个资源记录里面需要配置该服务器管理的域名，上级域名服务器，邮件服务器等信息；

点击服务器设置后面的“**编辑**”进入 DNS 服务器的配置页面：



域名：首先该域名需要向 ISP 申请，假定 ISP 的域名为 xxx.cn，那么申请的域名大概为

yyy.xxx.cn，就是说需要成为 ISP 域的一个子域，这样做的目的是 Internet 用户可以向 ISP 的 DNS 服务器请求域名解析，进而向该 DNS 服务器请求主机域名解析；
首选名称服务器：配置为自己的主机名称，例如 ns1；
管理员信箱：例如 admin@company.cn；
序列号：或者说版本号，每次修改 DNS 服务器上的记录时，序列号都要增加 1；
刷新间隔：该参数是告诉辅 DNS 服务器经过多久向主 DNS 服务器请求 DNS 记录列表，来更新辅 DNS 服务器上面的 DNS 记录；
重试间隔：该参数是告诉辅 DNS 服务器在第一次请求 DNS 记录列表未得到响应后，继续尝试请求的等待时间；
花费时间：该参数是告诉辅 DNS 服务器，经过多久 DNS 记录就变得不可用；
最小 TTL：最小存活时间，一般以秒表示；
名称服务器：指明谁是 yyy.xxx.cn 域的域名解析服务器，这里一般填写自己,例如:ns1.yyy.xxx.cn；
邮件转发服务器：为企业用户转发邮件,这里可以填写 IP 地址或者域名；
IP 地址：指定邮件转发服务器的 IP 地址为企业内部网络的还是公网上的，

1. **私有：**企业内部网络使用的 IP 地址；
2. **公有：**公网使用的 IP 地址；

3.2.3.3.3.2. 主机 URL 映射

主机 URL 映射是为了给企业内部的 Web 或者 FTP 服务器指定一个域名，同时配置服务器为虚拟服务器，虚拟服务器通常是指那些放在企业内部网络里面的服务器，但能提供给 Internet 用户访问；
点击“**主机 URL 映射**”后面的“**编辑**”进入域名与 IP 地址映射配置界面：

域名：DNS 服务器所提供的主域；
主机 URL：主机名称+主域名称，就成为 Internet 用户访问该服务器的 URL 地址；
私有 IP 地址：企业内部分配给该服务器的 IP 地址，也可以通过“**候选**”选择；
协议：该服务器所提供的应用所对应的协议，有以下 3 种：

1. **Any**：任意的协议，不对协议做特别指定；
2. **TCP**：TCP 协议的应用；
3. **UDP**：UDP 协议的应用；

端口范围：应用协议的端口号，也可以通过“**助手**”来选择；
记录名：主机名称的别名，主机名称假定为 www，那么可以为主机名称提供最多两个别名，假定别名 1 是 webserver1，别名 2 是 webserver2；

3.2.3.3.4. 协议绑定

协议绑定类似于高端路由器上的策略路由功能，用户可以指定哪些协议的报文从 WAN1 接口发送出去，哪些从 WAN2 接口发送出去；

点击“**创建**”进入规则的配置页面：

接口：选择该规则的报文是从 WAN1 发送出去还是 WAN2 发送出去；
源 IP 的范围：可以有两种配置方式：

1. **所有源 IP：**就是不限制源 IP 地址；
2. **指定源 IP：**就是指定某个 IP 地址或者 IP 地址范围；

目的 IP 地址范围：可以有两种配置方式：

1. **所有目的 IP：**就是不限制目的 IP 地址；
2. **指定目的 IP：**就是指定某个 IP 地址或者 IP 地址范围；

协议：有以下几个选项：

1. **任何**协议；
2. **TCP** 协议；
3. **UDP** 协议；

端口范围：也可以通过“**助手**”来选择；
请注意：协议绑定的优先级别比路由要高，也就是说报文做路由选择时先去查找协议绑定规则，没有匹配上时才去查找路由表；

3.2.3.4. 系统

系统配置包括系统时间配置、远程访问控制、版本更新、配置文件备份及恢复、系统重启、管理员密码修改等功能。

3.2.3.4.1. 时区

系统时间配置，能够为日志提供精确的事件发生时间。

时区：是否需要启用网络时间服务来同步系统时间；

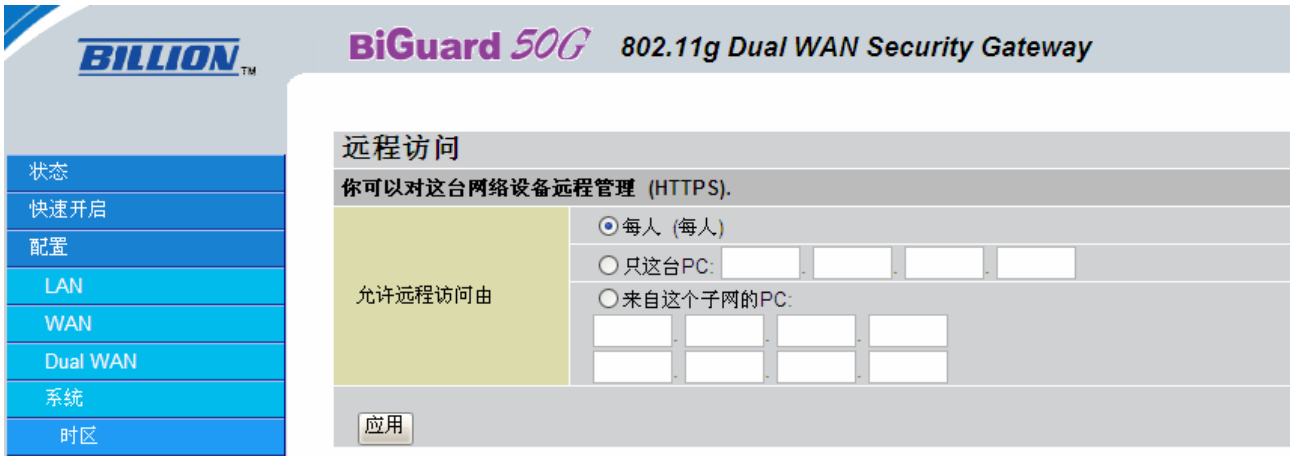
① **启用：**启用该功能，一般推荐启用该功能；
② **禁用：**禁用该功能；

本地时区：中国的时区为东八区；
NTP 服务器地址：指定时间服务器，以便设备系统时间与此同步，时间服务器可以选择 Internet 上面的服务器，也可以是企业内部自己的时间服务器；

3.2.3.4.2. 远程访问

控制对设备进行 web 页面的远程访问。

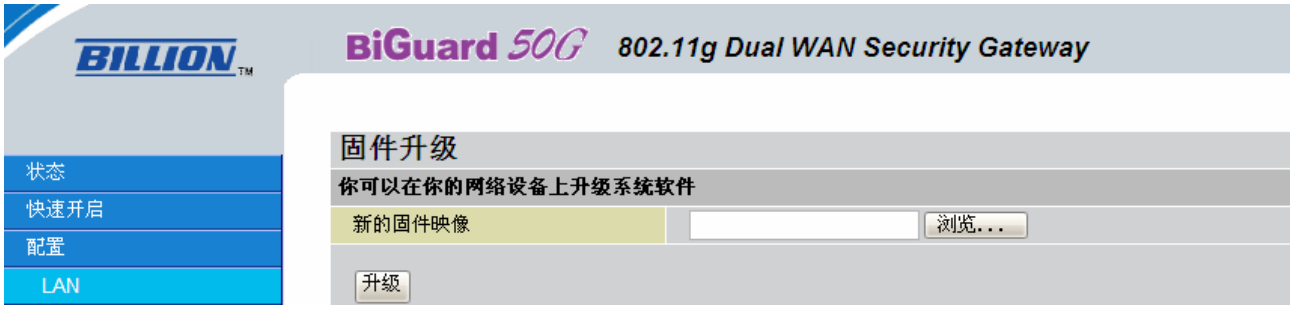
动作：是否启用远程访问控制功能，
① **启用：**允许远程访问，通过 HTTPS 的方式进行访问；
② **禁用：**不允许远程访问；
HTTPS 端口：HTTPS 方式访问设备所使用的端口号;
请注意端口号的修改需要重启系统才能生效；
远程访问表：允许远程访问的主机，点击“**创建**”进入配置界面：



远程访问由：允许远程访问的主机可以通过下面 3 种方式来配置，
① **每人：**任意主机都可以远程访问；
② **只这台 PC：**指定某个主机才可以远程访问；
③ **来自这个子网的 PC：**指定某个网段的主机可以远程访问；

3.2.3.4.3. 固件升级

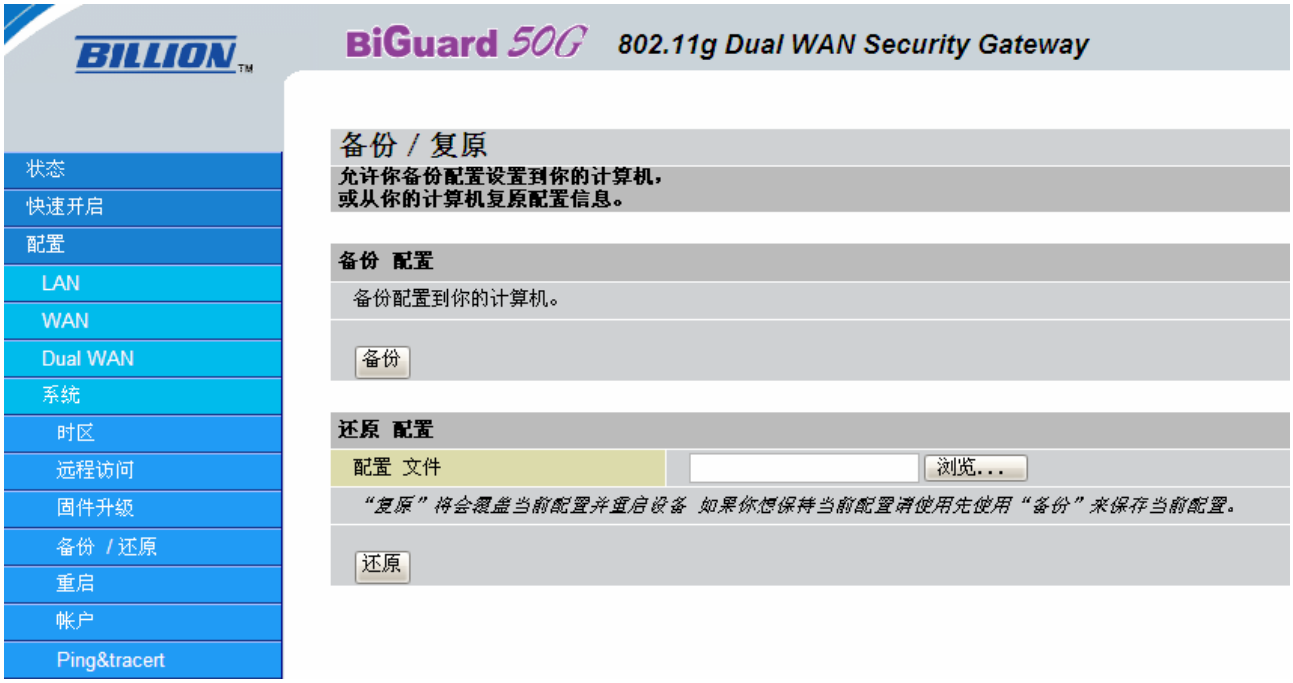
版本更新配置界面：



新的固件映像：选择新的版本文件的路径；
升级：点击“**升级**”，进行版本文件的上传，系统会自动重启并且加载新的文件系统；

3.2.3.4.4. 备份/复原

可以把配置文件保存到某个主机或者是服务器上面，以便以后配置出现问题或者版本更新时，重新导入配置文件，大大减少了配置和管理的复杂程度；



备份配置：把设备上面的配置文件保存到某个主机或者服务器上面；
还原配置：把主机或者服务器上面的配置文件导入，设备会自动重启并启用配置文件的配置；

3.2.3.4.5. 重启

重新启动设备，可以通过设备上面的硬件开关来控制，也可以通过这里的软件方式来控制。

重启路由器使用：重启设备后加载的配置可以是：

① **当前设置；**

② **出厂设置：**出厂时的默认配置，通常会在配置出现问题而又不清楚具体是由哪些配置引起，那么可以尝试出厂配置来使设备正常运行；

3.2.3.4.6. 账户

管理员增加账户和密码的修改页面。

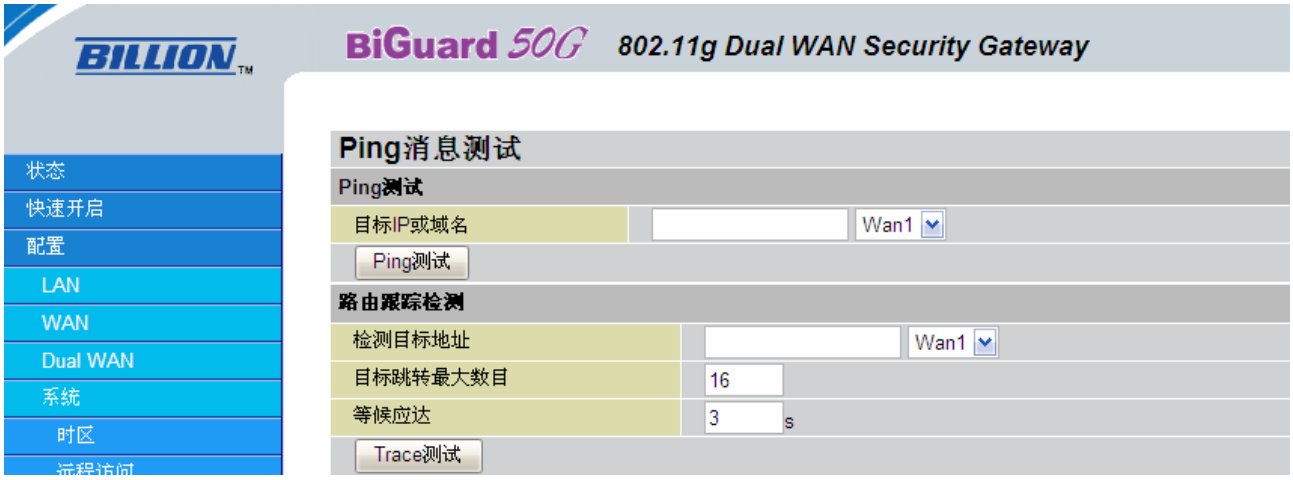
账户：输入用户名。
确认账户：再次输入确认账户名。
密码：新的密码，请注意最大输入的字符数是 32 个字符；；
确认密码：确认新的密码；
应用：应用新的密码；
重置：清空输入的密码，以便重新输入；

3.2.3.4.7. Ping&tracert

用户可以通过该功能对现有网络进行诊断。点击 Ping&Tracert 打开 Ping 消息测试界面。可以选择以下两种诊断方式：

Ping 测试：用 Ping 工具可以测试网络是否连接及网络延时，相当于操作系统中的 Ping 命令。

路由跟踪检测：用 Trace 工具可以检测路由的状况，相当于操作系统中的 Tracert 或 Traceroute 命令。



Ping 测试：输入 Ping 测试的目标 IP 地址或 DNS 名，然后选择数据包出站接口,WAN1 或 WAN2，点击 Ping 测试就可以进行测试。

路由跟踪检测：输入检测的目标地址，然后选择数据包出站的接口，WAN1 或 WAN2，选择路由最大跳数和等候应答时间，然后点击 Trace 测试就可以进行测试。

3.2.3.5. 防火墙

防火墙，用来控制企业内部与外部的通信，提高计算机的安全性。我们的防火墙将限制从一些计算机发送另一些到计算机上的信息，这使得企业内部可以更好地控制内部的数据，并针对那些未经邀请而尝试连接到您的计算机的用户或程序提供了一条防御线。防火墙也被认为是一道屏障，它检查来自 Internet 或网络的通信信息，然后根据防火墙设置，拒绝信息或允许信息到达企业的内部网络。

3.2.3.5.1. IM 过滤

IM 过滤可以根据计划分时段禁止使用 IM 软件。

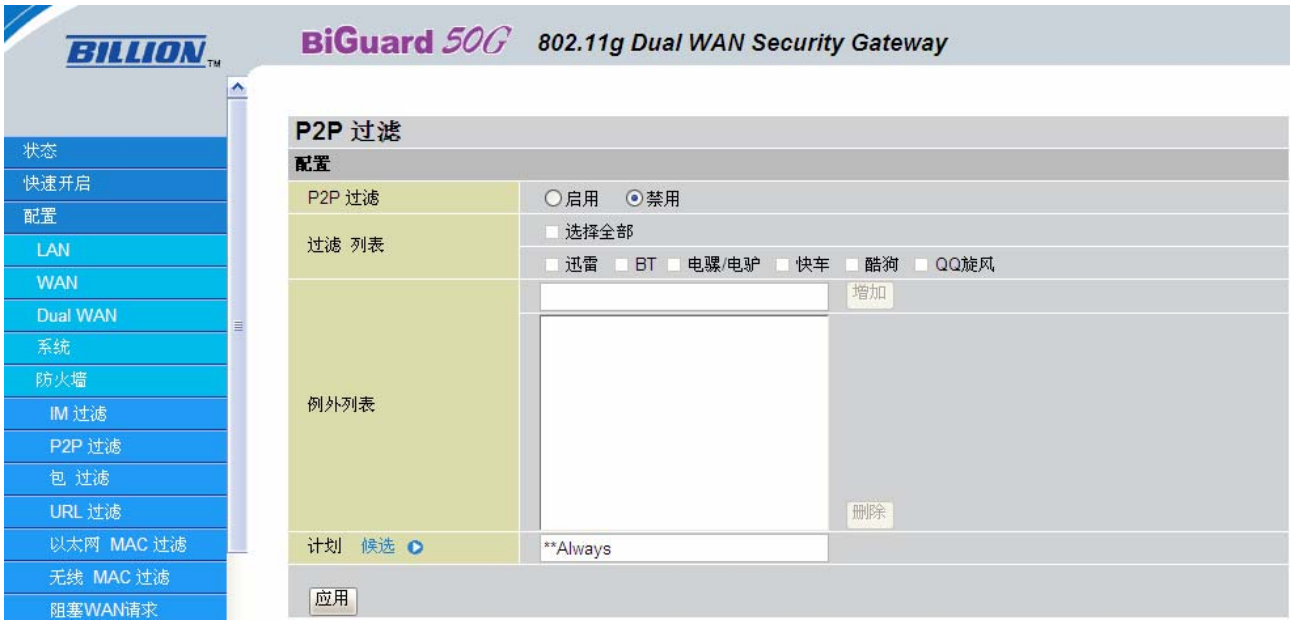
IM 过滤：启用或禁用 IM 过滤功能。
过滤列表：选择需要过滤的 IM 软件。
例外列表：输入例外的 IP 地址，点击**增加**，例外的 IP 允许使用 IM 软件软件。
计划：过滤 IM 软件的时间。
点击**候选**，选择时间

名称	一星期中哪天	时间	
○	**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00

候选中的时间设置可在**配置—高级—计划**中设置。

3.2.3.5.2. P2P 过滤

P2P 过滤可以根据计划分时段禁止使用 P2P 软件。



P2P 过滤：启用或禁用 P2P 过滤功能。
过滤列表：选择需要过滤的 P2P 软件。
例外列表：输入例外的 IP 地址，点击**增加**，例外的 IP 允许使用 P2P 软件软件。
计划：过滤 P2P 软件的时间。
点击**候选**，选择时间

名称	一星期中哪天	时间	
○	**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00

候选中的时间设置可在**配置—高级—计划**中设置。

3.2.3.5.3. 包过滤

包过滤，方向可以是从企业内部网络到外部网络，或者是外部网络到内部网络；

包过滤表：报文过滤规则列表；
ID：序号或者说标识号；
启用：规则是否启用的开关；
动作：对于匹配规则的报文所做的处理，丢弃还是发送；
方向：报文从企业内部到外部，或者外部到企业内部；

点击“**创建**”，进入规则具体的配置页面：

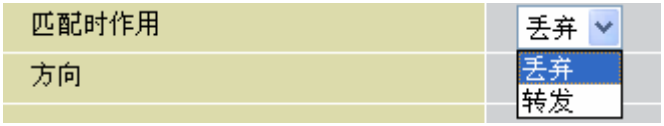
ID：标识该规则；

策略：规则的启用或者禁用开关；

① **启用**：启用该规则；

② **禁用**：禁用该规则，也就是该规则不生效；

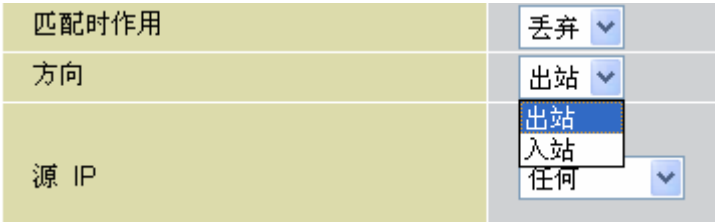
匹配时作用：对匹配该规则的报文如下处理：



① **丢弃**；

② **发送**；

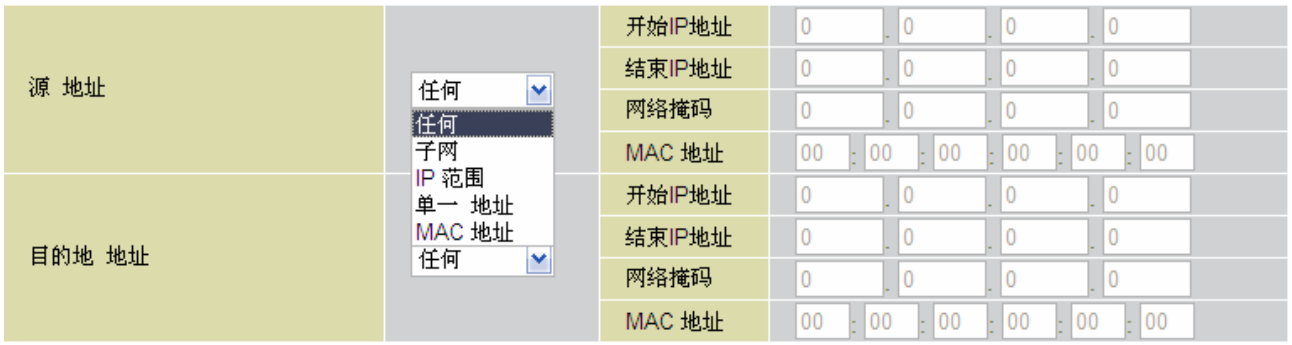
方向：有如下两个方向；



① **出站**：从 LAN 侧到 WAN 侧的报文做规则匹配；

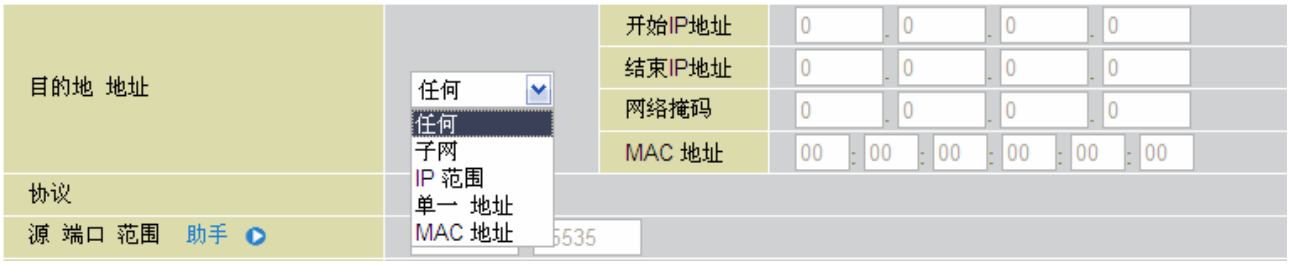
② **入站**：从 WAN 侧到 LAN 侧的方向做规则匹配；

源地址：对于源地址的指定有如下 5 种方式：



① **任何：**不特别指定 IP 地址，可以是任意的 IP 地址；
② **子网：**IP 地址为一个子网的 IP 地址范围，包括该子网所有的可用 IP 地址；
③ **IP 范围：**IP 地址为某个子网的一段 IP 地址，只是一部分可用 IP 地址；
④ **单一地址：**特定的某个 IP 地址；

目的地地址：对于目的地址的指定也有如下 5 种方式：



① **任何：**不特别指定 IP 地址，可以是任意的 IP 地址；
② **子网：**IP 地址为一个子网的 IP 地址范围，包括该子网所有的可用 IP 地址；
③ **IP 范围：**IP 地址为某个子网的一段 IP 地址，只是一部 IP 地址；
④ **单一地址：**特定的某个 IP 地址；

协议：规则所指定的协议，有以下 4 种：

① **任何：**任意的协议，不对协议做特别指定；
② **TCP：**指定报文为 TCP 协议的报文；
③ **UDP：**指定报文为 UDP 协议的报文；

源端口范围：以上所指定的协议所对应的源端口号，如果上面的协议选择为“**任何**”，则该参数不用指定，也可以通过“**助手**”来选择；

目的地端口范围：协议所对应的目的端口号，如果上面的协议选择为“**任何**”，则该参数不用指定，也可以通过“**助手**”来选择；

匹配时作用	应用	协议	端口号	
方向	Any-TCP	TCP	1~65535	
源 地址	Any-UDP	UDP	1~65535	0 . 0 . 0
	FTP	TCP	20~21	0 . 0 . 0
	SSH	TCP	22	0 . 0 . 0
	TELNET	TCP	23	: 00 : 00 : 00 : 00
目的地 地址	SMTP	TCP	25	0 . 0 . 0
	DNS	UDP	53	0 . 0 . 0
	HTTP	TCP	80	0 . 0 . 0
	POP3	TCP	110	: 00 : 00 : 00 : 00
协议	NTP	UDP	123	
源 端口 范围 助手	SNMP	UDP	161	
目的地 端口 范围 助手	HTTPS	TCP	443	
计划 候选	IKE	UDP	500	
日志	syslog	UDP	514	

计划：计划时间表，可以为该规则做个时间控制，规定某个时段该规则对报文处理，通过“**候选**”来选择已经配置好的计划时间表：

日志：是否在日志里面记录该事件，

① **启用：**记录该事件；

② **禁用：**禁用该事件；

3.2.3.5.4. URL 过滤

URL 过滤，控制对 Internet 的访问。过滤的方式有：通过关键字过滤 URL、通过域名过滤 URL、还可以过滤一些控件程序；

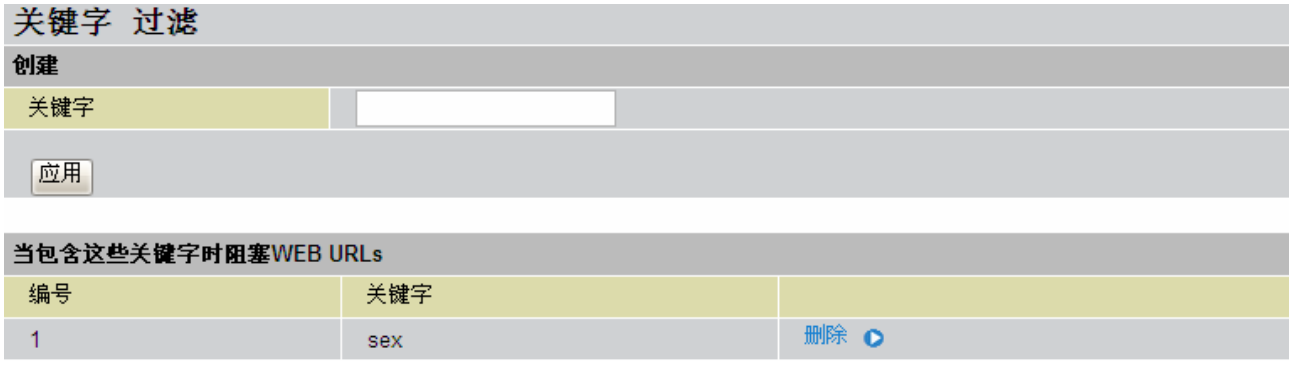
URL 过滤：URL 过滤开关，控制 URL 过滤是否生效：

① **启用**：URL 过滤功能启用；

② **禁用**：URL 过滤功能禁用；

关键字过滤：通过关键字过滤来过滤 URL 的访问，

点击“**细节**”，进入关键字配置界面：



关键字：可以是字母也可以是数字，可以是字母和数字的组合；

域名过滤：通过域名来过滤 URL 访问，有两种方式来配置：

启用：启用域名过滤，具体配置点击“**细节**”进入域名配置界面：

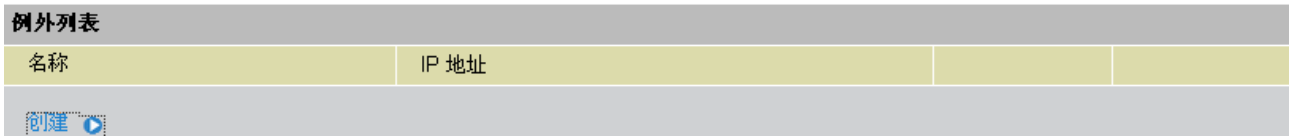
域名：完整的域名；
类型：对于上面的域名做如下处理方式：

① **禁止的域名：**就是被过滤掉的域名；
② **信任的域名：**就是没有被过滤掉可以访问的域名；

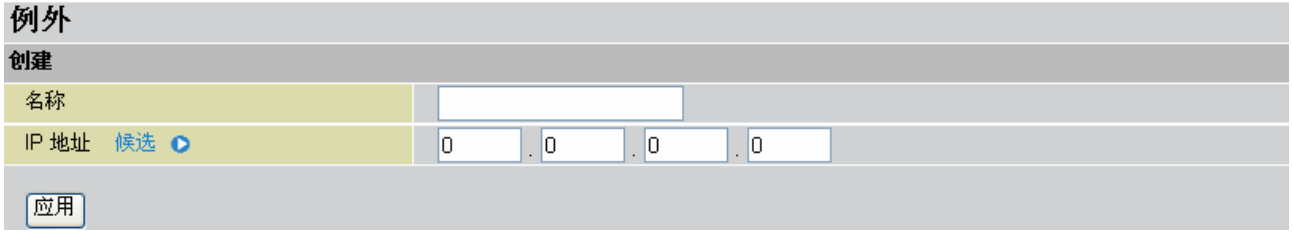
禁止访问信任域名以外的域名：除了信任的域名外，访问其他所有域名的报文都将被过滤掉；
限制 URL 特性：比如说一些控件程序，有以下几种：

① **阻塞 java Applet；**
② **阻塞 ActiveX；**
③ **阻塞 web 代理；**
④ **阻塞 cookie；**
⑤ **用 IP 地址阻塞上网；**

日志：是否把 URL 过滤事件记录到日志中去；
启用：启用该功能；
以上都是过滤配置，当然还是需要让企业内部一些人能访问 Internet。
例外列表：通过列表来规划例外的主机，这个列表中的主机表示可以访问 Internet；



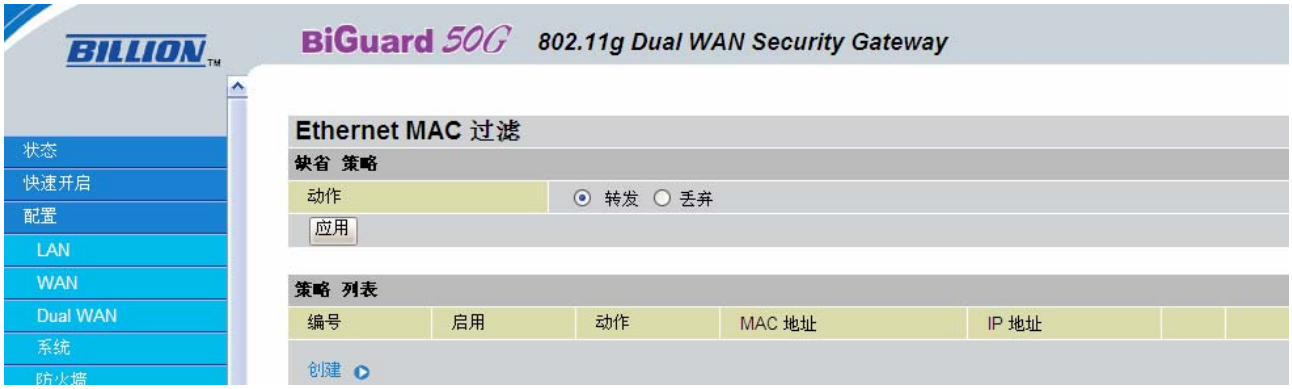
名称：规则名称；
IP 地址：主机的 IP 地址；
点击“**创建**”进入允许访问 Internet 的主机的配置界面：



名称：规则名称，可以用来表示某个用户，例如：“小明”；
IP 地址：主机的 IP 地址，或者使用“**候选**”中的的主机：

3.2.3.5.5. 以太网 MAC 过滤

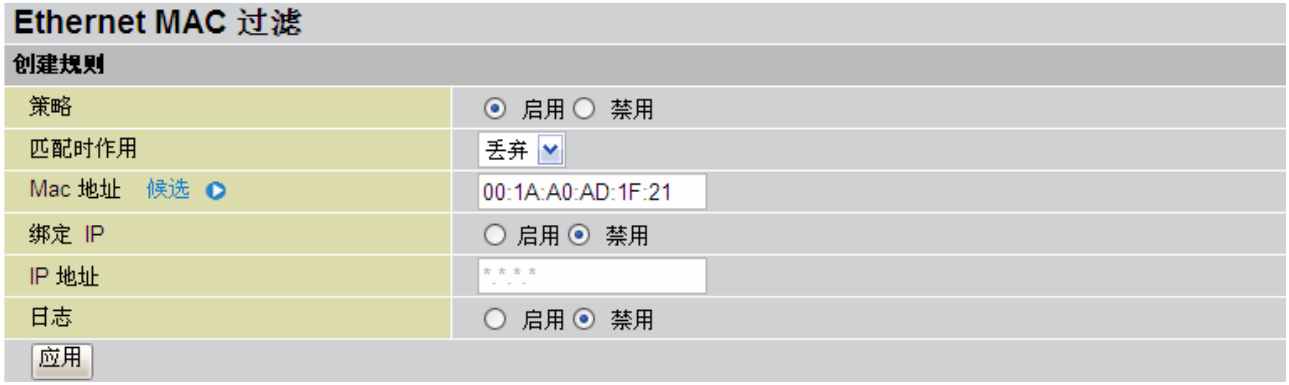
MAC 过滤是一种简单而有效的过滤方式，和包过滤和 URL 过滤相比较，它只需要稍微配置，就可以起到过滤的效果；



缺省策略：当报文不能匹配新建规则时才去匹配默认规则，那么默认规则对报文的处理方式有下面 2 种，

① **转发：**通常都会是这种方式；
② **丢弃：**那么 LAN 侧的主机发送的报文有可能都被丢弃掉；

策略列表：新建的规则列表，部分参数如下：
启用：该规则是否被启用；
动作：该规则对报文的处理方式，丢弃或者发送；
MAC 地址：报文发送端的 MAC 地址；
点击“**创建**”，进入规则配置界面：



策略：规则是否被启用；

① **启用：**规则被启用；
② **禁用：**规则被禁用，即不生效；

匹配时作用：当报文匹配规则时所做的处理，方式如下；

① **丢弃**；

② **转发**；

Mac 地址：LAN 侧主机的 Mac 地址，形式如：11：22：33：44：55：66；

也可以通过点击“**候选**”进入侯选列表来选择：

日志：可以把 MAC 地址过滤事件记录到日志中，

① **启用：**记录该规则的过滤事件；

② **禁用：**不记录该规则的过滤事件；

3.2.3.5.6. 无线 MAC 过滤

动作：转发或者丢弃；
规则列表：新建的规则列表，部分参数如下：
启用：该规则是否被启用；
动作：该规则对报文的处理方式，丢弃或者发送；
MAC 地址：报文发送端的 MAC 地址；
点击“**创建**”，进入规则配置界面：

创建无线 MAC 过滤规则；

3.2.3.5.7. 阻塞 WAN 请求

阻止 WAN 侧的访问请求，主要是防止 ping 攻击。

阻塞 WAN 请求：

① **启用**：启用该功能，可以有效的阻止 WAN 侧的 ping 攻击；

② **禁用**：禁用该功能，但有可能受到 WAN 侧的 ping 攻击；

阻塞 WAN ICMP 请求：

③ **启用**：启用该功能。

④ **禁用**：禁用该功能。

3.2.3.5.8. 入侵侦测

入侵侦测主要用来防御黑客攻击。

入侵侦测：

① **启用**：启用该功能，能够有效防御一些黑客攻击；

② **禁用**：禁用该功能；

入侵日志：

① **启用**：写入日志；

② **禁用**：不写入日志；

ARP 保护：防御 ARP 攻击，

① **启用**：启用该功能；

② **禁用**：禁用该功能；

连接限制：对连接做一些数量上的限制，

① **无限制**：连接数量没有限制；

② **限制每个 IP 连接最大到**：限制每个 IP 地址发起的连接的最大数量，当达到最大数量的时候，后续的连接报文都丢弃；

③ **限制每个 IP 连接最大到**：限制每个 IP 地址发起的连接的最大数量，当达到最大数量的时候，可以通过下面两种策略来有选择的限制连接数量，

- **拒绝来自这个 IP 新的连接**：该 IP 的连接数达到限制值时，需要等待一段时间後才允許建立新的连接；
- **丢弃来自这个 IP 的所有包**：该 IP 的连接数达到限制值时，在一段时间内将会丢弃所有从该 IP 来的报文；

3.2.3.5.9. ALG 开关

ALG，也叫做应用层网关（Application Layer Gateway），是由一个扩增防火墙或计算机网络应用或 NAT 的安全部件组成的一类防火墙。它允许合法应用数据通过防火墙的安全检测，另外将严格限制不符合它的有限过滤标准的运输流。

控制是否启用或关闭应用层上的各个协议。

例如，SIP ALG:

启用：SIP 协议可以通过应用层网关。

禁用：SIP 协议无法通过应用层网关。

3.2.3.6. VPN

VPN 技术保证了 VPN 中任何一对主机之间的通信对于外来者都是隐藏的，这主要得益于通道传输技术和加密技术。BiGuard 50G 支持两种 VPN 技术：IPsec 和 PPTP。

3.2.3.6.1. IPSec

IPsec 是由 IETF 设计的一套提供 IP 安全通信的协议集来实现的，IPsec 采用了如下信息安全的防护措施：

数据完整性：系统保护信息不被未授权的用户改变；
数据保密性：数据即使被中间人获得，也不能明白数据的内容；
鉴别：两个通信实体能互相鉴别对方的身份；

BiGuard 50G 为企业总部和分部之间的安全通信提供了有力的保障，最多可以保证 50 条安全通道同时工作，并且数据的带宽仍可以达到 30Mbps；

3.2.3.6.1.1. IPSec 向导

IPsec 的向导部分指导用户进行一些简单的配置就可以实现 IPsec VPN 的建立。

连接名称：用来标识该规则；
接口：配置 IPsec 规则的接口，

1. **WAN1：**WAN1 接口上面配置 IPsec 规则；
2. **WAN2：**WAN2 接口上面配置 IPsec 规则；
3. **自动：**系统自动指定在哪个接口上面配置 IPsec 规则；

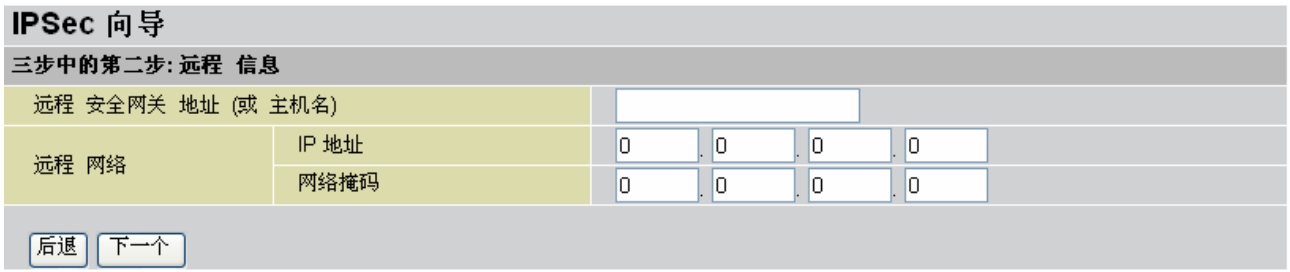
连接类型：有以下五种方式：

1. **LAN 到 LAN：**本地子网和远程子网实现 IPsec VPN，最常用的方式；
2. **LAN 到 LAN（移动 LAN）：**本地子网和远程子网实现 IPsec VPN，远程子网是个动态的 IP 地址子网；
3. **LAN 到主机：**本地子网和远程主机实现 IPsec VPN；
4. **LAN 到主机（移动客户机）：**本地子网和远程主机实现 IPsec VPN，远程主机是个动态 IP 地址的主机；

5. LAN 到主机（对 BiGuard VPN 客户机）；

下面就最常用的 LAN 到 LAN 方式做配置说明：

1. Step1，“**连接类型**”选择“**LAN 到 LAN**”；
2. Step2，如下图所示：



远程安全网关地址（或主机名）：通道对端 IP 地址或者主机域名；

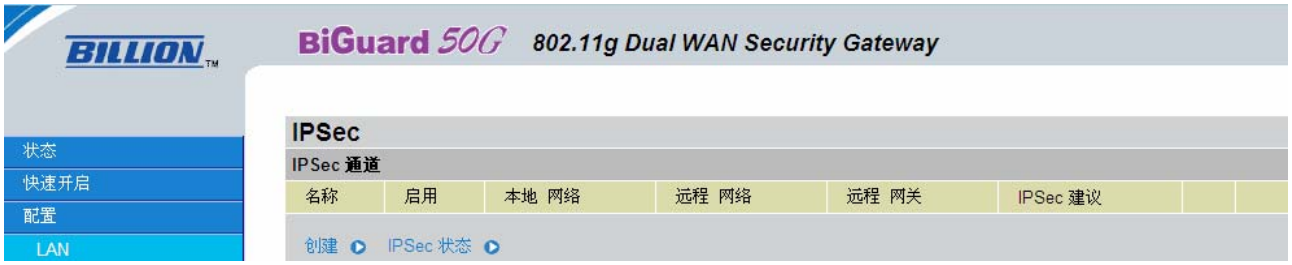
远程网络：对端的子网网段 IP 地址；

3. Step3

点击“**完成**”保存 IPsec 的向导配置；

3.2.3.6.1.2. IPsec 策略

除了向导的快速配置，还可以通过 IPsec 策略进行进行更详细的 IPsec 的配置。



IPsec 通道：IPsec 通道规则列表显示了基本的几个参数：

名称：通道名称；

启用：通道是否启用的状态说明，如果未启用，会显示叉符号“**X**”；

本地网络：可以是一个子网或者单个主机；

远程网络：可以是一个子网或者单个主机；

远程网关：也就是通道的另一端；

IPsec 建议：IPsec 通道建立的一些建议项，比如协商时用主模式还是简单模式，数据完整性检查的算法数据加密算法等等；

3.2.3.6.1.2.1. 创建 IPsec 通道

所需配置的必要参数和可选参数被分成 4 个部分；

3.2.3.6.1.2.1.1. 本地

连接名称：用来标识该通道规则；

通道：是否启用该通道规则，

- **启用**：启用该通道规则；
- **禁用**：禁用该通道规则；

接口：通道规则应用的接口，

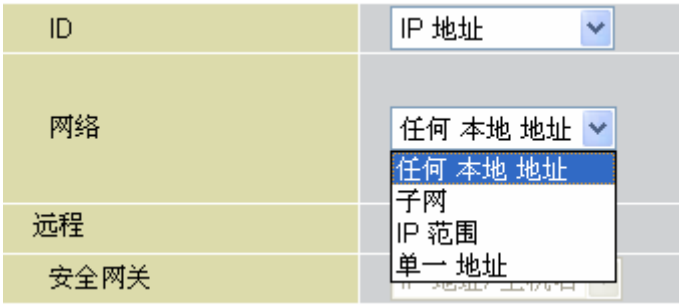
- **WAN1**：在 WAN1 接口上面应用该通道规则；
- **WAN2**：在 WAN2 接口上面应用该通道规则；
- **自动**：系统自动选择应用该通道规则的接口；

本地：通道本地端的配置项有：

■ **ID** ：通道本地端的身份标识，用于身份鉴别，有以下四种形式：

- ◆ **WAN IP 地址**：使用本地端接口的 IP 地址标识本地端身份；
- ◆ **IP 地址**：使用某个 IP 地址标识本地端身份，写在后面“**数据**”中；
- ◆ **FQDN（DNS）**：使用一个完整的域名来标识本地端身份，写在后面“**数据**”中；
- ◆ **FQUN（E-Mail）**：使用电子邮件地址来标识本地端身份，该电子邮件地址只是个标识而已，与通道本地端接口的 IP 地址没有关系的；

■ **网络**：通道本地端的网络，有如下四种：



- ◆ **任意本地地址**；
- ◆ **子网**：IP 地址为一个子网的 IP 地址范围，包括该子网所有的可用 IP 地址；
- ◆ **IP 范围**：IP 地址为某个子网的一段 IP 地址，只是一部分可用 IP 地址；
- ◆ **单一地址**：特定的某个 IP 地址；

3.2.3.6.1.2.1.2. 远程

安全网关：通道对端的 IP 地址或者主机名称，写在后面“**数据**”中；

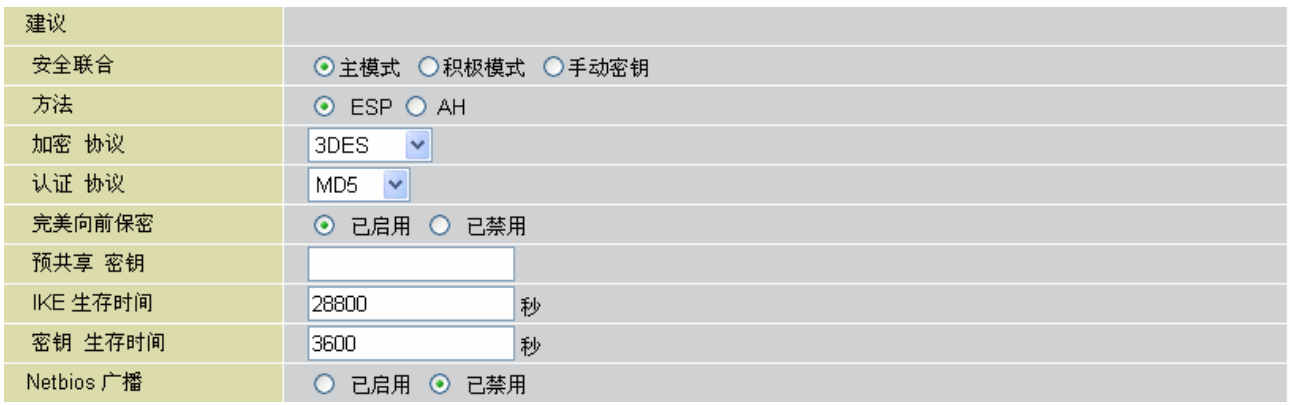
■ **ID** ：通道对端的身份表识；有如下四种形式：

- ◆ **远程 WAN IP：**用对端的 IP 地址来标识对端身份；
- ◆ **IP 地址：**使用某个 IP 地址标识对端端身份，写在后面“**数据**”中；
- ◆ **FQDN（DNS）：**使用一个完整的域名来标识对端身份，写在后面“**数据**”中；
- ◆ **FQUN（E-Mail）：**使用电子邮件地址来标识对端身份，该电子邮件地址只是个标识而已，与通道对端接口的 IP 地址没有关系的，写在后面“**数据**”中；

■ **网络：**通道对端的网络，有以下四种形式：

- ◆ **子网：**IP 地址为一个子网的 IP 地址范围，包括该子网所有的可用 IP 地址；
- ◆ **IP 范围：**IP 地址为某个子网的一段 IP 地址，是子网的一个子集；
- ◆ **单一地址：**特定的某个 IP 地址；
- ◆ **网关地址：**通道对端的 IP 地址；一般用于对对端设备进行远程控制时，隐藏传输的数据以达到安全的目的；

3.2.3.6.1.2.1.3. 建议



IPsec 通道配置的一些建议，通常是协商安全联合时的参数建议：

安全联合：一个数据库记录，记录了数据加密算法，验证算法，密钥生存期等数据；

通常协商安全联合分为两个阶段，对于第一阶段有下面两种协商模式：

- **主模式：**协商时的交互数据是被加密的；
- **积极模式：**协商的交互数据只有一部分被加密的；

主模式和积极模式是自动协商安全联合所采用的方式，也可以采用人工指定的方式配置安全联合：

手动密钥：人工指定的方式来配置安全联合的参数：

入站 SPI：对于进来的报文检查它的 SPI 值是否与该参数一致；

出站 SPI：本地发送出去的报文需要携带该参数值以便对端检查；

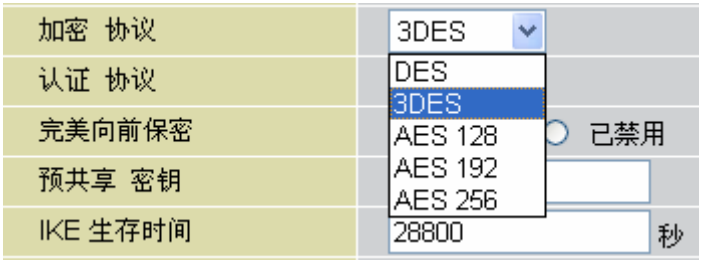
加密协议：手工设定双方加密数据的密钥；

认证协议：完整性检测时使用的密钥；

方法：指的是 IPsec 通道的封装方式，有如下两种：

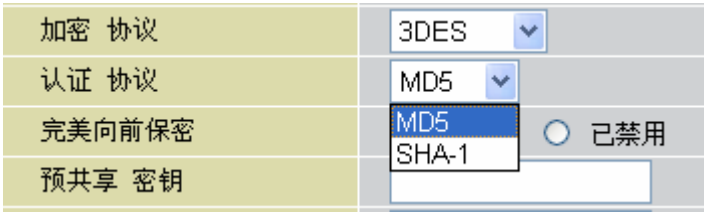
- **ESP：**封装安全载荷；
- **AH：**鉴别头；

加密协议：数据加密的算法，通常都有如下五种：



- **DES：**数据加密标准，是一个块数据加密的标准算法；
- **3DES：**三重数据加密标准，比 DES 更高级的算法，DES 和 3DES 的密钥长度为 64 位；
- **AES 128：**高级加密标准，和 DES 和 3DES 比起来是算法更高级，密钥长度为 128 位；
- **AES 192：**密钥长度为 192 的加密算法；
- **AES 156：**密钥长度为 256 的加密算法；

认证协议：用于数据完整性验证的协议，主要有以下两种：

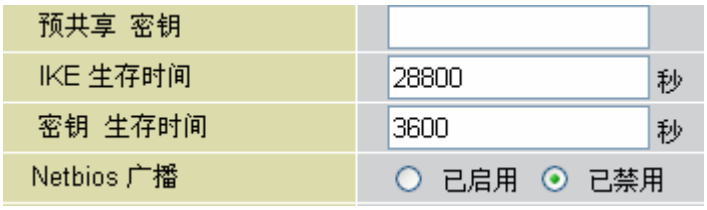


- **MD5：**信息摘要-5，对于任意长度的数据进行运算后的到一个 128 位的摘要值；
- **SHA-1：**标准散列算法-1，基本思想也是对于任意长度的数据进行运算后的到一个 128 位的散列值；

完美向前保密：该功能的作用是防止协商安全联合时产生的公钥生存期到期后，重新生成的公钥是从到期的公钥衍生出来的，也就是说每个公钥的生成都是独立的，前后没有任何依赖

关系；

- **启用：**启用该功能；
- **禁用：**禁用该功能；



预共享密钥：被用来做隧道本地端和远端的身份验证；

IKE 生存时间：IKE 协议协商产生的安全联合的有效时间；

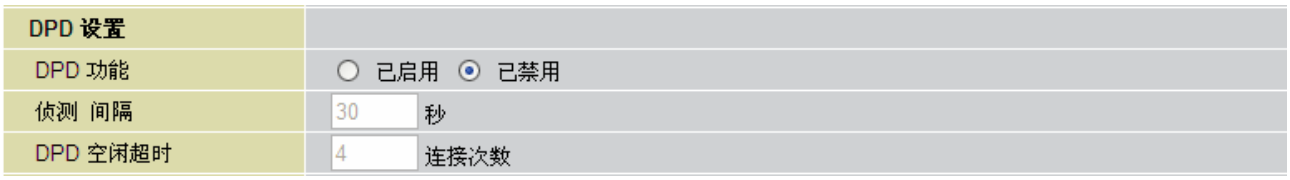
密钥生存时间：双方使用的公钥的有效时间；

Netbios 广播：是否支持 Windows 操作系统上面的一些广播服务，

- **启用：**启用该功能；
- **禁用：**禁用该功能；

3.2.3.6.1.2.1.4. DPD 设置

对端生存探测主要的目的是确认对端“活着”还是“死了”，以防止报文向“黑洞”发送；这个部分的参数是可选参数：



DPD 功能：对端生存探测功能是否开启，

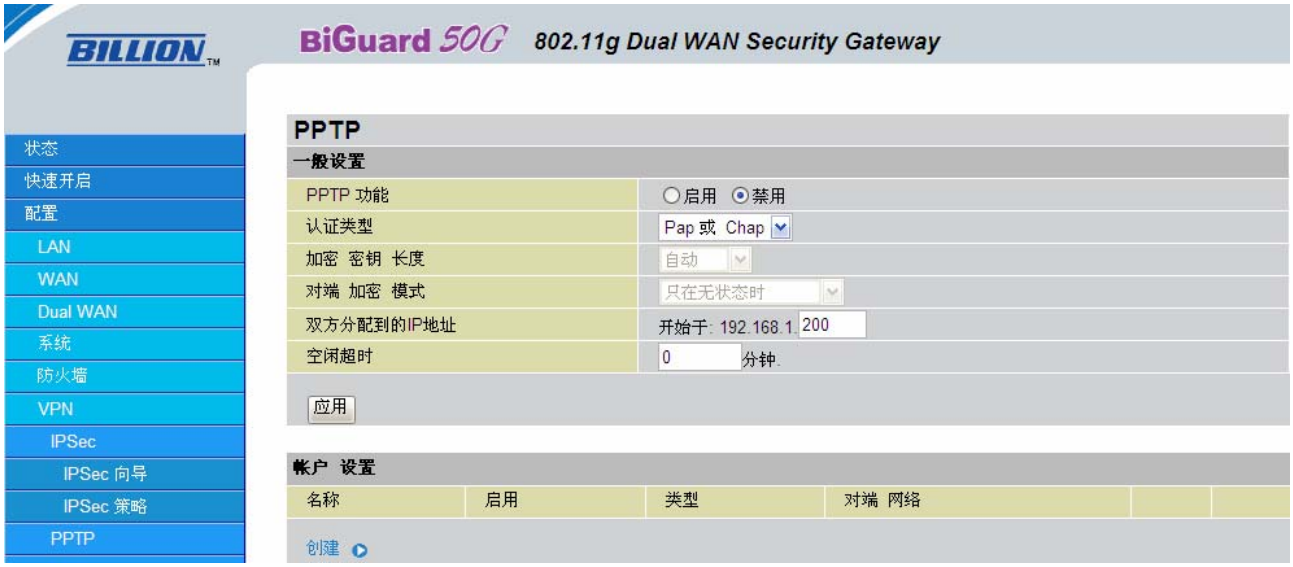
- **启用：**启用该功能；
- **禁用：**禁用该功能；

侦测间隔：探测间隔时间；

空闲超时：当连续探测几次没有响应时，断开隧道连接；

3.2.3.6.2. PPTP

PPTP，点到点隧道协议，另一种 VPN 的实现，BiGuard 50G 支持 4 个远程用户同时拨入。



PPTP 功能：是否启用该 PPTP 服务器，

- **启用：**启用该 PPTP 服务器；
- **禁用：**禁用该 PPTP 服务器；

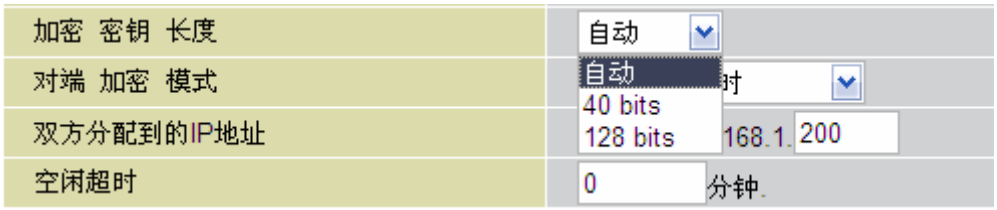
对方分配到的 IP 地址：分配给对端客户端的 IP 地址；
空闲超时：空闲时间多久后 PPP 连接断开；
认证类型：用户验证协议，主要有以下两种：

- **Pap：**一种简单的验证协议；
- **Chap：**比 Pap 更安全的验证协议；
- **Pap or Chap：**两种方式，由服务器端和客户端协商决定使用哪种验证方式；
- **MS-CHAP v2：**微软开发的第二版的质询握手身份验证协议，它提供了相互身份验证和更强大的初始数据密钥，而且发送和接收分别使用不同的密钥。

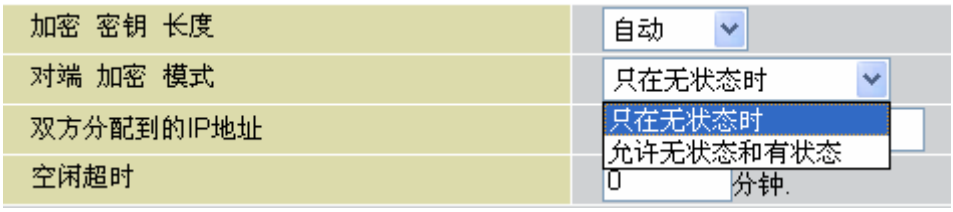
加密密钥长度：密钥长度；

- **自动：**双方协议决定；
- **40 bits：**服务器指定密钥长度为 40 位；

- **128 bits**：服务器指定密钥长度为 128 位；



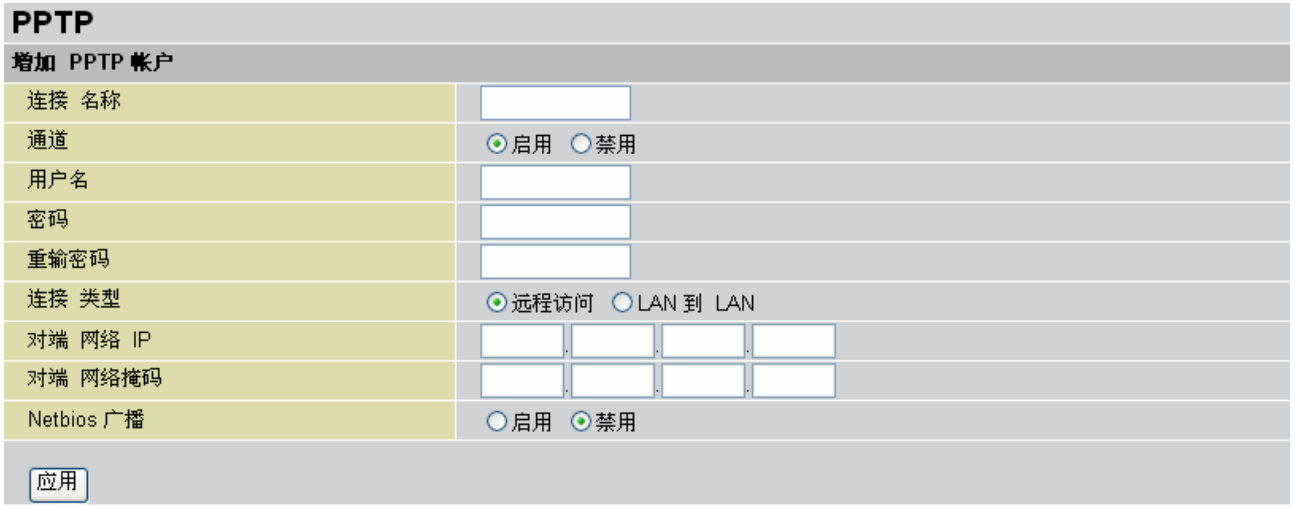
对端加密模式：



- **只在无状态时**：每次有一个包发送时，密钥都会改变，一般在网络状况不好的情况下通常被建议使用；
- **允许无状态和有状态**：有状态表明密钥只在发送了 255 个包后才会改变，服务器同时提供无状态和有状态给客户端选择使用；

帐号设置：最多可以配置 4 个用户帐号；

点击“**创建**”，进入用户帐号设定界面：



连接名称：只是为了标记该用户帐号；

通道：该帐号是否可用，

- **启用**：该帐号可以有效的；
- **禁用**：该帐号被禁用，是无效的；

连接类型：有以下两种：

- **远程访问**：可以是任何主机的请求连接；
- **LAN 到 LAN**：限制拨入用户的网络范围，只有某个网络的连接请求，PPTP 服务器才响应；

对端网络 IP：拨入用户端网络 IP 地址段；

Netbios 广播：是否支持 Windows 操作系统上的一些广播服务，例如网上邻居；

- **启用：**支持广播服务；
- **禁用：**禁用广播服务；

3.2.3.6.3. PPTP Client

PPTP 客户机：启用或禁用 PPTP 客户机功能。

连接时间：选择总是在线或手动连接。

用户名：输入用户名。

密码：输入与用户名对应的密码。

重输密码：再次输入密码。

PPTP 服务器地址：输入 PPTP 服务器地址。

对端网络 IP/对端网络掩码：输入对端的网络 IP 地址和子网掩码。

3.2.3.7. 服务质量

服务质量解决了实时应用程序如何最有效地使用网络带宽的问题，BiGuard 50G为 WAN 接口提供了双向的服务质量保证。

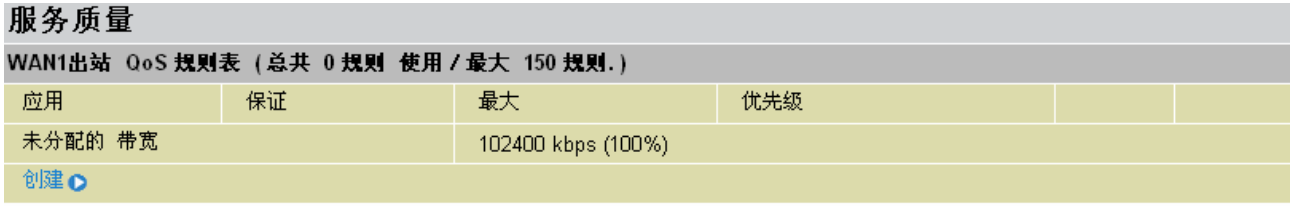
上面的配置界面同时显示了 WAN1 和 WAN2 接口的服务质量配置入口界面；

3.2.3.7.1. WAN1

3.2.3.7.1.1. WAN1 出站

为从接口发送出去的数据流提供服务质量保证。

3.2.3.7.1.1.1. 规则表



WAN1 出站 QoS 规则表，部分表项参数如下：

应用：规则名称；

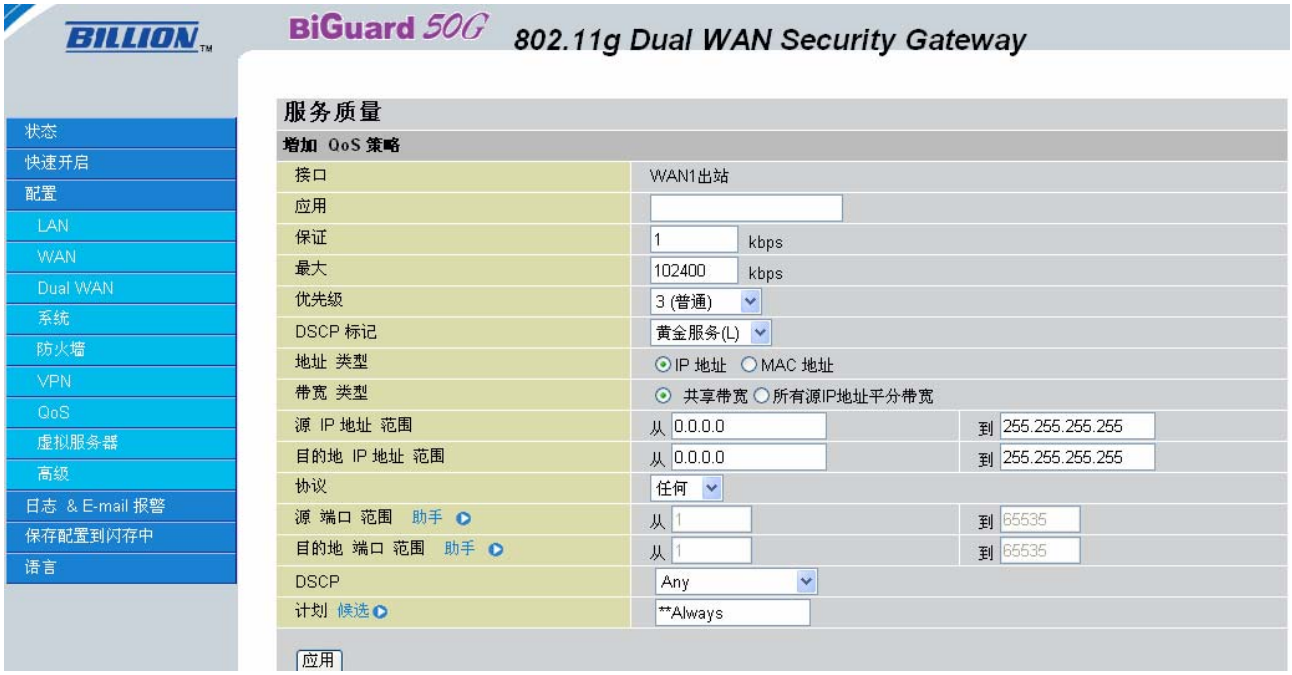
保证：分配给匹配该规则的数据流的保证的带宽；

最大：匹配该规则的数据流处于突发状态时，能够享受的最大带宽；

优先级：发送优先级，一共 7 个优先级别，0 是最先处理（发送或者接收），6 是最后处理；

未分配的带宽：也就是剩余带宽；

3.2.3.7.1.1.1.1. 创建 WAN1 出站 QoS 规则



应用：标记该规则；
保证：保证的带宽，最小为该接口总带宽的 1%，最大为该接口总带宽的 100%；
最大：可以使用的最大带宽，最小为该接口总带宽的 1%，最大为该接口总带宽的 100%；
优先级：用来表明该数据流在接口上被发送时的优先程度；分为下面 7 个优先级别，优先级别越高越早被发送，优先级别越低越晚被发送；

DSCP 标记：DSCP 是实现服务质量的一种方法，它通过在 IP 报文中的 TOS 字段做标记，以便被路由器快速转发出去，这里的作用是在报文从接口发送出去之前设置 DSCP 标记；

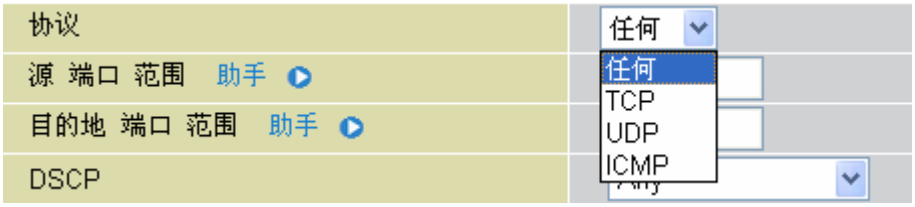
地址类型：可以是 IP 地址，也可以是 MAC 地址；

1. **IP 地址：**那么需要配置下面的 IP 地址段，
   源 IP 地址范围；
   目的地 IP 地址范围；
2. **MAC 地址：**那么需要配置下面的源 MAC 地址，

带宽类型：只有在“**地址类型**”选择“**IP 地址**”时该参数才有效，

1. **共享带宽：**所有在 IP 地址范围内的主机都享有同样的带宽；
2. **所有源 IP 地址平分带宽：**所有在 IP 地址范围内的主机平均分配带宽；

协议：有以下几种，



1. **任何：**任意的协议，不对协议做特别指定；
2. **TCP：**指定报文为 TCP 协议的报文；
3. **UDP：**指定报文为 UDP 协议的报文；
4. **ICMP：**指定报文为 ICMP 协议的报文；

源端口范围：可以手工输入也可以通过“助手”来选择：

应用	协议	端口号
Any-TCP	TCP	1~65535
Any-UDP	UDP	1~65535
FTP	TCP	20~21
SSH	TCP	22
TELNET	TCP	23
SMTP	TCP	25
DNS	UDP	53
HTTP	TCP	80
POP3	TCP	110
NTP	UDP	123
SNMP	UDP	161
HTTPS	TCP	443

目的地端口范围：和源端口范围的指定方式一样；

应用	协议	端口号
Any-TCP	TCP	1~65535
Any-UDP	UDP	1~65535
FTP	TCP	20~21
SSH	TCP	22
TELNET	TCP	23
SMTP	TCP	25
DNS	UDP	53
HTTP	TCP	80
POP3	TCP	110
NTP	UDP	123
SNMP	UDP	161
HTTPS	TCP	443

DSCP：规则的最后一个匹配条件，当某个报文 DSCP 值与这里的值相同时，该报文才被应用到该规则；
计划：时间计划表，该规则被应用的时段，可以参照配置->高级->计划的配置说明；

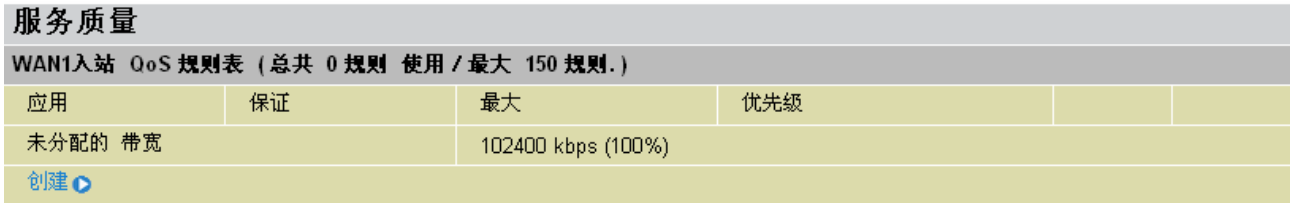
3.2.3.7.1.1.2. 带宽设置

服务质量所能提供的带宽也就接口的总带宽，当接口总带宽减少时，服务质量所拥有的带宽也随之减少，所以一般会设置接口总带宽足够大；

3.2.3.7.1.2. WAN1 入站

对于从接口接收的数据流，同样可以做服务质量的保证。

3.2.3.7.1.2.1. 规则表



WAN1 入站 QoS 规则表，部分表项参数如下：

应用：规则名称；

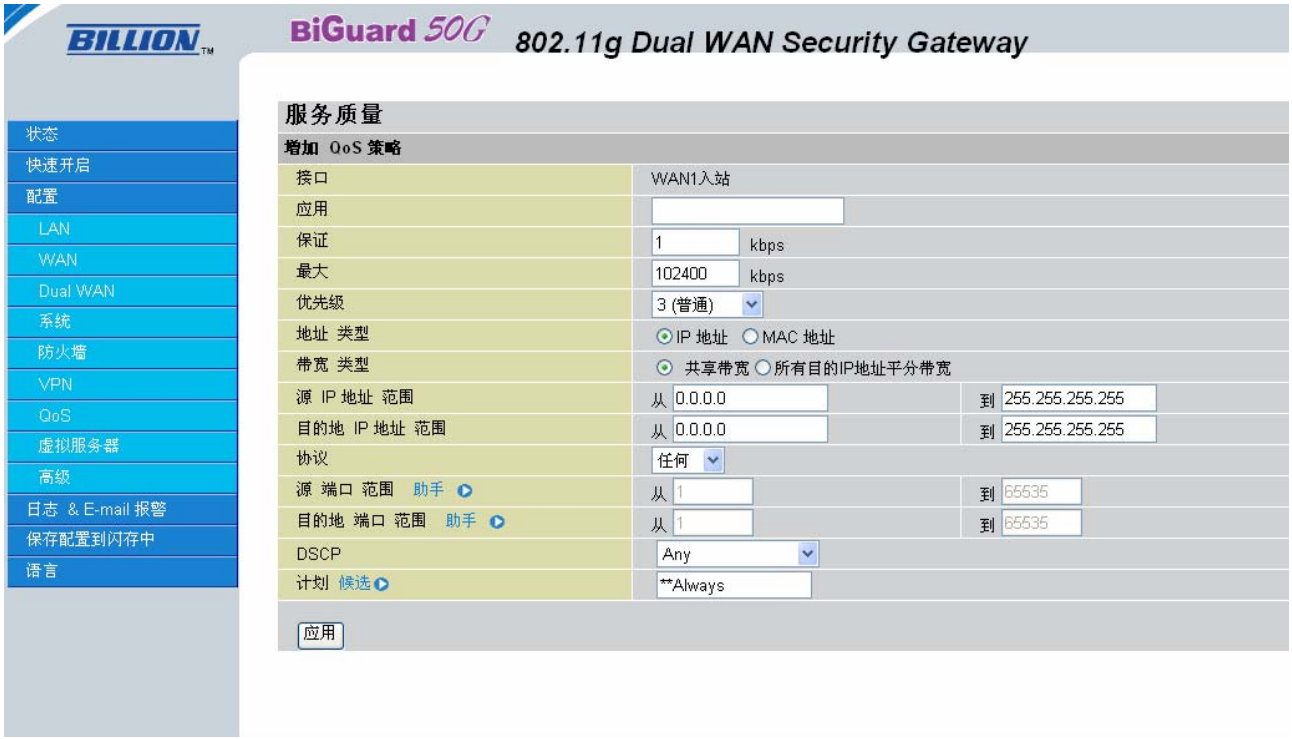
保证：分配给匹配该规则的数据流的保证的带宽；

最大：匹配该规则的数据流处于突发状态时，能够享受的最大带宽；

优先级：一共 7 个优先级别，0 是最先处理（发送或者接收），6 是最后处理；

未分配的带宽：也就是剩余带宽；

3.2.3.7.1.2.1.1. 创建 WAN1 入口 QoS 规则

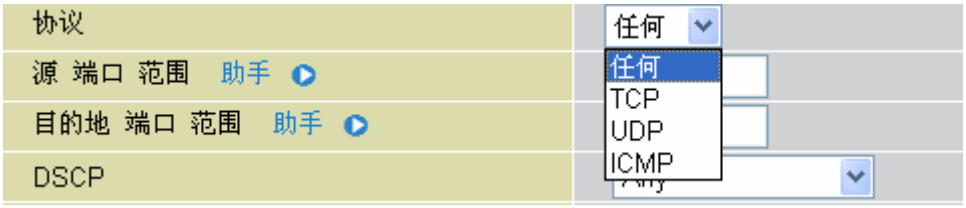


应用：标记该规则；
保证：保证的带宽，最小为该接口总带宽的 1%，最大为该接口总带宽的 100%；
最大：可以使用的最大带宽，最小为该接口总带宽的 1%，最大为该接口总带宽的 100%；
优先级：用来表明该数据流在接口上被接收时的优先程度，分为下面 7 个优先级别，优先级别越高越早被接收，优先级别越低越晚被接收；

地址类型：可以是 IP 地址，也可以是 MAC 地址；
1. **IP 地址：**那么需要配置下面的 IP 地址段，
   源 IP 地址范围；
   目的地 IP 地址范围；
2. **MAC 地址：**那么需要配置下面的源 MAC 地址，

带宽类型：只有在“**地址类型**”选择“**IP 地址**”时该参数才有效，
1. **共享带宽：**所有在 IP 地址范围内的主机都享有同样的带宽；
2. **所有源 IP 地址平分带宽：**所有在 IP 地址范围内的主机平均分配带宽；

协议：有以下几种；



1. **任何**：任意的协议，不对协议做特别指定；
2. **TCP**：指定报文为 TCP 协议的报文；
3. **UDP**：指定报文为 UDP 协议的报文；
4. **ICMP**：指定报文为 ICMP 协议的报文；

地址类型：可以是 IP 地址，也可以是 MAC 地址，

1. **IP 地址**：那么需要配置下面的 IP 地址段，
   源 IP 地址范围；
   目的地 IP 地址范围；
2. **MAC 地址**：那么需要配置下面的源 MAC 地址，

源端口范围：可以手工输入源端口范围，也可以利用“**助手**”提供的选项：

应用	协议	端口号
Any-TCP	TCP	1~65535
Any-UDP	UDP	1~65535
FTP	TCP	20~21
SSH	TCP	22
TELNET	TCP	23
SMTP	TCP	25
DNS	UDP	53
HTTP	TCP	80
POP3	TCP	110
NTP	UDP	123
SNMP	UDP	161
HTTPS	TCP	443

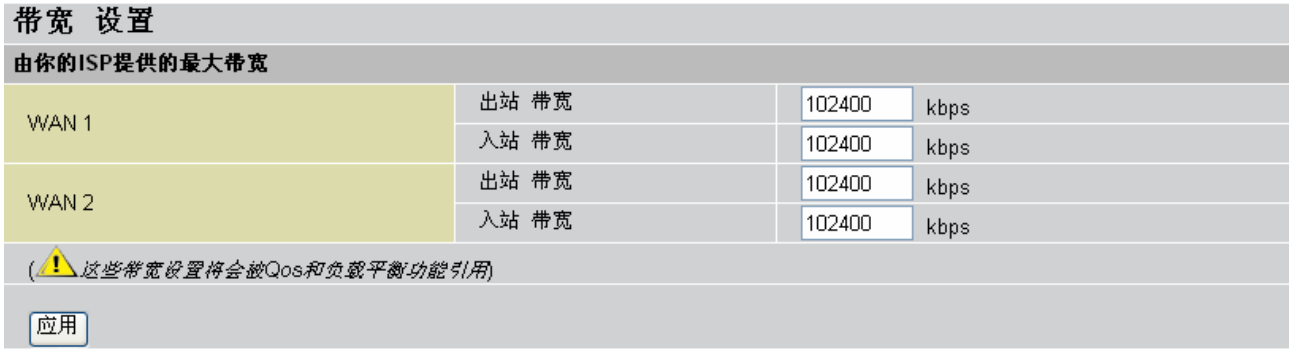
目的地端口范围：目的地端口范围的指定与源端口指定的方法一样；

应用	协议	端口号
Any-TCP	TCP	1~65535
Any-UDP	UDP	1~65535
FTP	TCP	20~21
SSH	TCP	22
TELNET	TCP	23
SMTP	TCP	25
DNS	UDP	53
HTTP	TCP	80
POP3	TCP	110
NTP	UDP	123
SNMP	UDP	161
HTTPS	TCP	443

DSCP：规则的最后一个匹配条件，当某个报文 DSCP 值与这里的值相同时，该报文才被应用到该规则；
计划：时间计划表，可以参照**配置->高级->计划**的配置说明；

3.2.3.7.1.2.2. 带宽设置

接口的接收带宽也会影响服务质量，所以尽量使接收带宽足够大。



3.2.3.7.2. WAN2

请参考 WAN1 接口上服务质量保证的配置步骤。

3.2.3.8. 虚拟服务器

虚拟服务器，通常是指那些放在企业内部网络里面的服务器，但能提供给 Internet 用户访问。

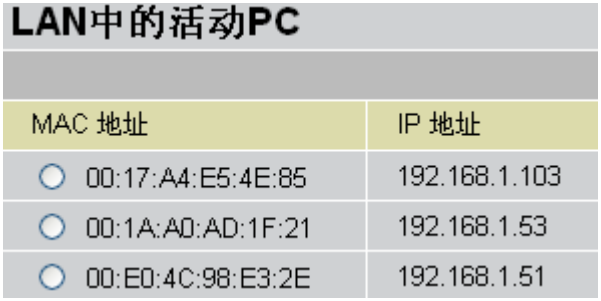
DMZ：俗称非军事区域，对于该区域中的主机或者服务器，能被 Internet 上面的用户穿过企业防火墙而访问到；

启用 DMZ 功能：是否启用该功能，

1. **启用**：启用该功能；
2. **禁用**：禁用该功能；

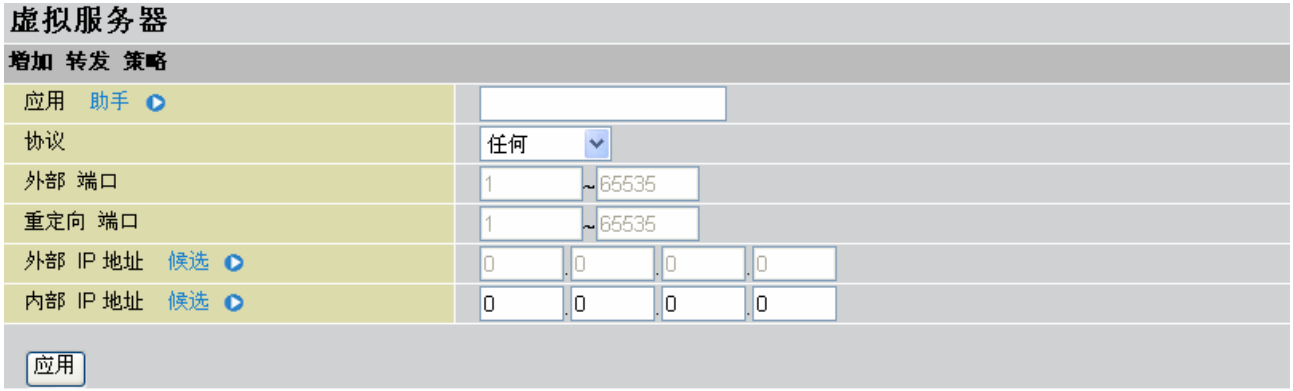
DMZ IP 地址：配置企业内部的某个服务器 IP 地址；

点击“**候选**”，进入侯选主机列表：



3.2.3.8.1. 增加转发策略

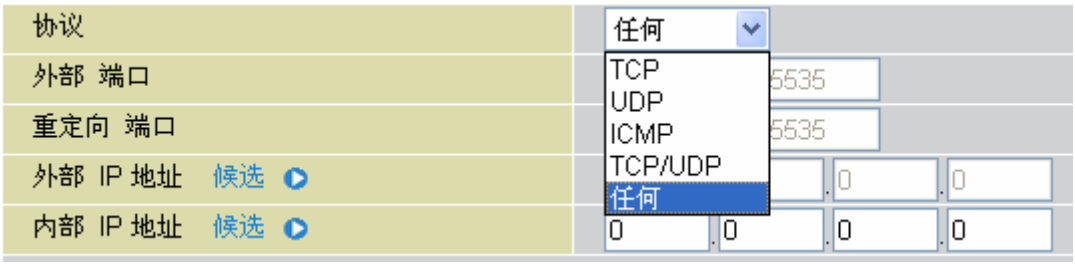
端口转发功能，一种让 Internet 用户访问企业内部架设的服务器的方法，他的功能与 DMZ 类似，只是优先级别比 DMZ 高，也就是说在同时配置 **DMZ** 和**端口转发**的情况下，Internet 用户首先能够访问到的是**端口转发**配置的服务器。



应用：应用程序名称，也可以点击“**助手**”来选择具体的应用程序：

应用	协议	端口号
Any-TCP	TCP	1~65535
Any-UDP	UDP	1~65535
FTP	TCP	20~21
SSH	TCP	22
TELNET	TCP	23
SMTP	TCP	25
DNS	UDP	53
HTTP	TCP	80
POP3	TCP	110
NTP	UDP	123
SNMP	UDP	161
HTTPS	TCP	443

协议：提供的应用程序的协议

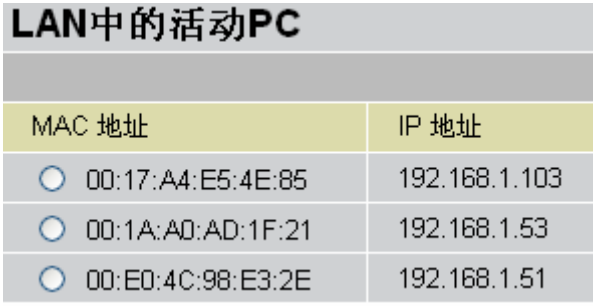


1. **任何：**任意协议；
2. **TCP：**TCP 协议的应用程序；
3. **UDP：**UDP 协议的应用程序；
4. **ICMP：**ICMP 协议的应用程序；
5. **TCP/UDP：**TCP 或者 UDP 协议的应用程序；

外部端口：也就是 Internet 用户访问的企业内部服务器时，所使用的端口号，当协议选择“**任何**”和“**ICMP**”时，该端口号不用配置；

重定向端口：也就是企业内部服务器上的应用程序所使用的端口号，当协议选择“**任何**”和“**ICMP**”时，该端口号不用配置；

内部 IP 地址：内部服务器的 IP 地址，也可以通过点击“**候选**”，进入侯选主机列表选择服务器的 IP 地址：



3.2.3.9. 高级

高级功能包括静态路由和动态域名系统，以及设备管理、计划时间表等功能；

3.2.3.9.1. 静态路由

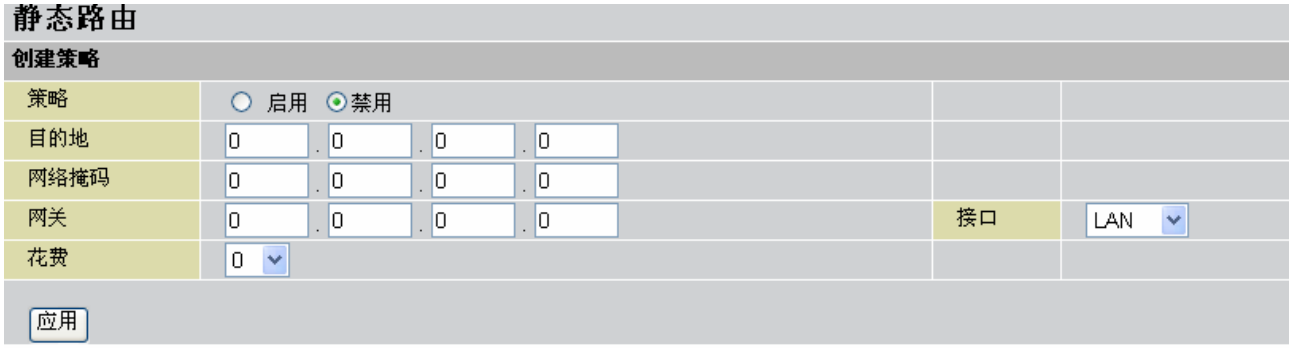
静态路由表：路由表条目一般有以下几个参数：

启用：该路由规则是否有效；

目的地：目的网络，可以是网段，也可以是单个 IP 地址；

网关/接口：或者说下一跳的 IP 地址；

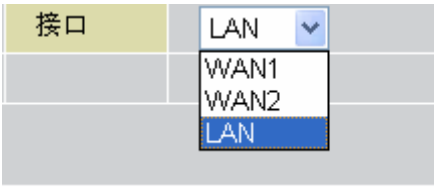
3.2.3.9.1.1. 创建策略



策略：是否启用该路由规则，

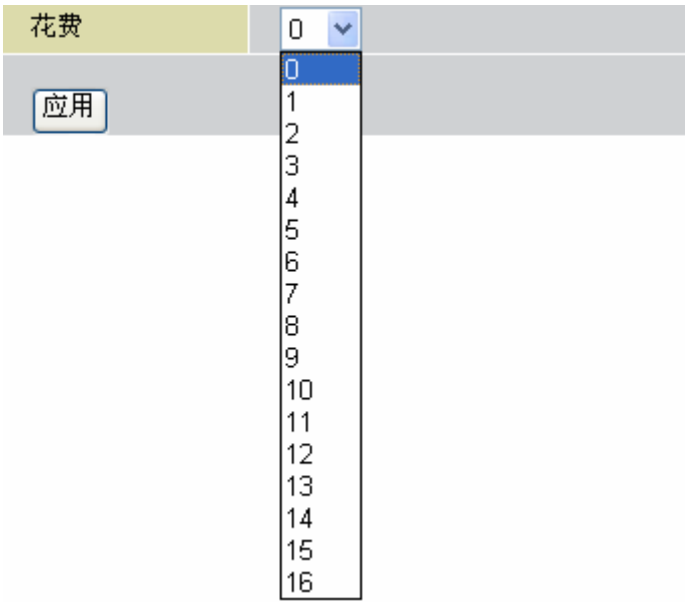
1. **启用：**启用该路由规则；
2. **禁用：**禁用该路由规则；

目的地：目的网络，可以是网段，也可以是单个 IP 地址；
网络掩码：与目的地址联合使用来表示一个网段还是单个 IP 地址；
网关：也就是下一跳的 IP 地址；
接口：表明从哪个接口发送出去；



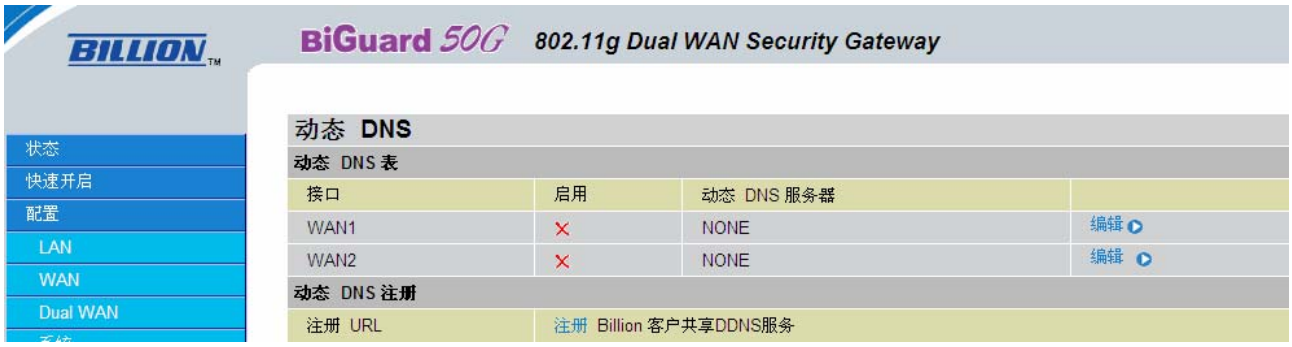
1. **WAN1：**从 WAN1 接口发送出去；
2. **WAN2：**从 WAN2 接口发送出去；
3. **LAN：**从 LAN 接口发送出去；

花费：路由好坏的一个度量指标，路由器能智能的根据开销来选择路由；



3.2.3.9.2. 动态 DNS

DDNS 常常被用于动态 IP 地址的场景，以便 Internet 用户能够通过域名来访问企业内部的服务器；



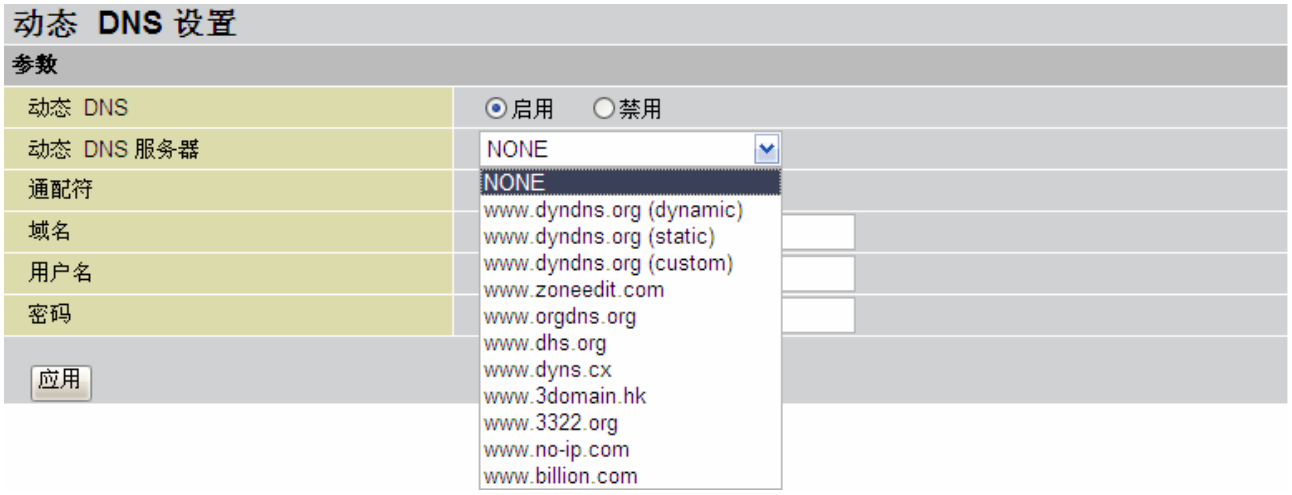
在每个 WAN 接口上面都可有配置一个 DDNS 系统，每当 WAN 接口的 IP 地址变化后，会更新 Internet 上面的 DDNS 服务器的域名和 IP 地址的对应关系；

点击“**编辑**”进入配置界面：

动态 DNS：是否启用 DDNS 的功能；

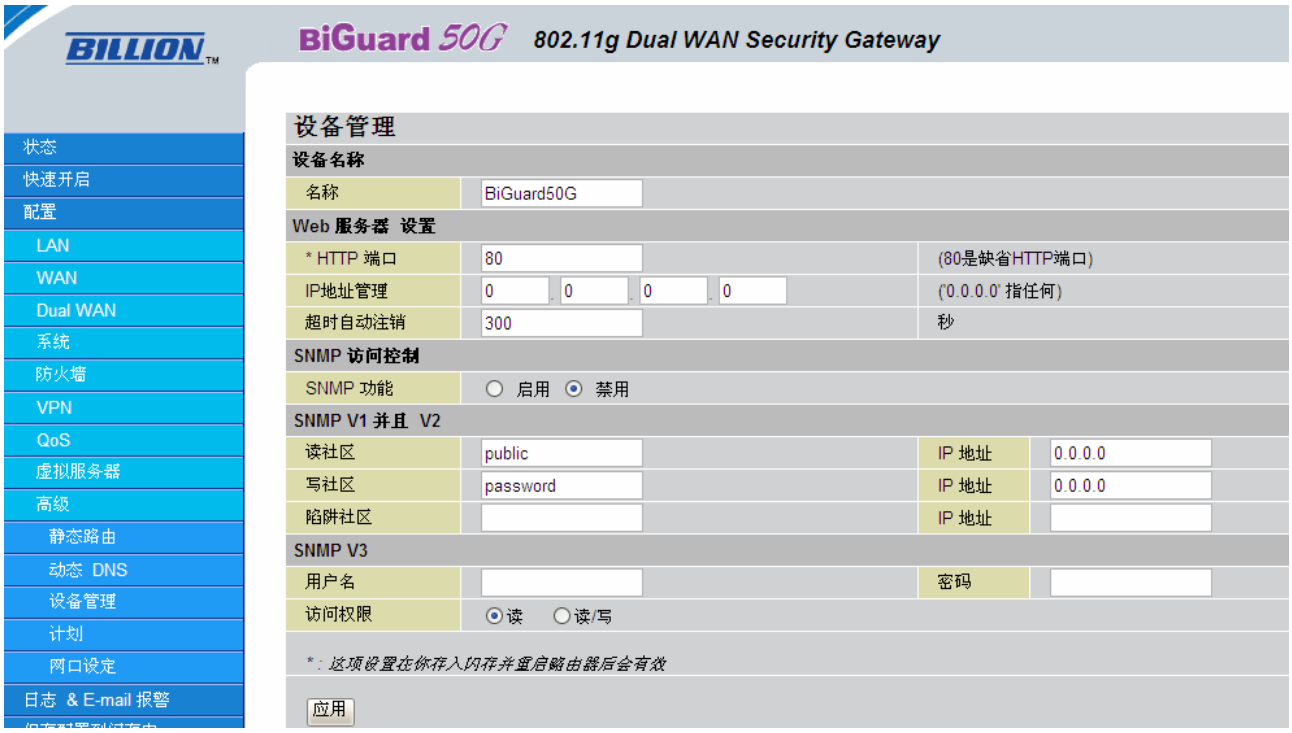
1. **启用：**启用该功能；
2. **禁用：**禁用该功能；

动态 DNS 服务器：当启用 DDNS 功能后，可以通过下拉列表选择 DDNS 服务器，为了使用这些服务器，需要在它们的网站注册用户 ；



域名：向 DDNS 服务器提供商申请的域名；
用户名：注册的用户名；
密码：用户密码；

3.2.3.9.3. 设备管理



HTTP 端口：访问该设备时默认的 HTTP 应用的端口是 80，但也可以修改为其他端口号，以便只有管理员才能对该设备进行配置管理，请注意该端口的修改需要重启设备才能生效；
IP 地址管理：指定管理该设备的主机 IP 地址；
超时自动注销：管理员登录到设备上后，不对设备进行配置时，管理员帐号会在经过一段时间后自动登出；
SNMP 访问控制：SNMP 协议是一种常用的管理设备的协议，下面可以配置 SNMP V1 和 V2，V3：

SNMP V1 并且 V2：V1 和 V2 配置项一样的：

Read 社区：可以认为读操作时使用的身份验证字符串；
IP 地址：对该设备进行读操作的主机 IP 地址；
Write 社区：可以认为写操作时使用的身份验证字符串；
IP 地址：对该设备进行写操作的主机 IP 地址，可以是和读操作同一主机；
陷阱社区：当设备某写状态改变时，会主动发送信息告诉该陷阱主机；
IP 地址：陷阱主机，接收设备发送的信息；

SNMP V3：SNMP 协议的第三个版本，对身份验证数据进行了保密；
访问权限：

1. **读：**对设备只能进行读操作；
2. **读/写：**对设备可以进行读操作和写操作；

3.2.3.9.4. 计划

计划时间表为很多应用提供了弹性，比如说防火墙功能、质量服务保证等等。

计划：计划时间表，主要由以下几个参数构成：
名称：计划表名称；
一星期中哪天：可以同时选择星期一到星期天；
时间：一天中的时段；

3.2.3.9.5. 网口设定

通过网口设置对路由器的以太网端口进行配置，从而解决连接到 Internet 时可能发生的兼容性问题，用户也可以调整网络性能。

接口：有 2 个 WAN 接口和 4 个 LAN 接口可供选择。
端口 LAN 流量统计：选择是否启用对端口 LAN 的流量进行统计。
速度：有以下五个选项可供选择。

Auto
10M 全双工
10M 半双工
100M 全双工
100M 半双工

3.2.4. 日志 &E-mail 报警

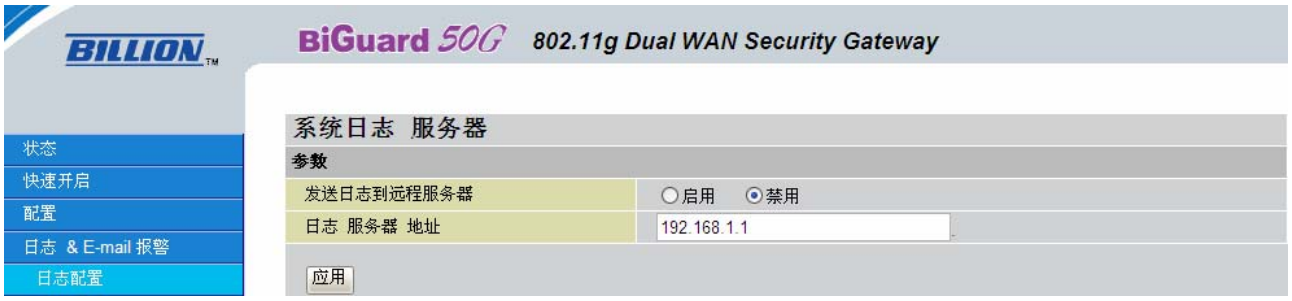
日志对于管理员维护系统护有很大的帮助，电子邮件告警让管理员随时随地都能获悉设备运行状况。

3.2.4.1. 日志配置

目录：日志事件种类；
系统日志：把日志记录在系统上面，通过**状态->系统日志**可以查看日志信息；
系统日志服务器：把日志记录在专门的日志服务器上面，具体配置请参照下一小节“**系统日志服务器**”的配置说明；
E-mail 报警：把日志通过邮件方式发送给管理员，具体配置请参照下面“**E-Mail 报警**”章节的配置说明；

3.2.4.2. 系统日志服务器

系统日志对于设备的维护很重要，所以可以专门利用一台主机来做日志服务器，设备会自动把日志保存到日志服务器上面去，当然服务器可以使用软件 Syslog 来搭建；



发送日志到远程服务器：是否把日志保存到日志服务器，

① **启用：**启用把日志保存到日志服务器的功能；

② **禁用：**日志保存在设备上面，并不保存到日志服务器上面去；

日志服务器 IP 地址：通常会在企业内部搭建日志服务器 ；以方便多个设备的日志管理；

3.2.4.3. E-Mail 报警

通过配置电子邮件报警功能，让管理员随时随地知道设备的运行情况。

E-Mail 报警：是否启用电子邮件报警功能，

① **启用：**启用该功能；

② **禁用：**不启用该功能；

接受者的 E-Mail 地址：管理员接收告警邮件的电子邮件信箱；

发送者的 E-Mail 地址：管理员的发送告警邮件的电子邮件信箱，设备会把产生的告警邮件先发送到该信箱，然后由该信箱的邮件发送服务器来发送给邮件接收者；

SMTP 邮件服务器：发送邮箱的发送邮件的服务器；

邮件服务器登录：发送邮件的时候先登录管理员的发送邮箱，

① **启用：**启用该功能，登录发送者邮箱；

② **禁用：**禁用该功能，不登录发送者邮箱；

通过电子邮件报警时机：

① **立即：**当有事件产生的时候，立即发送邮件给管理员；

② **每小时：**每小时发送一次；
③ **每日：**每天某个时间点才发送；
④ **每周：**每周星期几才发送；
⑤ **当日志已满：**当系统保存日志已经达最大日志量时，才发送给管理员；

3.2.5. 保存配置到闪存中

保存所有配置的修改内容到 Flash 里面去，配置信息写到 Flash 的时候，会有点延迟；

3.2.5.1. Save Config （保存配置）

可以通过点击界面底部的 SAVE CONFIG 按钮，来保存配置到 Flash。

3.2.5.2. Restart （重启系统）

可以通过点击界面底部的 RESTART 按钮来重启系统。

3.2.5.3. Logout （退出系统）

可以点击界面底部的 LOGOUT，弹出退出窗口，点击确认按钮退出系统。

4. 使用说明

BiGuard 50G 软件说明以及硬件规格说明；

4.1. 软件说明

BiGuard 50G 功能、性能、安全性说明；

4.1.1. VPN 特性

- 最多支持 50 条 IPsec 隧道并发；
- IPsec 隧道带宽可达 30Mbps；
- 最多支持 4 条 PPTP 连接；
- PPTP 连接带宽可达 10Mbps；
- 支持 IKE 自动协商密钥；

- 支持手工设置密钥；
- MD5，SHA-1 认证；
- DES/3DES 加密；
- AES128/192/256 加密；
- AH 封装 IPsec 数据；
- ESP 封装 IPsec 数据；
- IPsec VPN 中继功能；
- 动态 IPsec VPN（FQDN）；
- IPsec NAT 穿越；
- IPsec DPD 检测对端；
- 支持 LAN to Host 和 LAN to LAN 的 IPsec VPN；
- PPTP 服务器；

4.1.2. 防火墙特性

- 状态包检测；
- 防止黑客攻击；
- 包过滤；
- MAC 过滤；
- 入侵检测；
- URL，Domain 过滤；
- Java Applet/ActiveX 阻止；

4.1.3. 设备管理特性

- 基于 Web 的配置方式；
- 基于 Web 的版本更新方式；
- 远程管理；
- 备份配置文件；
- 恢复配置文件；

4.1.4. QoS 特性

- 支持差别服务（DiffServ）；
- 带宽管理；
- 优先级管理；
- 双向 QoS；

4.1.5. 网络特性

- 静态 IP，PPPoE，DHCP 等宽带接入；

- DHCP Server ，DHCP Relay；
- 网络地址转换（MultiNAT，SNAT，DNAT）；
- 路由信息协议（RIPv1，RIPv2）；
- 动态域名系统（DDNS）；
- 网络管理协议（SNMP）；
- 虚拟服务器；
- 时间同步（SNTP）；
- 支持组播转发（IGMP Proxy，Snooping）
- 路由及透明桥（VLAN）；
- SIP 透明传输；

4.2. 硬件规格说明

4.2.1. 物理接口

- 2 个 10/100Mbps WAN 接口；
- 8 个 10/100Mbps LAN 接口；
- 电源开关；
- 重置按钮；
- 天线；

4.2.2. 电源要求

- 12V DC、1A 电源；

4.2.3. 环境要求

运行环境温度：0~40 C；
运行环境湿度：20%~95% 非冷凝；

5. 常见 FAQ

1. Q：**通过设备面板上的“重启”按钮怎么把设备到恢复出厂设置？**

A：设备带电状态下，按住“**重启**”按钮持续 8 秒；或者观察“**状态**”灯变成橙黄色，说明恢复成功。

2. Q：**LAN 主机不能访问设备 LAN 接口？**

A：首先请检查主机和设备的物理连接是否有问题；

其次是请检查主机是否和设备 LAN 接口在同一网段，方法是不配置主机网关，在命令行下使用 arp –d 命令清除缓存，然后 ping 设备 LAN 接口的 IP

地址，如果显示信息为“**Host Unreachable**”说明不在同一网段，如果显示信息为“**time out**”，说明在同一个网段。主机和设备 LAN 接口 IP 地址不在同一网段，而又不知道 LAN 接口网段的情况下，可以把设备恢复到出厂设置；

3. Q：**LAN 侧主机 192.168.1.33 只允许收发邮件，应该怎么配置？**

A：在**配置->防火墙->包过滤**里面配置如下 4 条规则：

- 第一条：
  1. 规则＝启用，
  2. 当匹配时作用=接收，
  3. 流向=出站，
  4. 源 IP=192.168.1.33，
  5. 目的地 IP=任何，
  6. 协议=UDP，
  7. 源端口=任何，
  8. 目的地端口=53；
- 第二条：规则其他参数①~⑤配置和第一条一样，协议=TCP，源端口=任何，目的地端口=25；
- 第三条：规则其他参数①~⑦配置和第二条一样，目的地端口=110；
- 最后一条：规则其他参数和第三条一样，当匹配时作用=丢弃，目的地端口=任何；

4. Q：**设备放在防火墙后面，怎么和企业中心建立 IPsec 隧道连接？**

A：Ipsec 隧道建立时参数配置仍然和前面没有防火墙时一样配置，防火墙能做

“**虚拟服务器**”的话，可以做个“**虚拟服务器**”指向 BiGuard 50G 的 WAN 接口；如果不能做，那么需要 BiGuard 50G 主机发起隧道连接的报文，具体操作是在 Ipsec 状态界面，点击“**连接**”按钮；

5. Q：**WAN 连接使用 PPPoE 方式，当天公司员工可以上网，但第二天早上需要重启设备才能 PPPoE 拨号成功，这是为什么，有什么办法改变这种现状？**

A：PPPoE 拨号成功后，ISP 的宽带接入服务器会检查该拨号连接是否空闲了一段时间，然后 ISP 会踢掉用户，导致用户不能上网，可以选择“**连接类型**”为“**按需触发**”方式，当没有用户上网时，BG50 自动断开和 ISP 宽带接入服务器的连接 ；

6. Q：**IPsec 隧道规则配置有哪些注意要点？**

A：首先本地端的 ID 与远端的 ID 需要一致，然后双方使用的加密算法和验证算法都必须相同，最后是共享密钥必须相同，这样隧道才能建立起来。

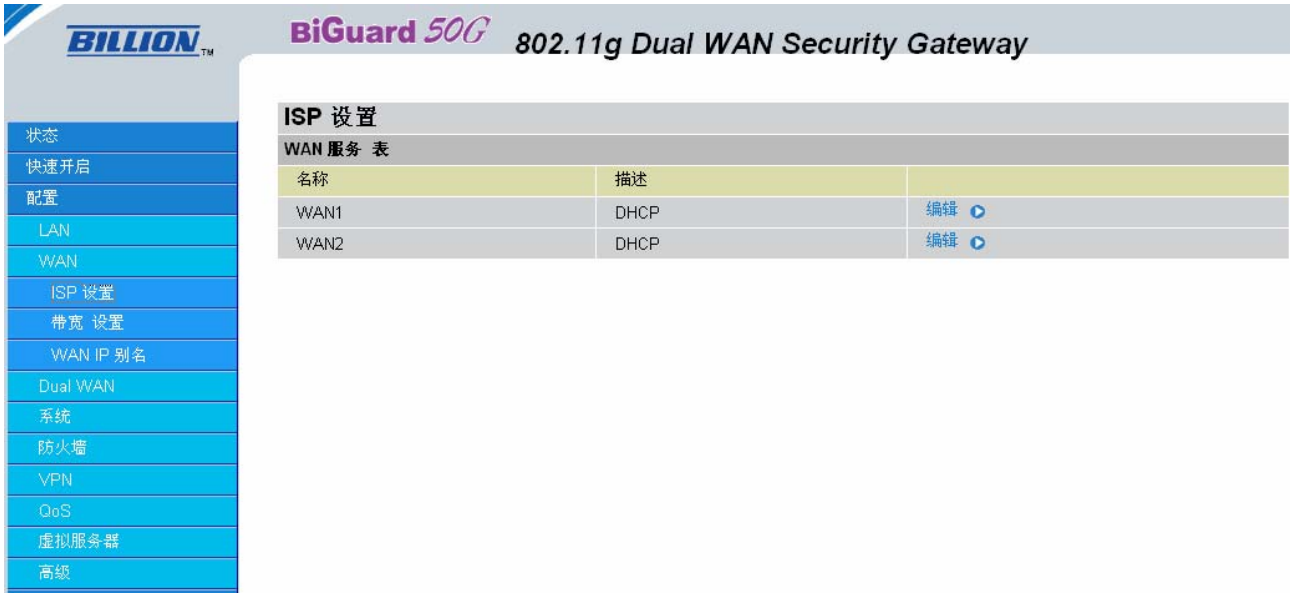
7. Q：**能否限制设备上的 LAN 侧端口上网？**

A：可以通过**配置->高级->VLAN 网桥**功能来实现，启用 VLAN 网桥模式，从 “**默认**”桥中移除想要被禁用的端口，该端口下的主机就没办法上网了。

6. 推荐方案

6.1. 出站自动线路备份

Step 1: 配置-〉WAN-〉ISP 设置，选择 WAN1 和 WAN2，然后点击“**编辑**”；



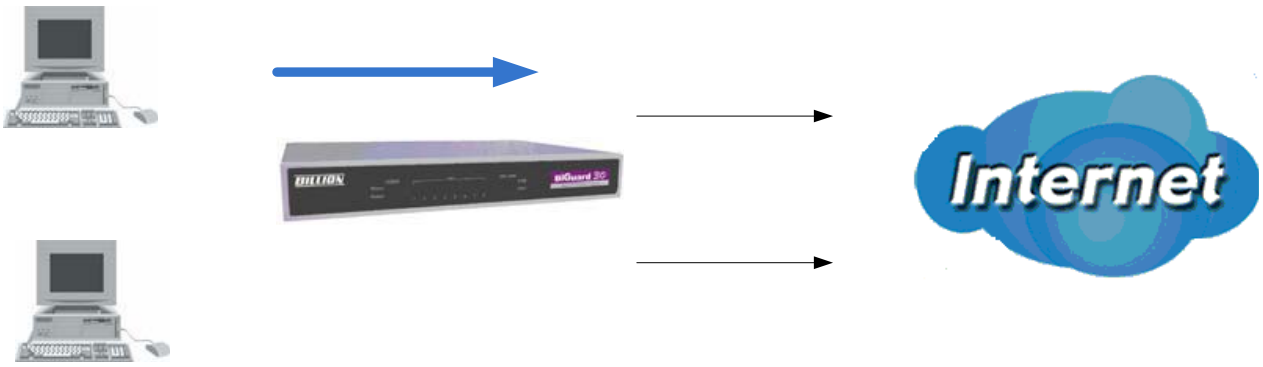
Step 2: 根据 ISP 提供的信息配置 WAN1 和 WAN2；

Step 3: 配置->Dual WAN->一般设置，选择“**失效切换**”，在连接决策菜单里面输入次数为了探测 WAN 与 ISP 提供服务的连通性(默认值是3次)，然后输入探测周期和探测方式；

选择是否要回切到 WAN1 (对于失效切换来说，当 WAN1 能够恢复到正常工作时)；

Step 4: 点击“**保存**”保存配置到闪存；

6.2. 出站负载均衡



根据下面的步骤来配置出站负载均衡:

Step 1：配置-> WAN -> ISP 设置，根据 ISP 提供的信息配置 WAN1 并点击“**应用**”；

192.168.2.2

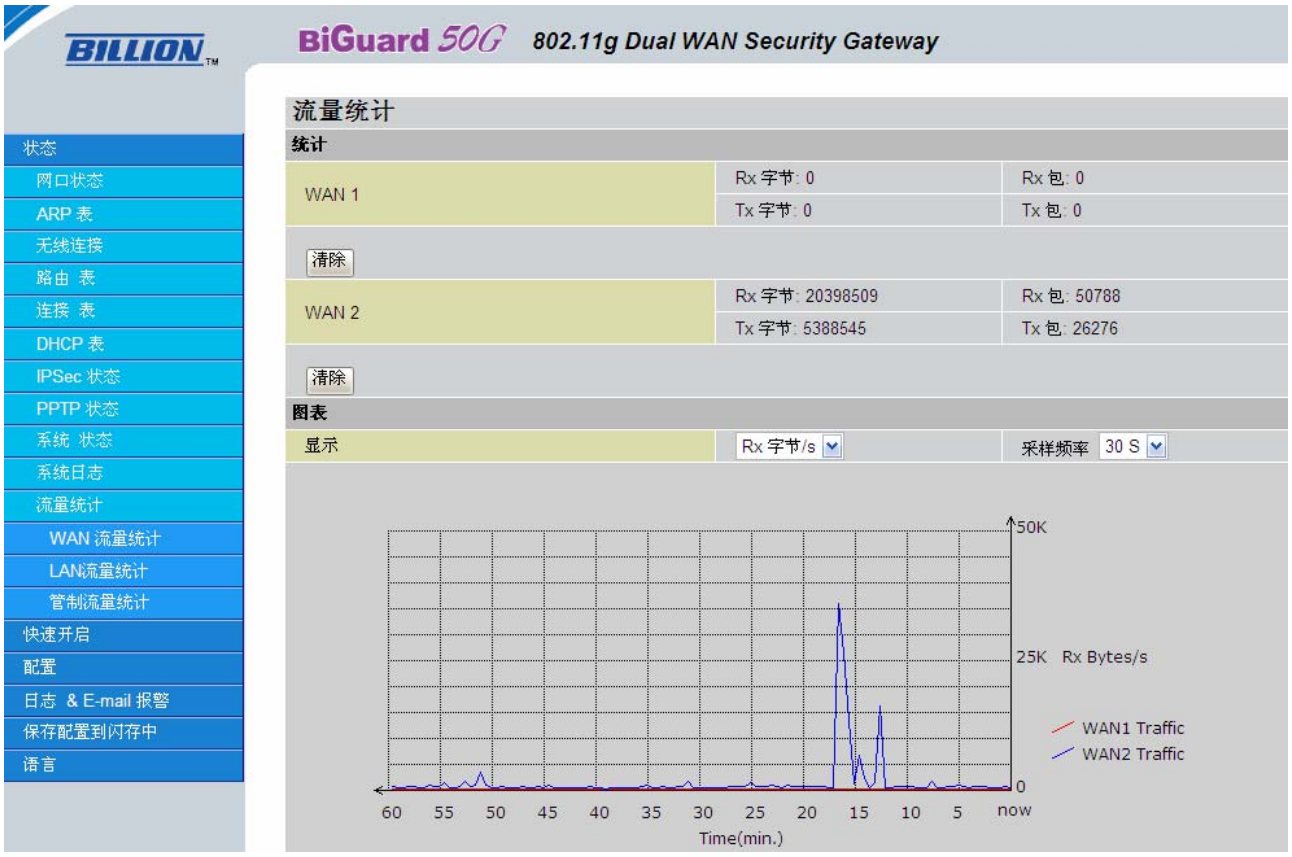

BILLION
BiGuard 50G
802.11g Dual WAN Security Gateway
状态
快速开启
配置
LAN
WAN
ISP 设置
带宽 设置
WAN IP 别名
Dual WAN
系统
防火墙
VPN
QoS
虚拟服务器
高级
WAN1
静态IP
连接方式
静态IP设置
由你的ISP分配的IP
230 . 100 . 100 . 1
IP 子网掩码
255 . 255 . 255 . 0
ISP 网关 地址
230 . 100 . 100 . 254
MAC 地址
候选
你的ISP要求你输入WAN以太网MAC
MAC 地址 00 - 00 - 00 - 00 - 00 - 00
首选 DNS
168 . 95 . 192 . 1
备用 DNS
168 . 95 . 1 . 1
RIP
禁用
RIP-2B
RIP-2M
MTU
1500
网络地址转换
启用
禁用
应用
重置

Step 2：配置-> WAN -> ISP 设置，根据 ISP 提供的信息配置 WAN2 并点击“**应用**”；

Step 3: 配置-> Dual WAN ->一般设置，选择“**负载均衡**”；

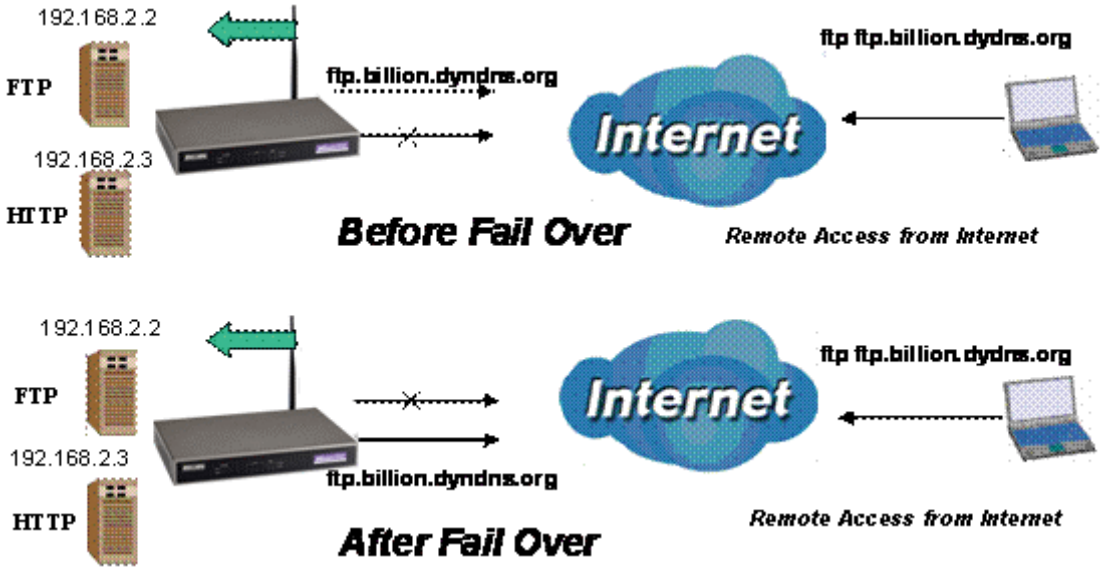
Step 4: 配置-> Dual WAN->出站负载均衡，选择你需要的负载均衡平衡机制，并点击“**应用**”；

Step 5: 完成后，检查流量统计,**状态->流量统计**；



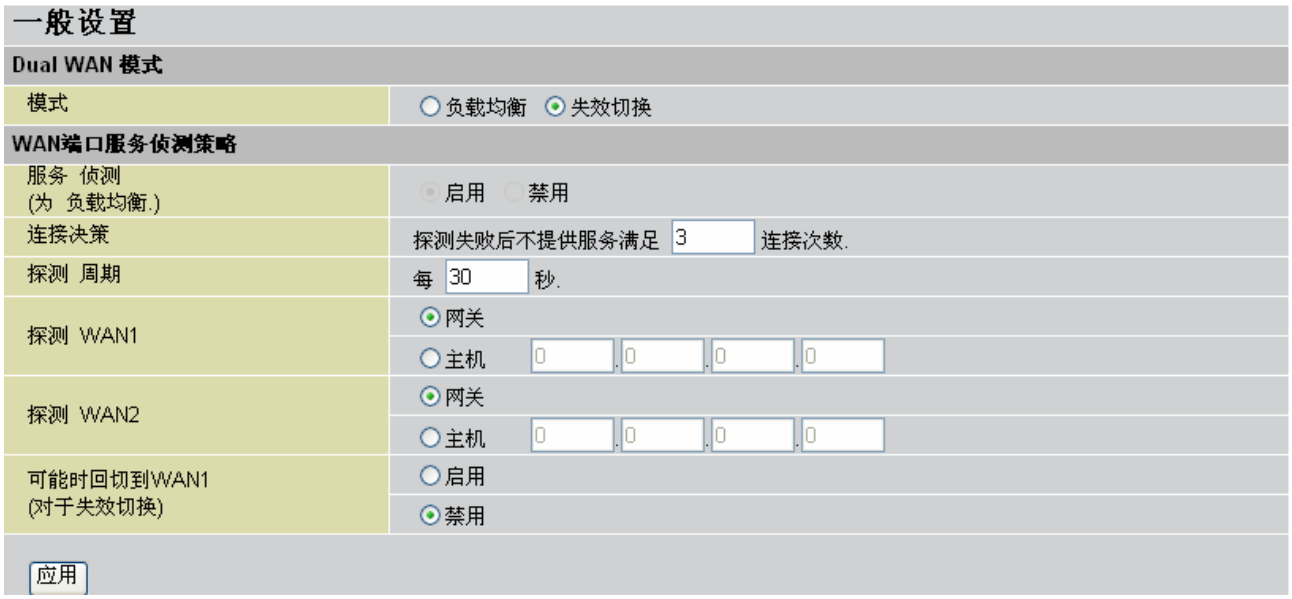
Step 6: 点击“**保存**”保存配置到闪存；

6.3. 入站失效切换

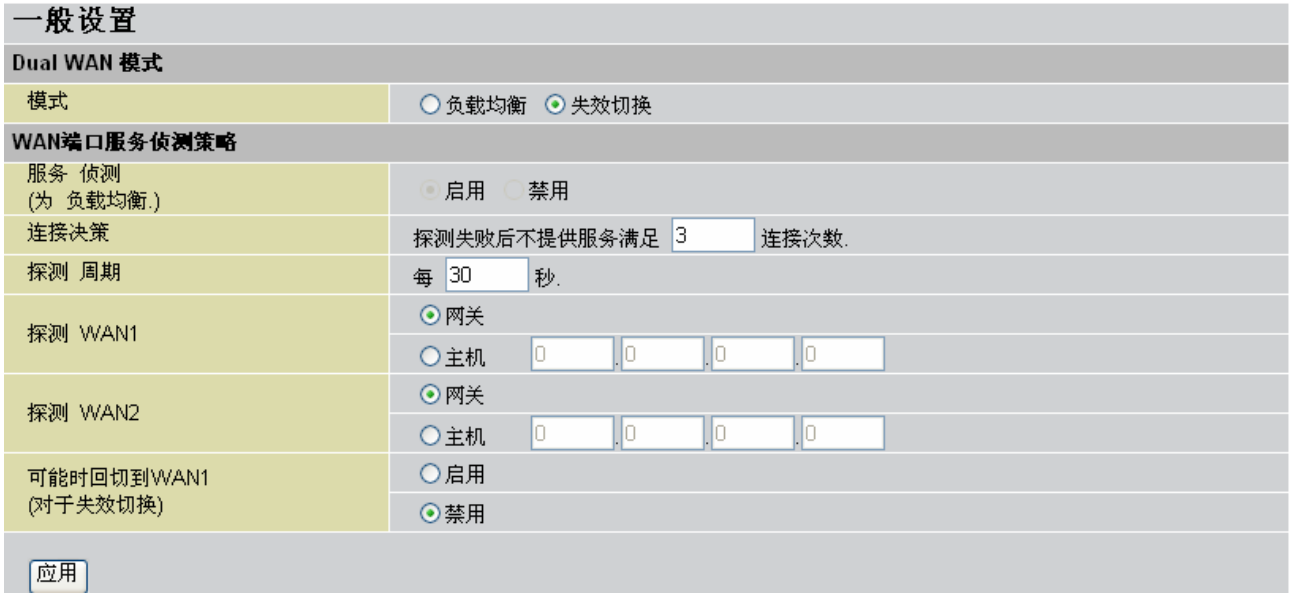


在配置之前，请确保已经配置好 WAN1 和 WAN2。

Step 1：进入 WEB 配置界面，**配置-> Dual WAN->一般设置**，选择“**失效切换**”；

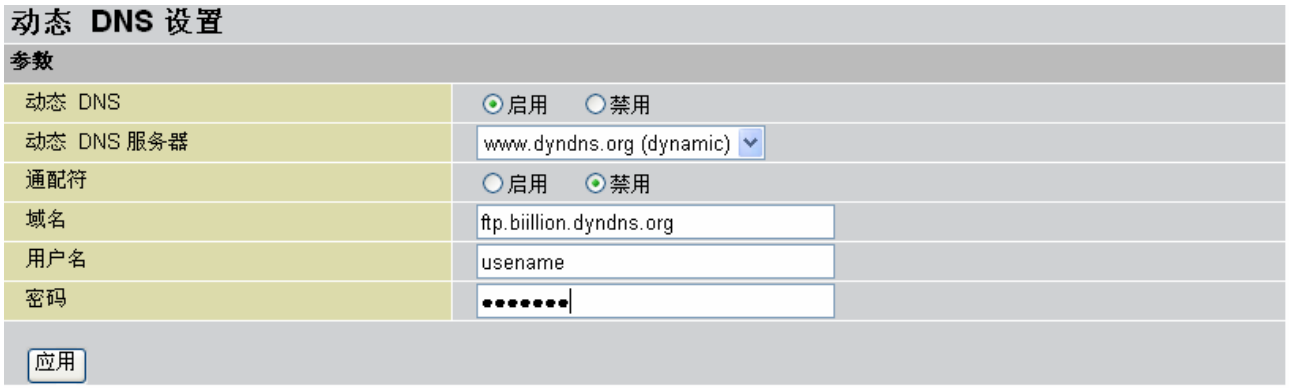


Step 2：根据需要配置失效切换选项；

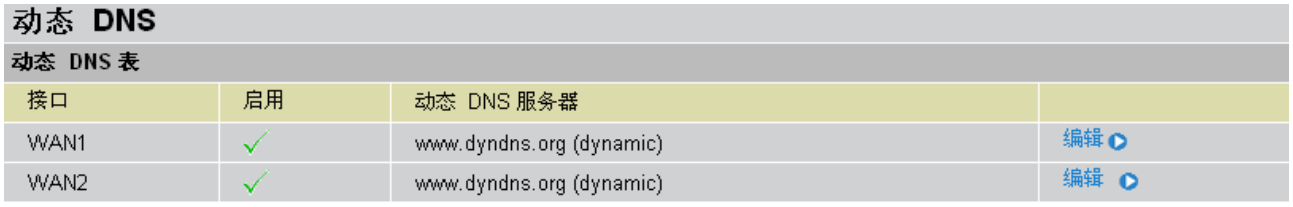


Step 3：**配置->高级->动态 DNS**，设置 WAN1 动态 DNS；

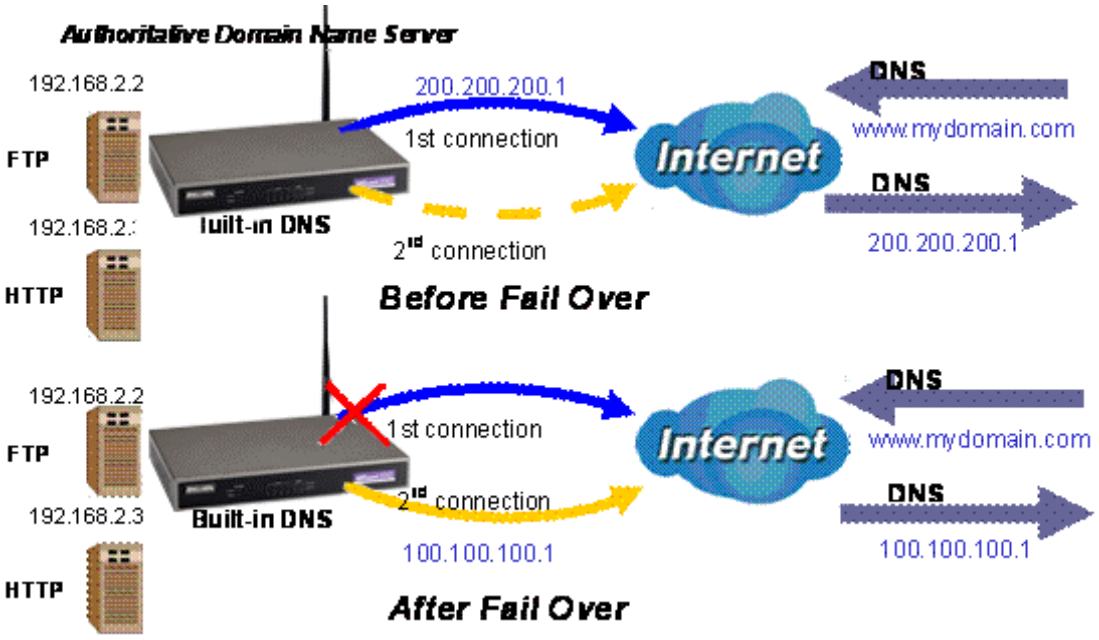
Step 4: 同样设置 WAN2 动态 DNS；



Step 5: 点击“**保存**”保存配置到闪存；



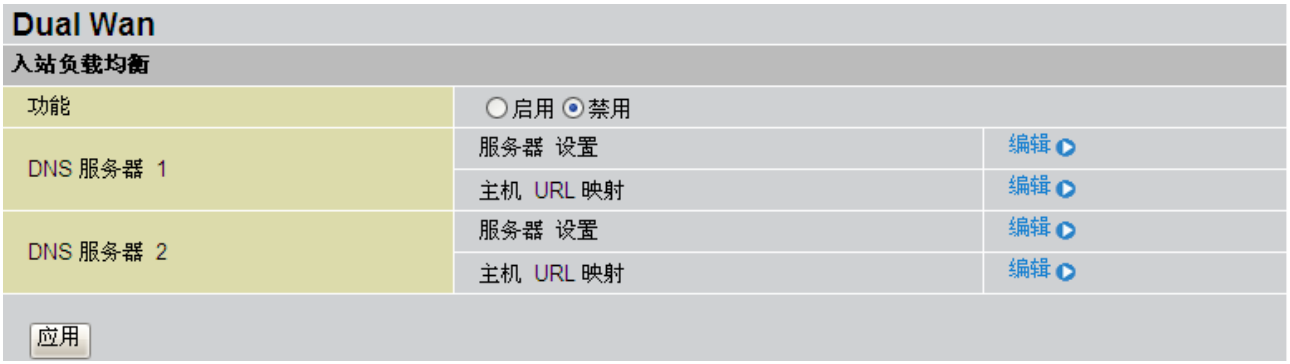
6.4. DNS 入站失效切换



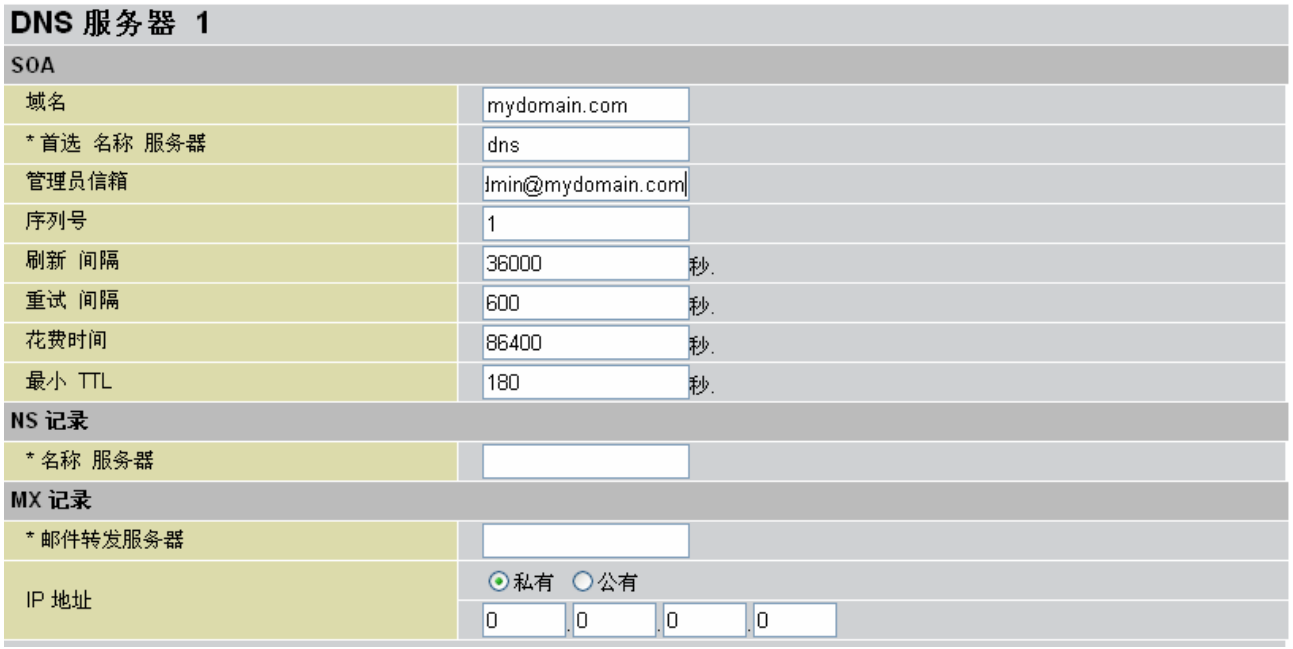
在配置前，请确认 WAN1 和 WAN2 已经配置好。

Step 1：配置->Dual WAN->一般设置，选择“**失效切换**”；

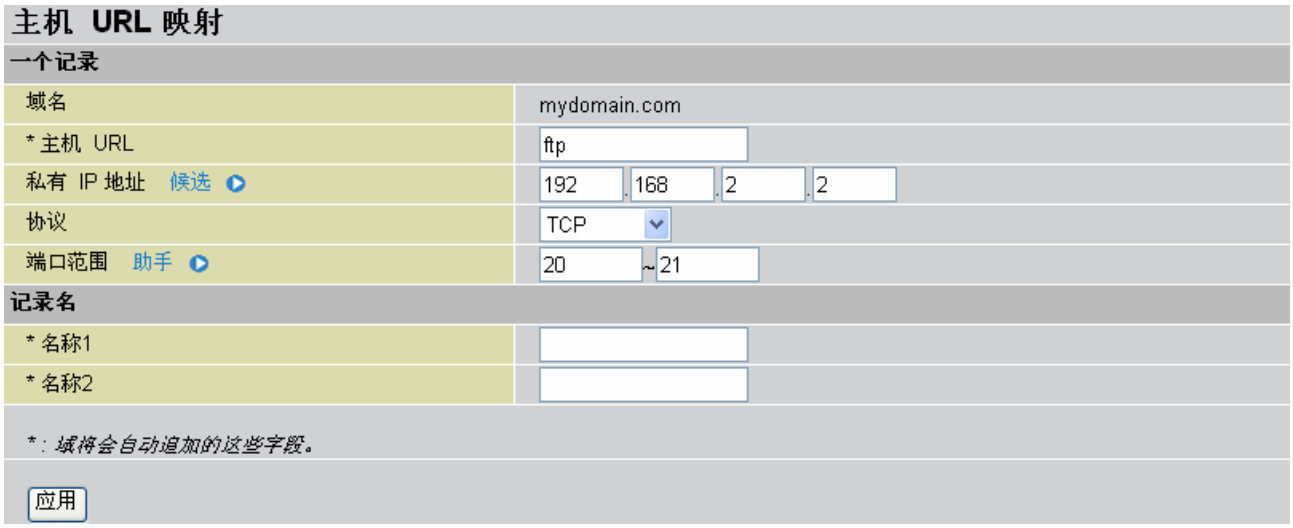
Step 2：配置->Dual WAN->入站负载均衡， 选择“**启用**”并点击“**编辑**”配置 DNS 服务器；



Step 3：配置 DNS 服务器 1，并点击“**应用**”；

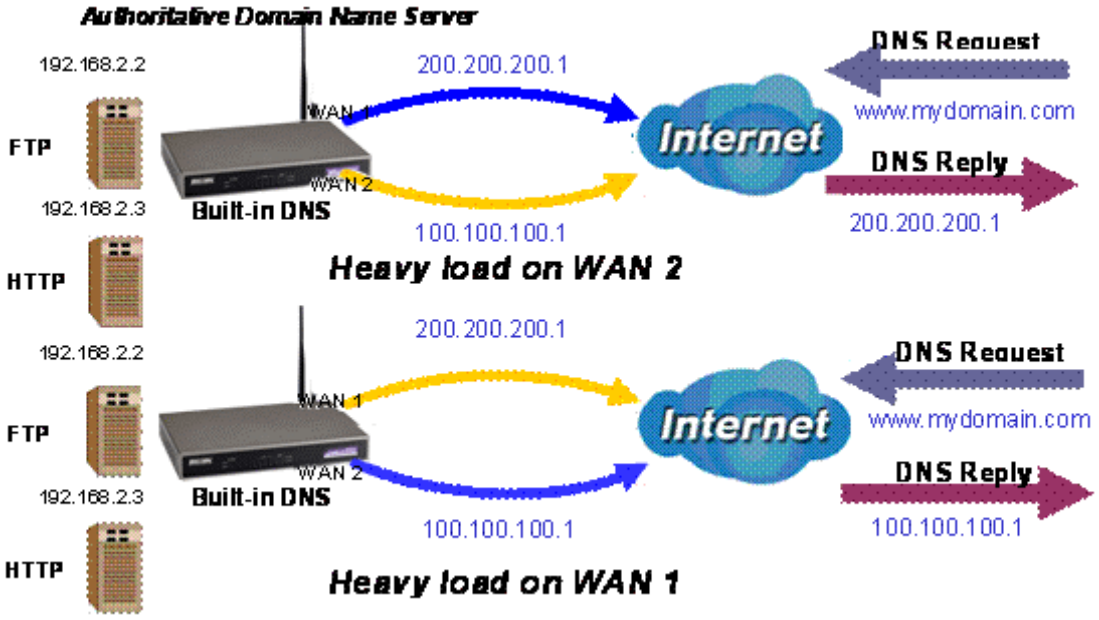


Step 4: 配置主机 **URL** 映射，点击“**编辑**”进入主机 URL 映射配置；



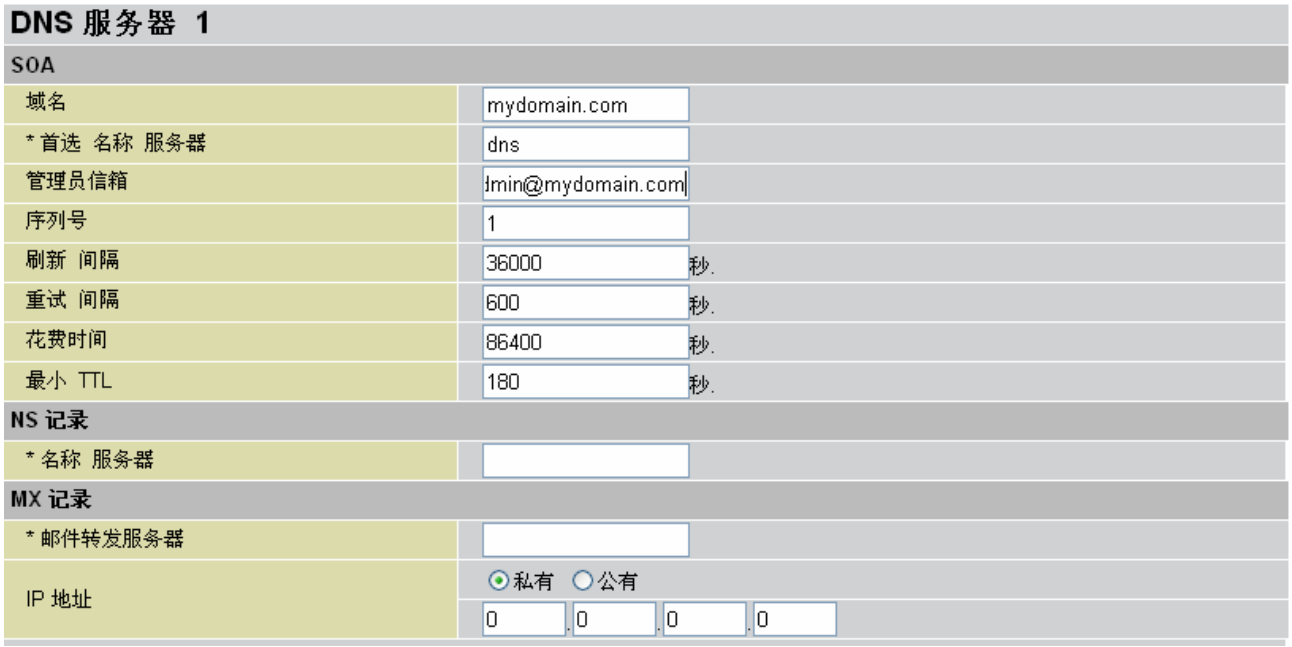
Step 5：点击“**保存**”保存配置到闪存；

6.5. DNS 入站负载均衡

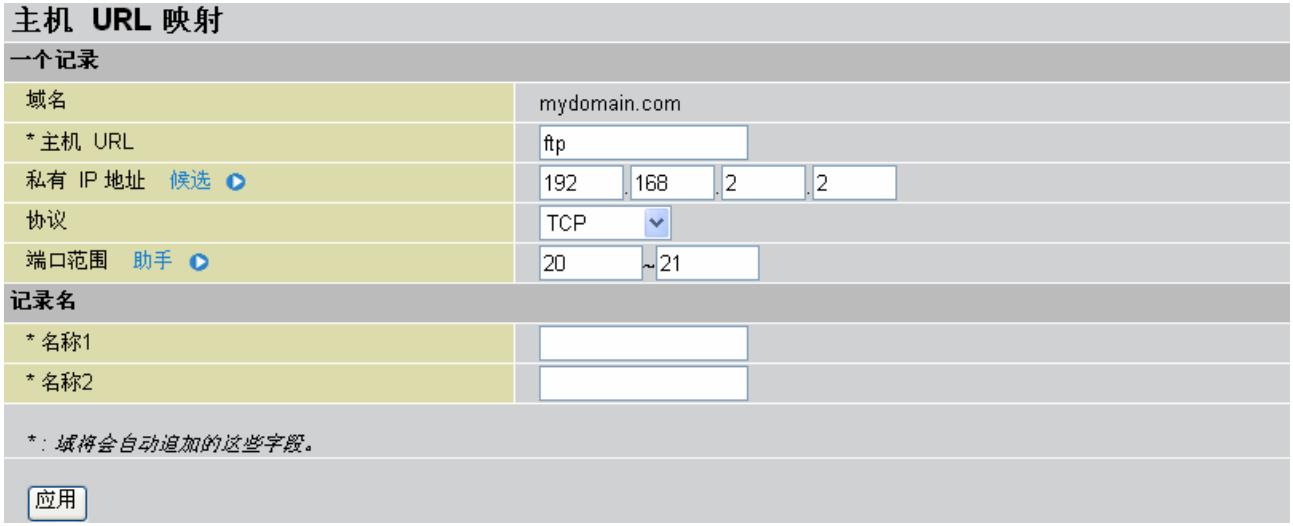


Step 1：配置->Dual WAN->一般设置，选择“负载均衡”；

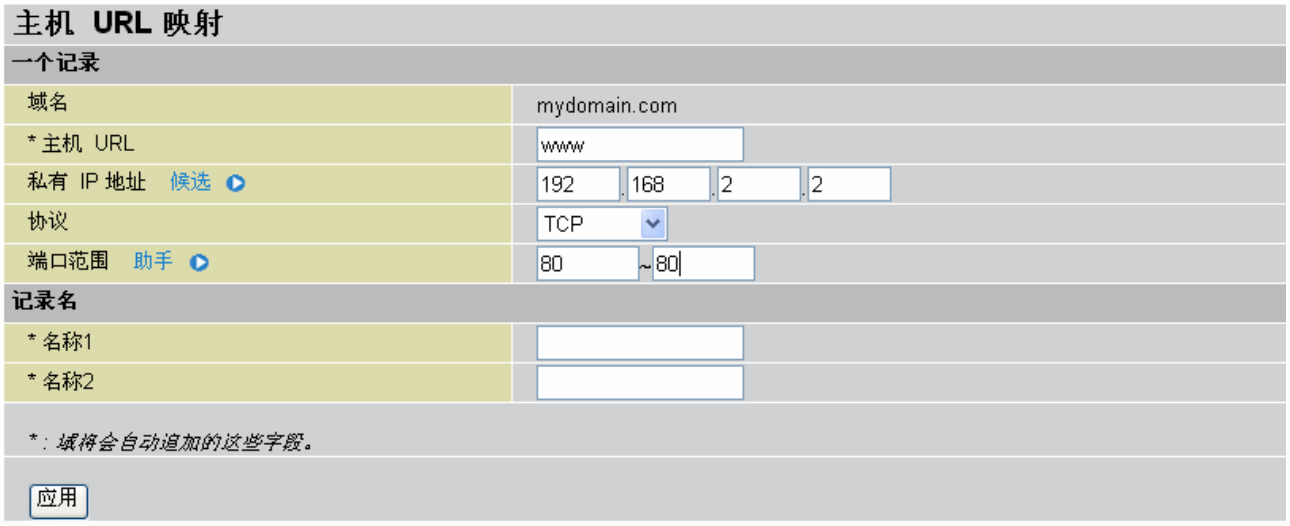
Step 2: 配置-> Dual WAN->入站负载均衡->DNS 服务器配置；



Step 3：配置->Dual WAN ->入站负载均衡->主机 URL 映射，并配置 FTP 映射；



Step 4：配置主机 URL 映射；



Step 5：点击“**保存**”保存配置到闪存；

6.6. 动态 DNS 入站负载均衡

Step 1: 配置-> WAN ->带宽设置，配置WAN的出站与入站带宽；

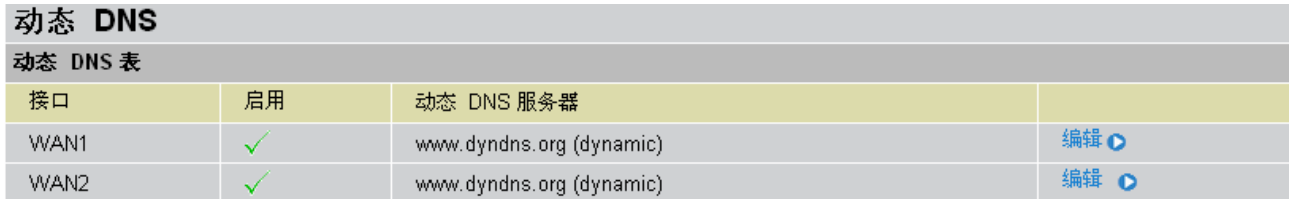
带宽 设置			
由你的ISP提供的最大带宽			
WAN 1	出站 带宽	102400	kbps
	入站 带宽	102400	kbps
WAN 2	出站 带宽	102400	kbps
	入站 带宽	102400	kbps
(⚠ *这些带宽设置将会被Qos和负载平衡功能引用*)			
应用			

Step 2: 配置-> Dual WAN ->一般设置，选择“**负载均衡**”模式，你可以选择“**服务侦测**”模式是否启用；

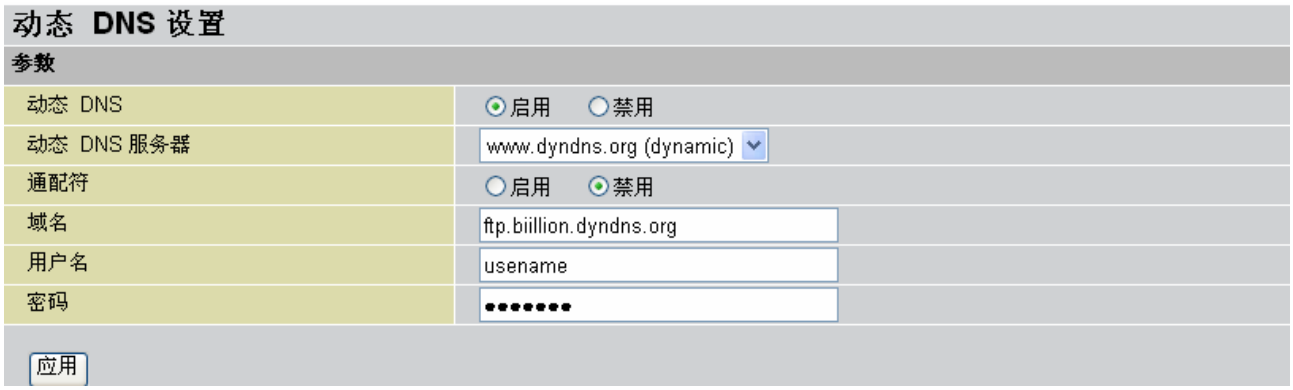
一般设置	
Dual WAN 模式	
模式	○ 负载均衡 ◉ 失效切换
WAN端口服务侦测策略	
服务 侦测 (为 负载均衡.)	○ 启用 ○ 禁用
连接决策	探测失败后不提供服务满足 3 连接次数.
探测 周期	每 30 秒.
探测 WAN1	◉ 网关
	○ 主机 0.0.0.0
探测 WAN2	◉ 网关
	○ 主机 0.0.0.0
可能时回切到WAN1 (对于失效切换)	○ 启用
	◉ 禁用
应用	

Step 3: 配置->Dual WAN ->出站负载均衡，选择“负载均衡策略”；

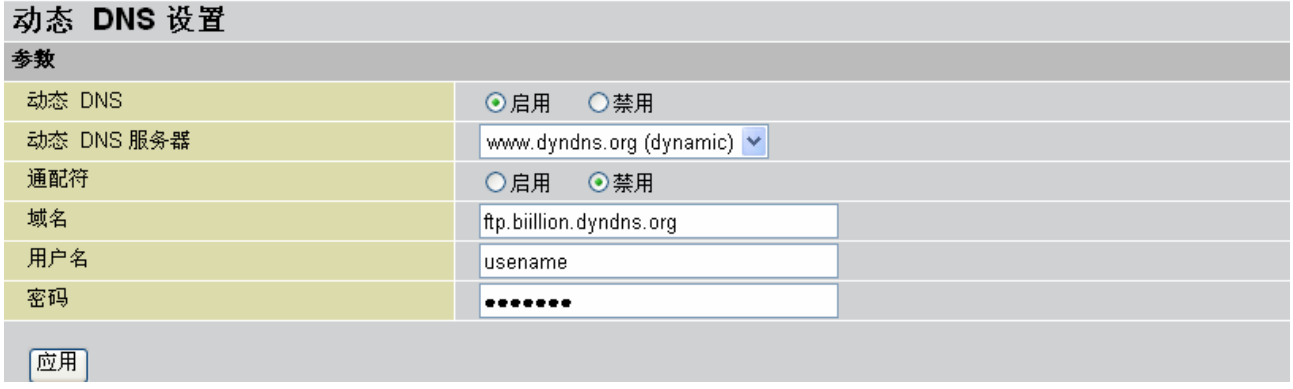
Step 4: 配置->高级->动态 DNS，为 WAN1 和 WAN2 分别配置动态 DNS；



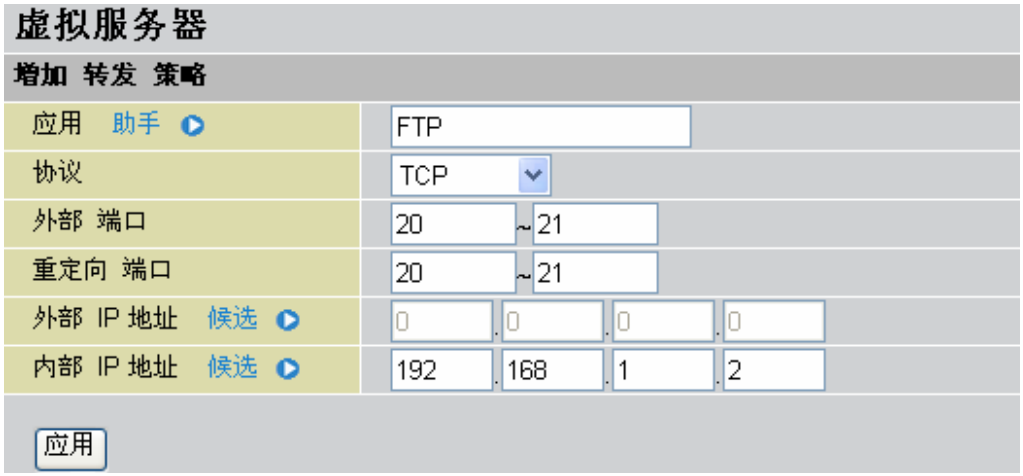
WAN1:

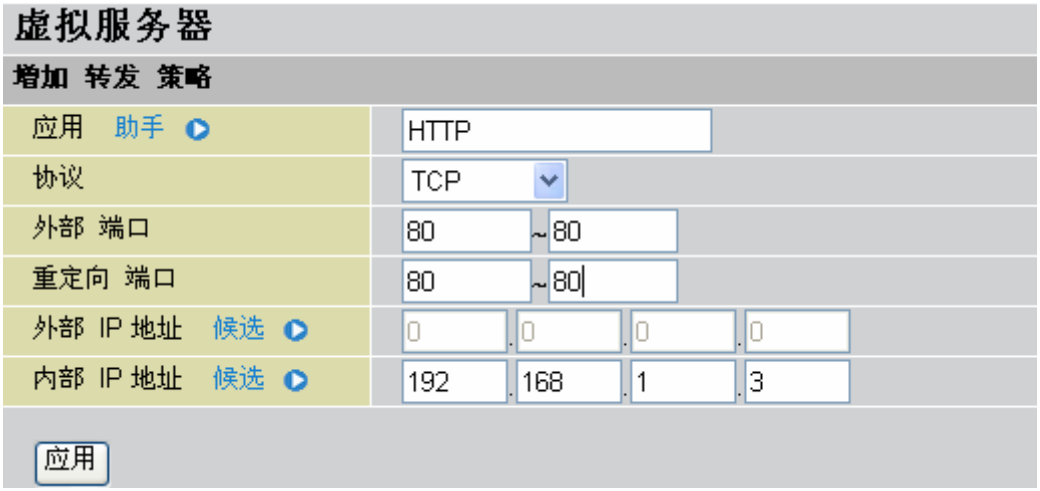


WAN 2:



Step 5: **配置->虚拟服务器**，为 FTP 与 HTTP 的应用建立虚拟的服务器；



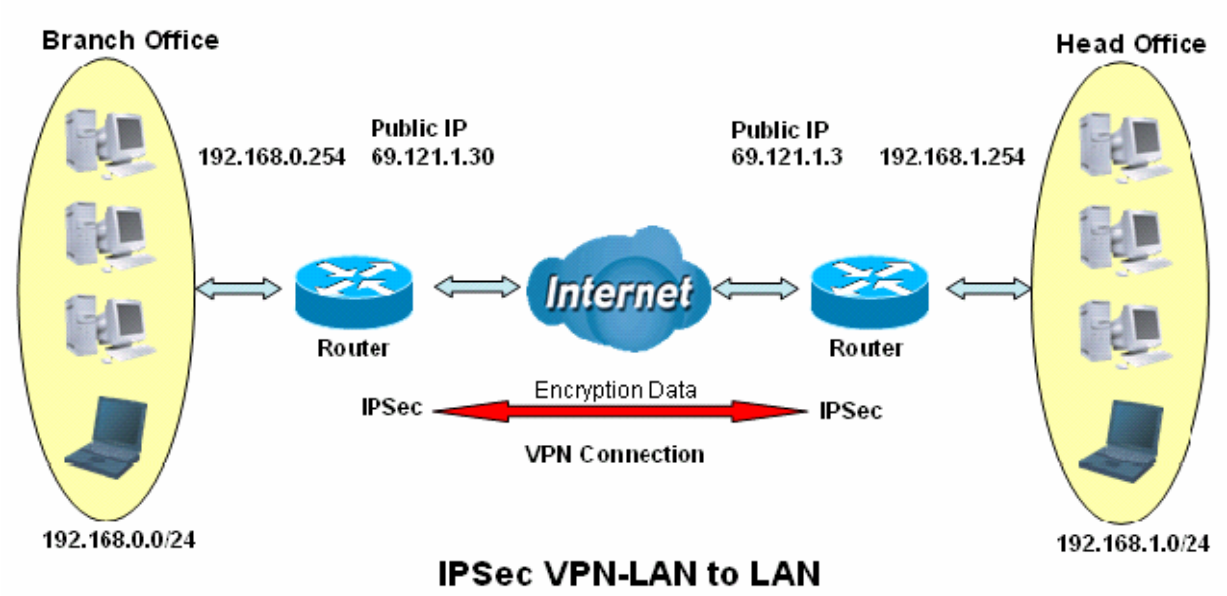


Step 6: 点击“**保存**”保存配置到闪存；

6.7. VPN 配置

这个案例将如何教会为 BiGuard 50G 配置 VPN 通道；

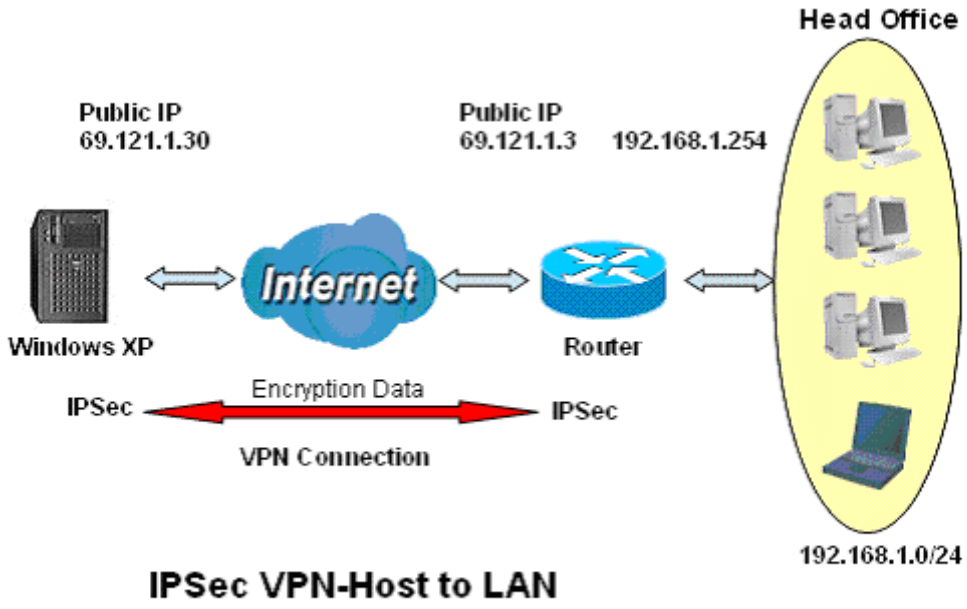
6.7.1 LAN TO LAN



	Branch Office	Head Office
本地		
ID	IP 地址	IP 地址
数据	69.121.1.30	69.121.1.3
网络	任何本地地址	任何本地地址
IP 地址	192.168.0.0	192.168.1.0
子网掩码	255.255.255.0	255.255.255.0

远程		
安全网关地址（或主机名）	69.121.1.3	69.121.1.30
ID	IP 地址	IP 地址
数据	69.121.1.3	69.121.1.30
网络	子网	子网
IP 地址	192.168.1.0	192.168.0.0
子网掩码	255.255.255.0	255.255.255.0

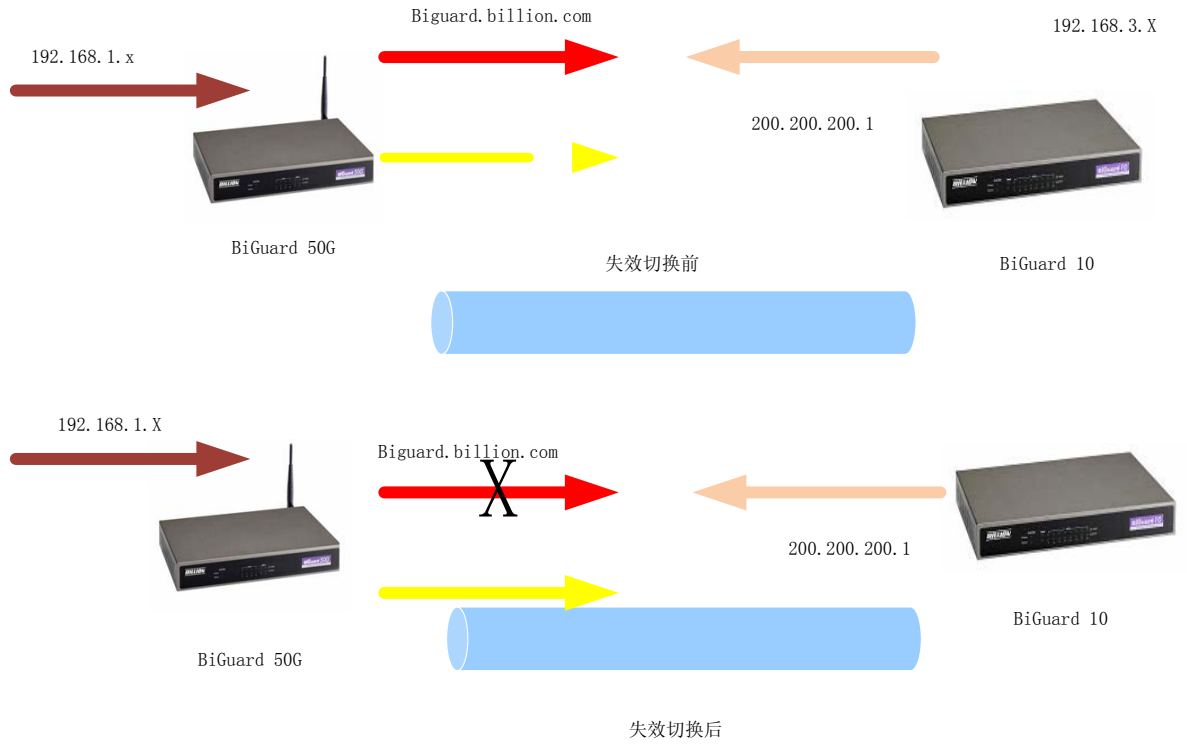
6.7.2Host TO LAN



IPSec VPN-Host to LAN

	Single client	**Head Office**
本地		
ID	IP 地址	IP 地址
数据	69.121.1.30	69.121.1.3
网络	任何本地地址	任何本地地址
IP 地址	0.0.0.0	192.168.1.0
子网掩码	0.0.0.0	255.255.255.0
远程		
安全网关地址（或主机名）	69.121.1.3	69.121.1.30
ID	IP 地址	IP 地址
数据	69.121.1.3	69.121.1.30
网络	子网	单个地址
IP 地址	192.168.1.0	69.121.1.30
子网掩码	255.255.255.0	255.255.255.0

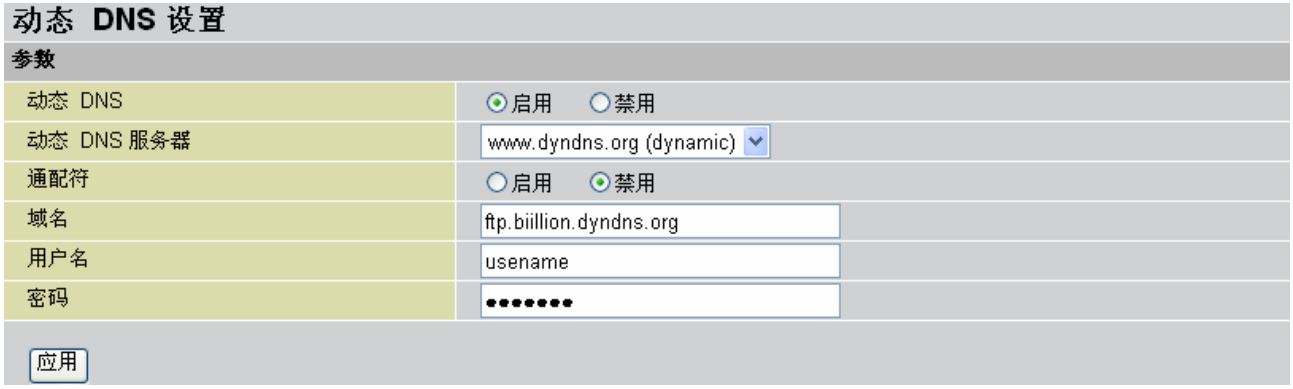
6.8. IPSec 失效切换（网关到网关）



Step 1: 配置->Dual WAN->一般设置，选择“**失效切换**”，然后配置失效切换策略；

一般设置	
Dual WAN 模式	
模式	○ 负载均衡 ◉ 失效切换
WAN端口服务侦测策略	
服务 侦测 (为 负载均衡.)	○ 启用 ○ 禁用
连接决策	探测失败后不提供服务满足 3 连接次数.
探测 周期	每 30 秒.
探测 WAN1	○ 网关
	◉ 主机 168 . 95 . 192 . 1
探测 WAN2	○ 网关
	◉ 主机 168 . 95 . 1 . 1
可能时回切到WAN1 (对于失效切换)	◉ 启用
	○ 禁用
应用	

Step 2: 配置->高级->动态 DNS，为 WAN1 和 WAN2 配置动态 DNS；



Step 3: 配置->VPN->IPSec->IPSec 策略，点击“创建”；

Step 4: 点击“保存”保存配置到闪存，配置对端网关；

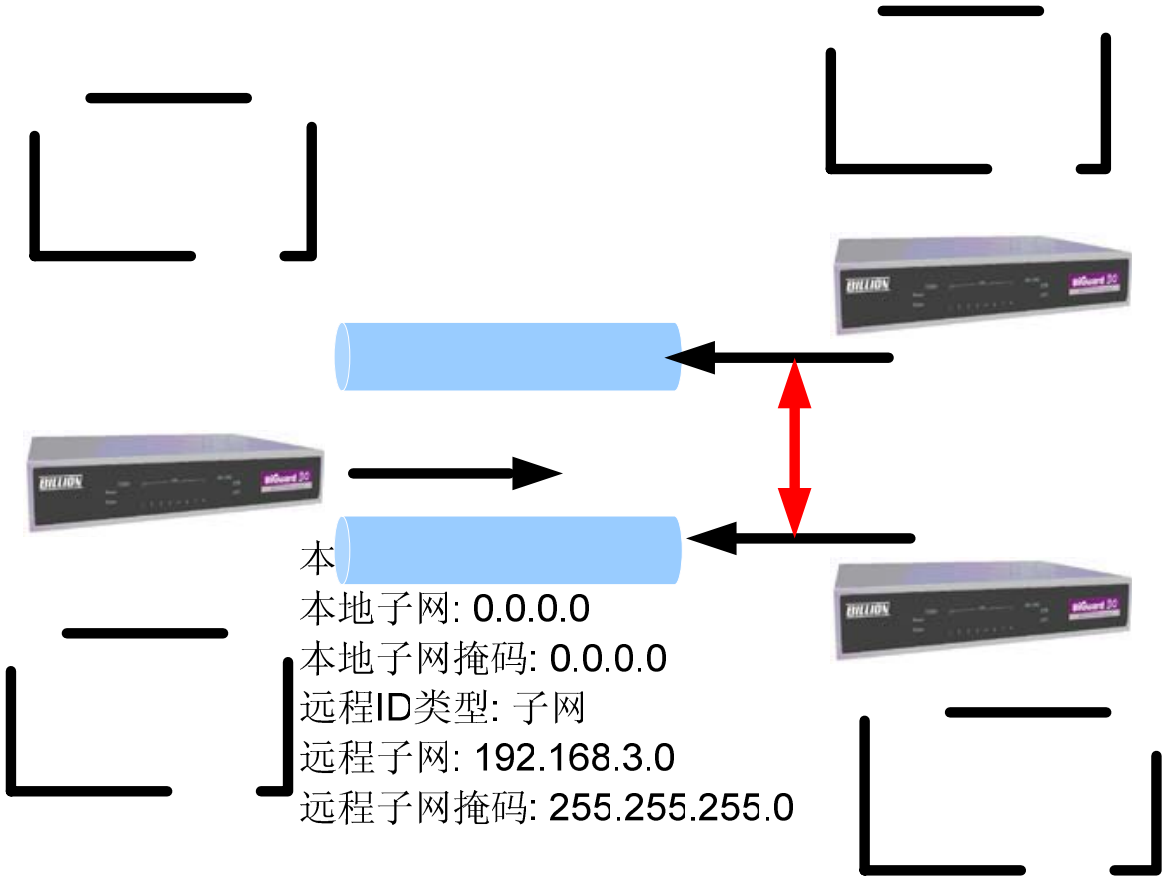
IPSec

创建

连接 名称	biguard		
通道	◉ 已启用 ○ 已禁用		
接口	○ WAN1 ○ WAN2 ◉ 自动		
本地			
ID	IP 地址	数据	200.200.200.1
网络	子网	IP 地址	192 . 168 . 3 . 0
		结束 IP 地址	0 . 0 . 0 . 0
		网络掩码	255 . 255 . 255 . 0
远程			
安全网关	IP 地址/ 主机名	数据	biguard.billion.com
ID	FQDN (DNS)	数据	biguard.billion.com
网络	子网	IP 地址	192 . 168 . 2 . 0
		结束 IP 地址	0 . 0 . 0 . 0
		网络掩码	255 . 255 . 255 . 0
建议			

安全联合	◉ 主模式 ○ 积极模式 ○ 手动密钥
方法	◉ ESP ○ AH
加密 协议	3DES
认证 协议	MD5
完美向前保密	◉ 已启用 ○ 已禁用
预共享 密钥	12345678
IKE 生存时间	28800 秒
密钥 生存时间	3600 秒
Netbios 广播	○ 已启用 ◉ 已禁用
DPD 设置	
DPD 功能	○ 已启用 ◉ 已禁用
侦测 间隔	30 秒;
空闲超时	4 连接次数

6.9. VPN HUB



Step 1: 配置->VPN ->IPSec ->IPSec 策略；

IPSec			
创建			
连接 名称	test1		
通道	◉ 已启用 ○ 已禁用		
接口	○ WAN1 ○ WAN2 ◉ 自动		
本地			
ID	IP 地址	数据	100.100.100.1
网络	子网	IP 地址	0 . 0 . 0 . 0
		结束 IP 地址	0 . 0 . 0 . 0
		网络掩码	0 . 0 . 0 . 0
远程			
安全网关	IP 地址/ 主机名	数据	200.200.200.1
ID	远程 WAN IP	数据	biguard.billion.com
网络	子网	IP 地址	192 . 168 . 3 . 0
		结束 IP 地址	0 . 0 . 0 . 0
		网络掩码	255 . 255 . 255 . 0
建议			

本地子网掩码: 0.0.0.0
远程ID类型: Subnet
远程子网: 192.168.4.0
远程子网掩码: 255.255.255.0

安全联合	◉主模式 ○积极模式 ○手动密钥
方法	◉ ESP ○ AH
加密 协议	3DES
认证 协议	MD5
完美向前保密	◉ 已启用 ○ 已禁用
预共享 密钥	12345678
IKE 生存时间	28800 秒
密钥 生存时间	3600 秒
Netbios 广播	○ 已启用 ◉ 已禁用
DPD 设置	
DPD 功能	○ 已启用 ◉ 已禁用
侦测 间隔	30 秒;
空闲超时	4 连接次数

Step 2: 配置-> VPN-> IPSec-> IPSec策略，配置 50G 与 BiGuard 10 之间的连接；

IPSec

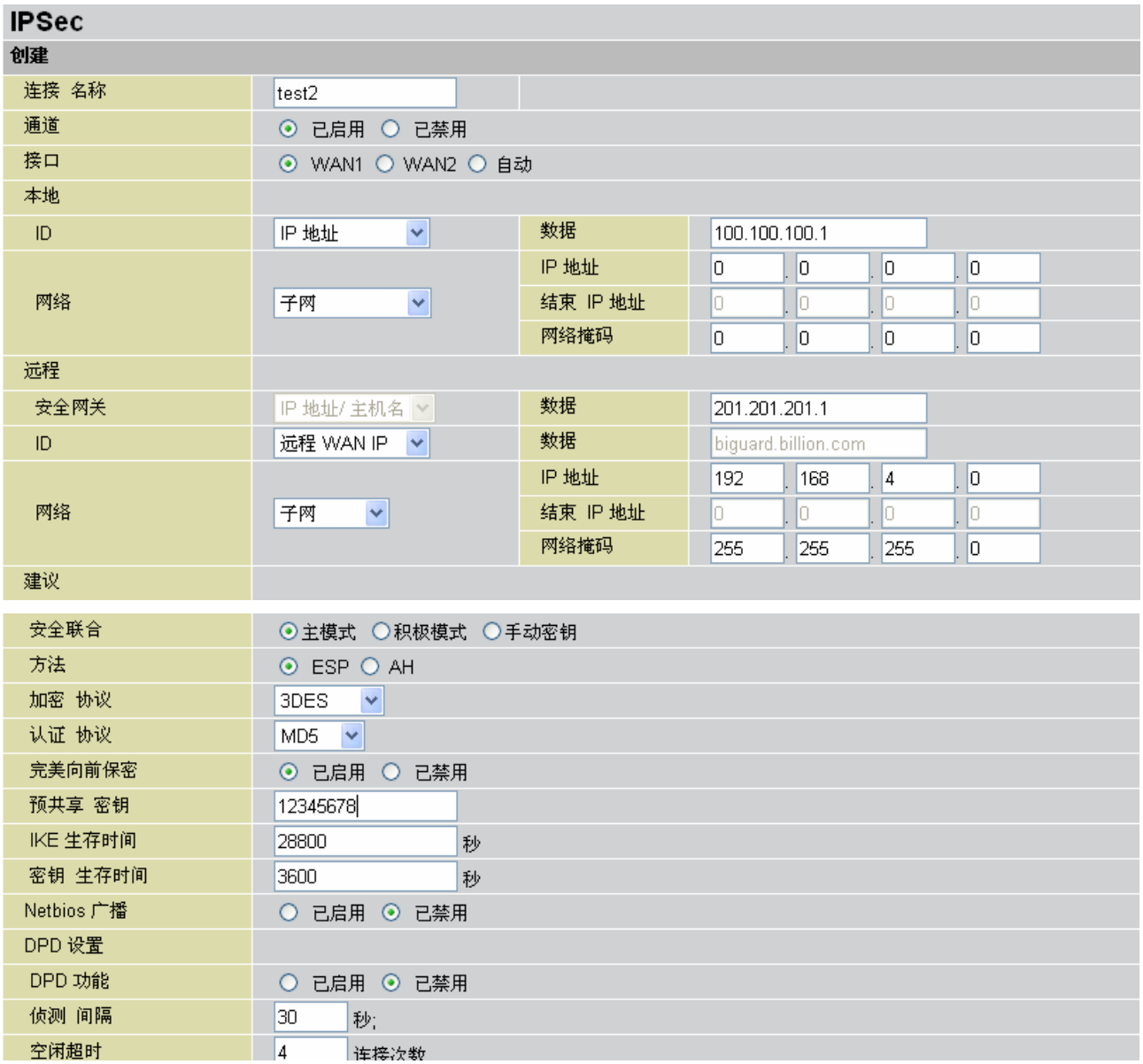
创建

连接 名称	test2		
通道	◉ 已启用 ○ 已禁用		
接口	◉ WAN1 ○ WAN2 ○ 自动		
本地			
ID	IP 地址	数据	100.100.100.1
网络	子网	IP 地址	0 . 0 . 0 . 0
		结束 IP 地址	0 . 0 . 0 . 0
		网络掩码	0 . 0 . 0 . 0
远程			
安全网关	IP 地址/ 主机名	数据	201.201.201.1
ID	远程 WAN IP	数据	biguard.billion.com
网络	子网	IP 地址	192 . 168 . 4 . 0
		结束 IP 地址	0 . 0 . 0 . 0
		网络掩码	255 . 255 . 255 . 0
建议			

安全联合	◉主模式 ○积极模式 ○手动密钥
方法	◉ ESP ○ AH
加密 协议	3DES
认证 协议	MD5
完美向前保密	◉ 已启用 ○ 已禁用
预共享 密钥	12345678
IKE 生存时间	28800 秒
密钥 生存时间	3600 秒
Netbios 广播	○ 已启用 ◉ 已禁用
DPD 设置	
DPD 功能	○ 已启用 ◉ 已禁用
侦测 间隔	30 秒;
空闲超时	4 连接次数

Step 3: 配置->VPN ->IPSec ->IPSec 策略，然后配置 BiGuard 10 与 BiGuard 50G 之间的连接(Branch A)；

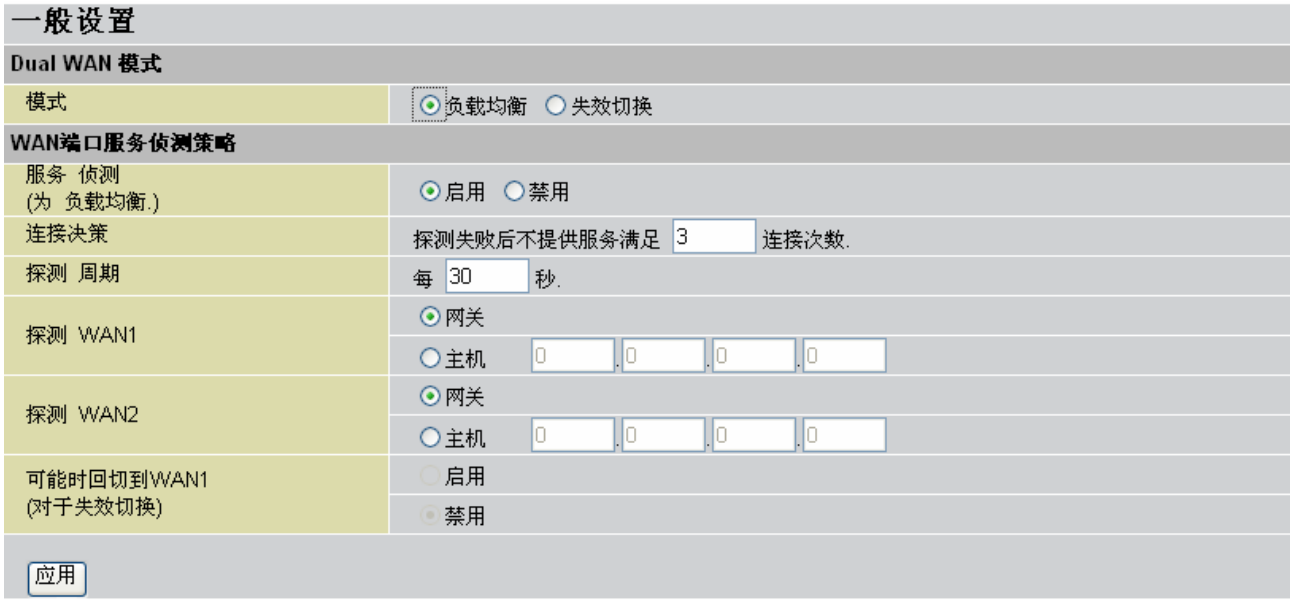
Step 4: 配置-> VPN-> IPSec -> IPSec策略，然后配置 BiGuard 10 与 BiGuard 50G 之间的连接（Branch B）；



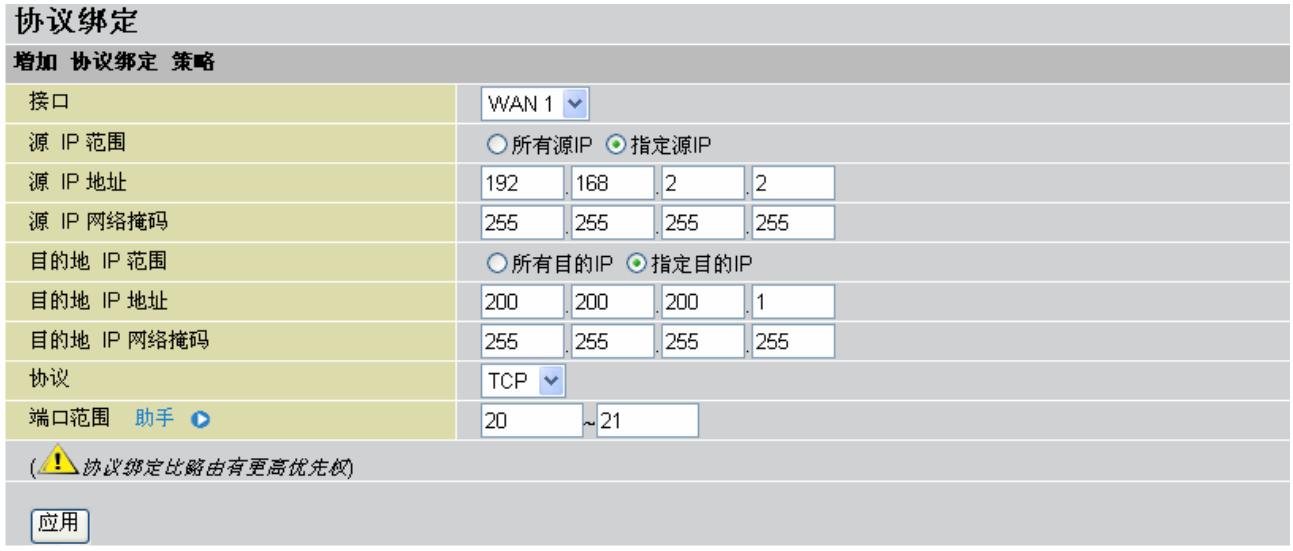
Step 5: 点击“**保存**”保存配置到闪存；

6.10. 协议绑定

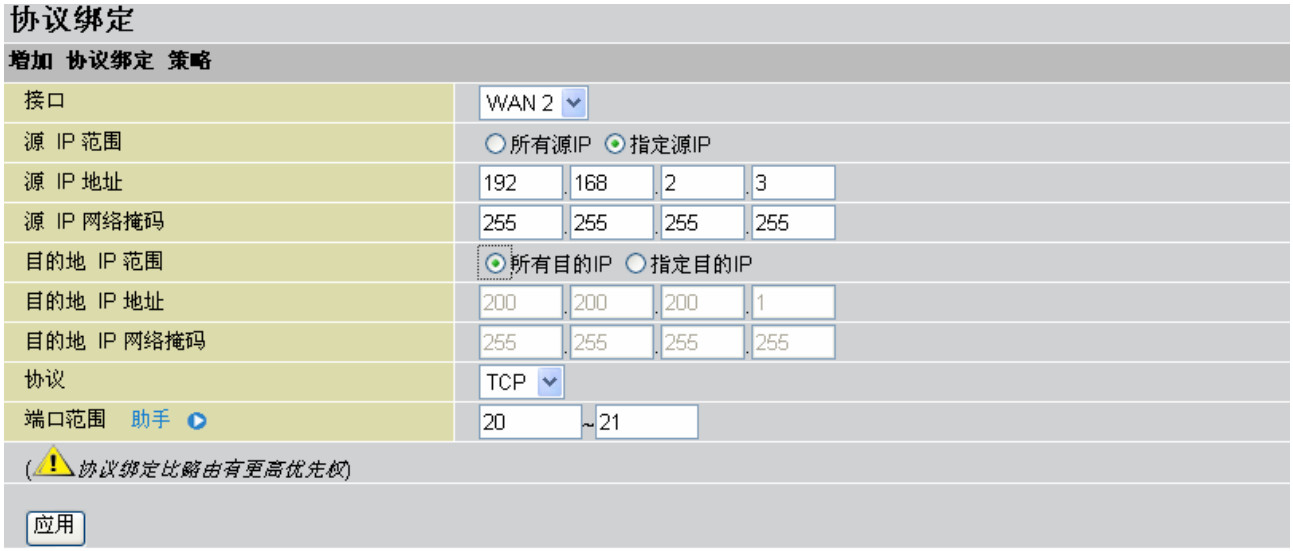
Step 1: 配置-> Dual WAN->一般设置，选择“负载均衡”；



Step 2: 配置-> Dual WAN->协议绑定，配置 WAN1 口的协议绑定；

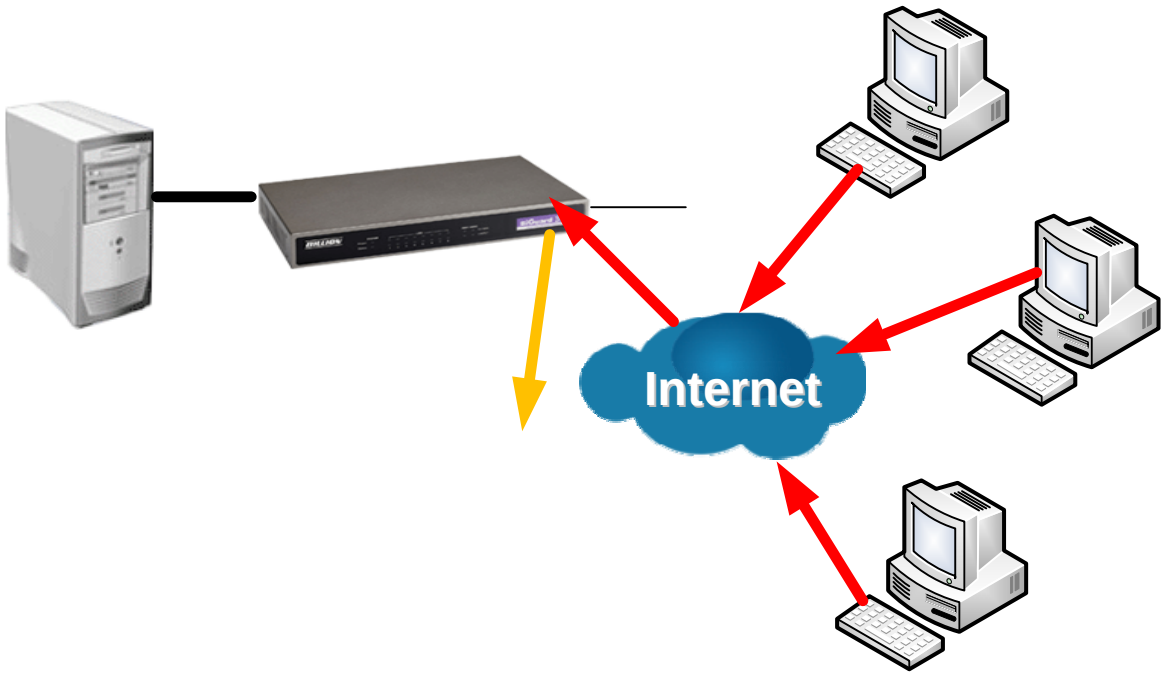


Step 3: 配置-> Dual WAN->协议绑定，配置 WAN2 口的协议绑定；



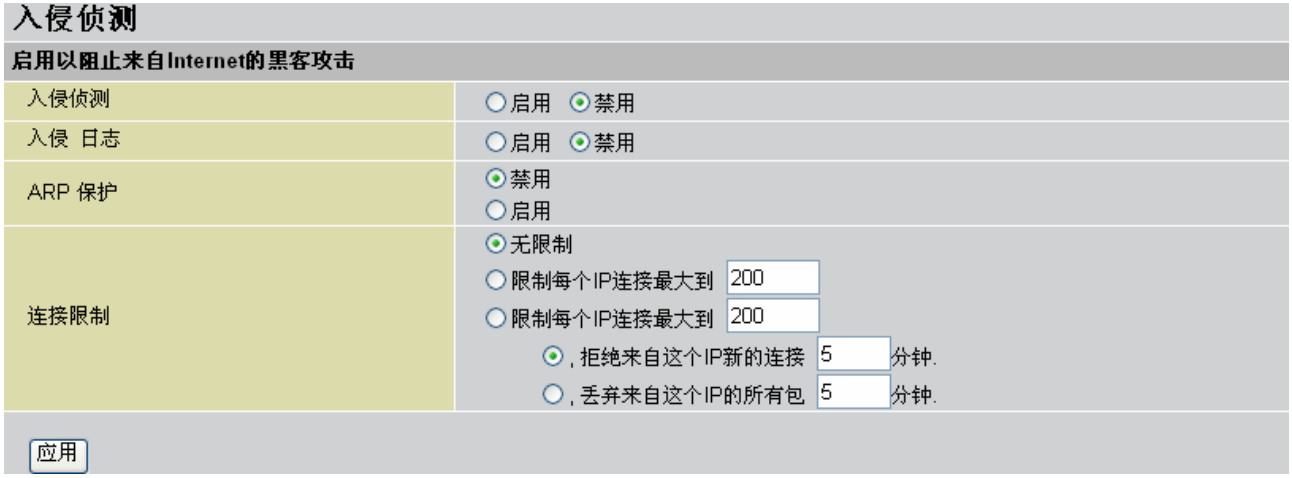
Step 4: 点击“**保存**”保存配置到闪存；

6.11. 入侵侦测



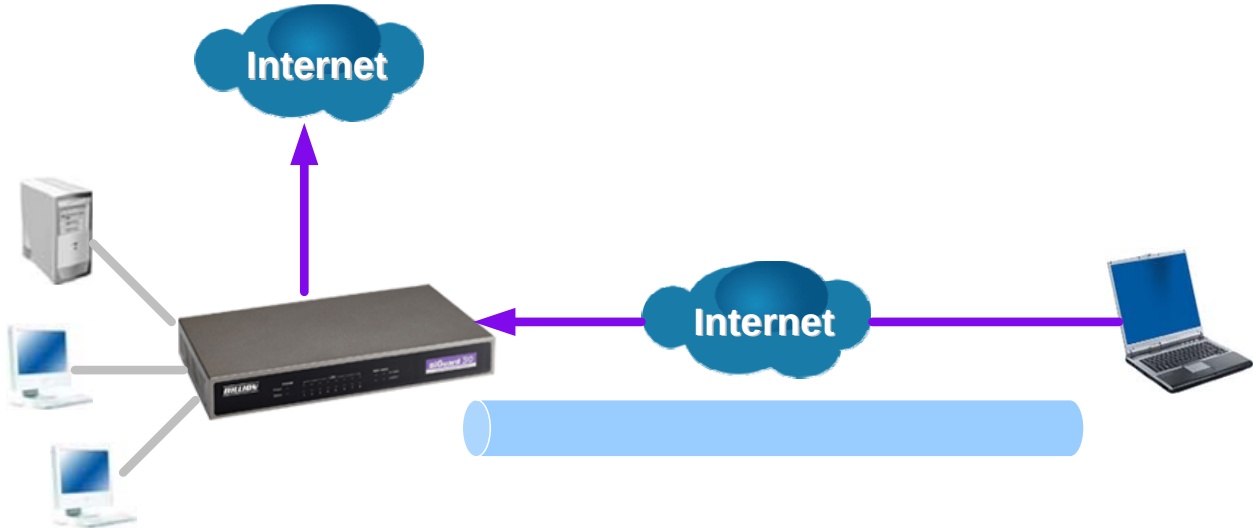
服务器定义

Step 1: **配置->防火墙->入侵侦测**，并启用该功能；



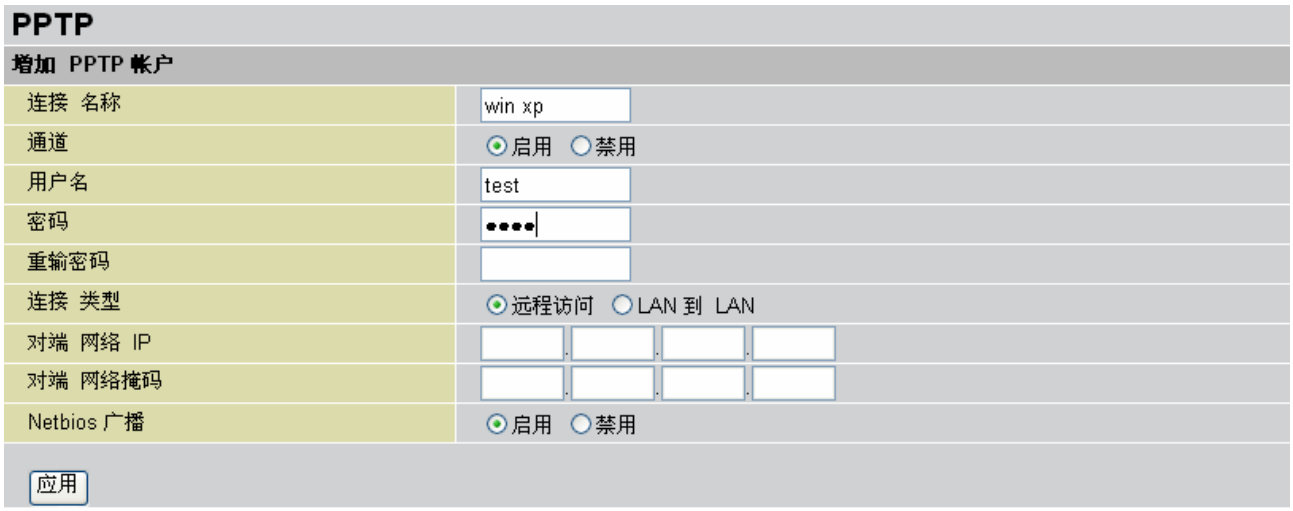
Step 2: 点击“**应用**”并“**保存**”保存配置到闪存；

6.12. PPTP（WINDOWS XP 系统用户的远端连接）



Step1: 配置-> VPN-> PPTP，设置 PPTP 功能，并点击“**应用**”；

Step2: 点击“**创建**”，创建 PPTP 帐户；



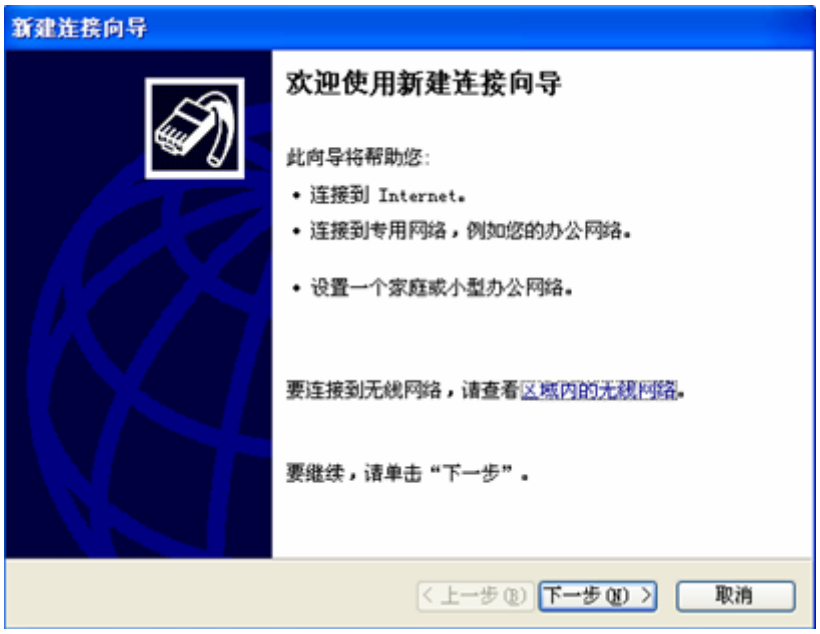
Step3: 点击“**应用**”，可以看见已经成功申请了 PPTP 帐户；

Step4: 点击“**保存**”保存配置到闪存；

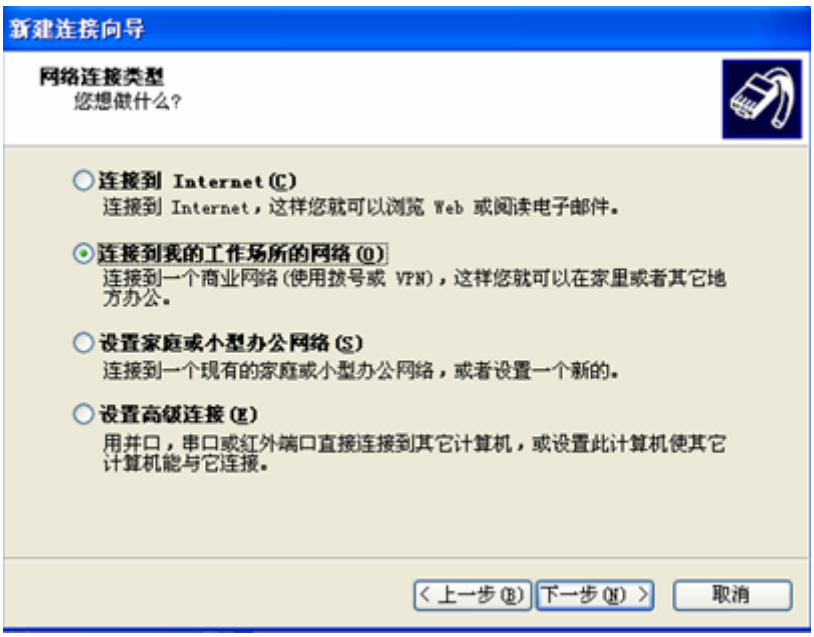
Step5: 在 WINDOWS 操作系统里面，**配置开始->设置->网络连接；**


vivian
电子邮件
Outlook Express
Internet Explorer
命令提示符
Microsoft Office PowerPoint 2003
Microsoft Office Word 2003
腾讯QQ
Microsoft Office Excel 2003
所有程序(P)
我的文档
我最近的文档(D)
图片收藏
我的音乐
我的电脑
网上邻居
控制面板(C)
设定程序访问和默认值
连接到(T)
打印机和传真
帮助和支持(H)
搜索(S)
运行(R)...
注销(L)
关闭计算机(U)
11
Standalone Network Extender
无线网络连接
显示所有连接(S)

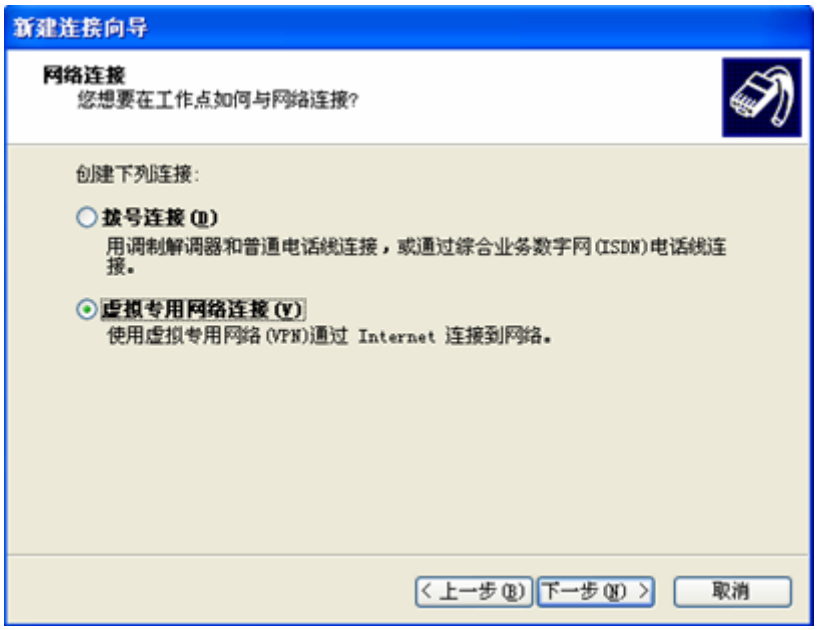
Step6: 在**“网络任务”**里面，点击**“创建一个新连接”**；



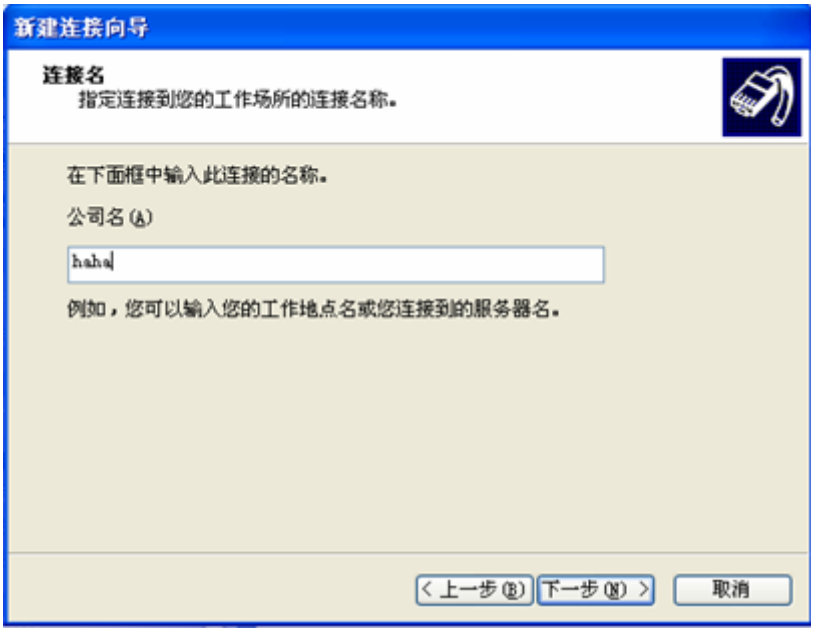
Step7: 选择**“连接到我的工作场所的网络”**；



Step8: 选择“**虚拟专用网络连接**”；

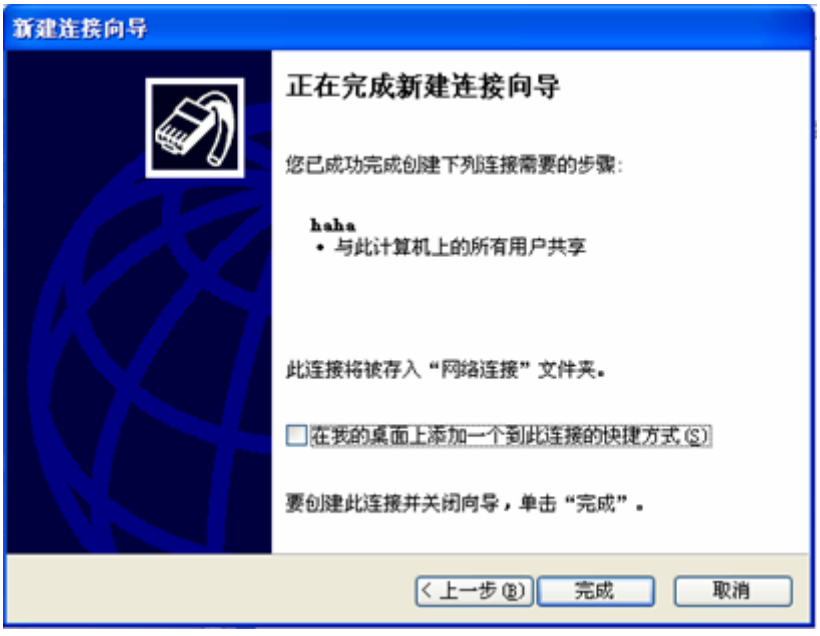


Step9: 输入**“连接名”；**



Step10: 输入**“主机名或者 IP 地址”；**

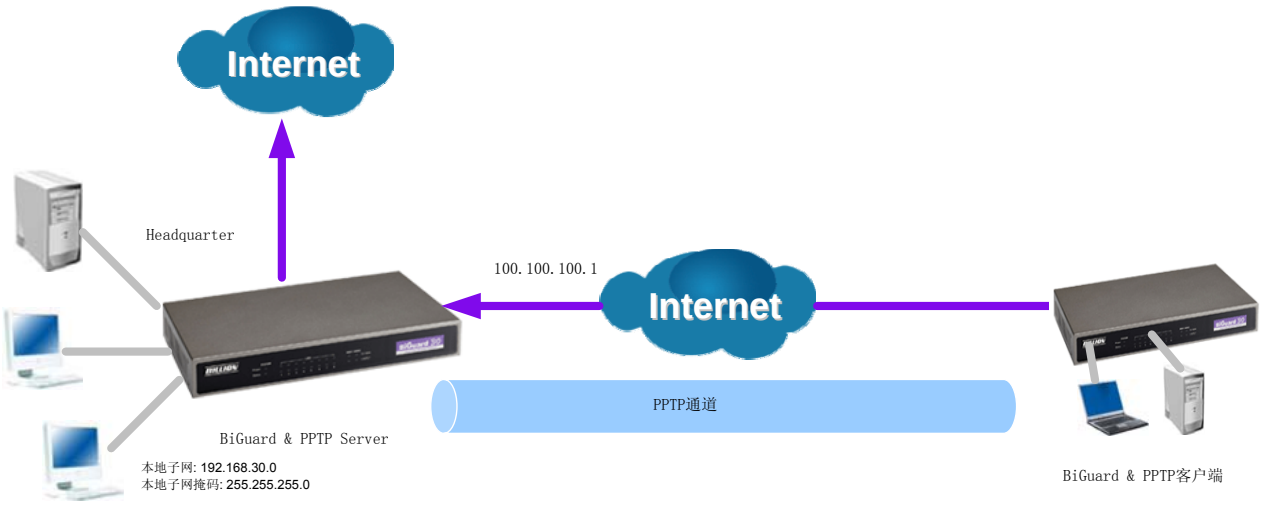
Step11: 点击**“完成”；**



Step12: 输入**“用户名”**和**“密码”**；

Step13: 点击**“属性”**，可以看见目的主机的 IP 地址或者主机名；

6.13. PPTP（用 BiGuard 远端连接）



Step1: 配置-> VPN -> PPTP，配置 PPTP 功能，禁用加密之后点击**“应用”**

PPTP

一般设置

PPTP 功能	启用 禁用
认证类型	Pap 或 Chap
数据 加密	启用
加密 密钥 长度	自动
对端 加密 模式	只在无状态时
双方分配到的IP地址	开始于: 192.168.1. 200
空闲超时	0 最小.

(*启用数据加密将使用MS-CHAPv2来对双方认证。*)

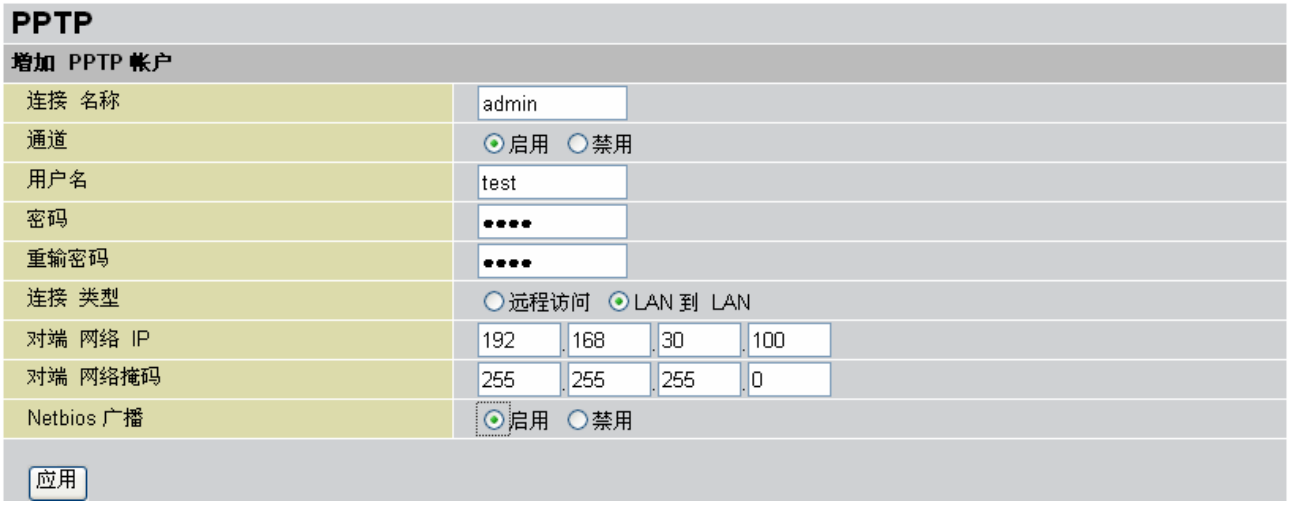
应用

帐户 设置

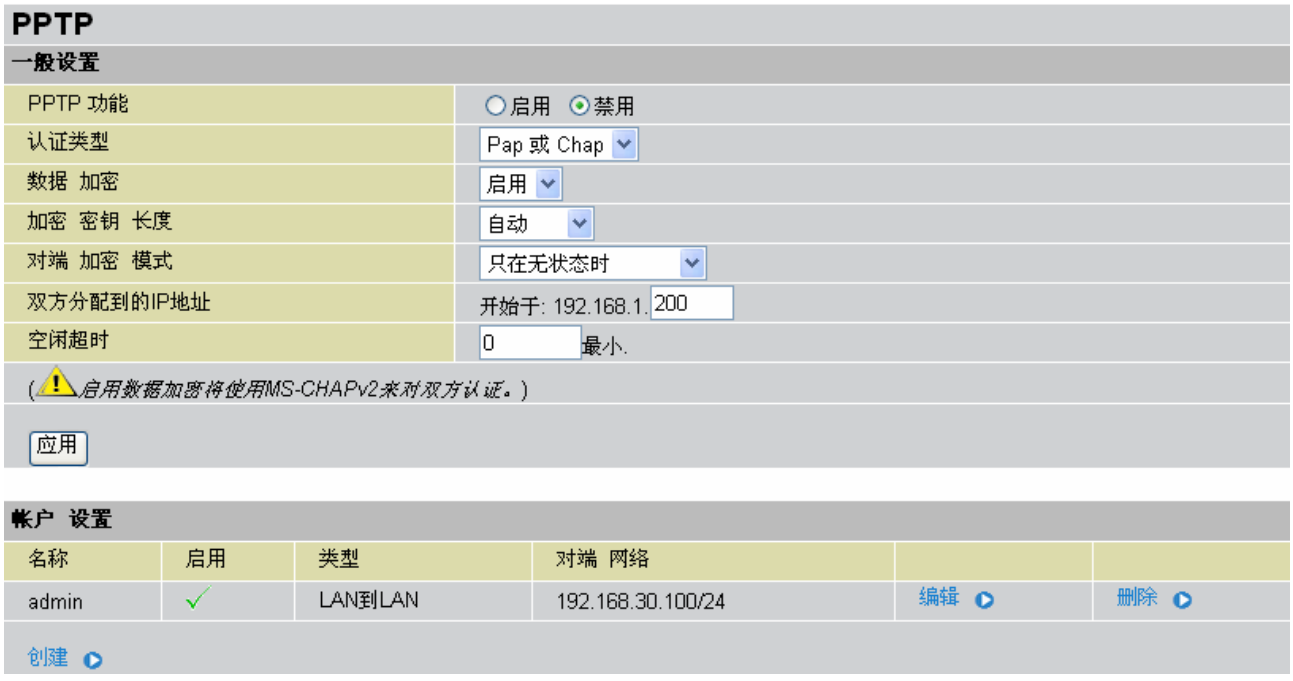
名称	启用	类型	对端 网络		

创建

Step2: 点击“**创建**”，创建一个帐户；

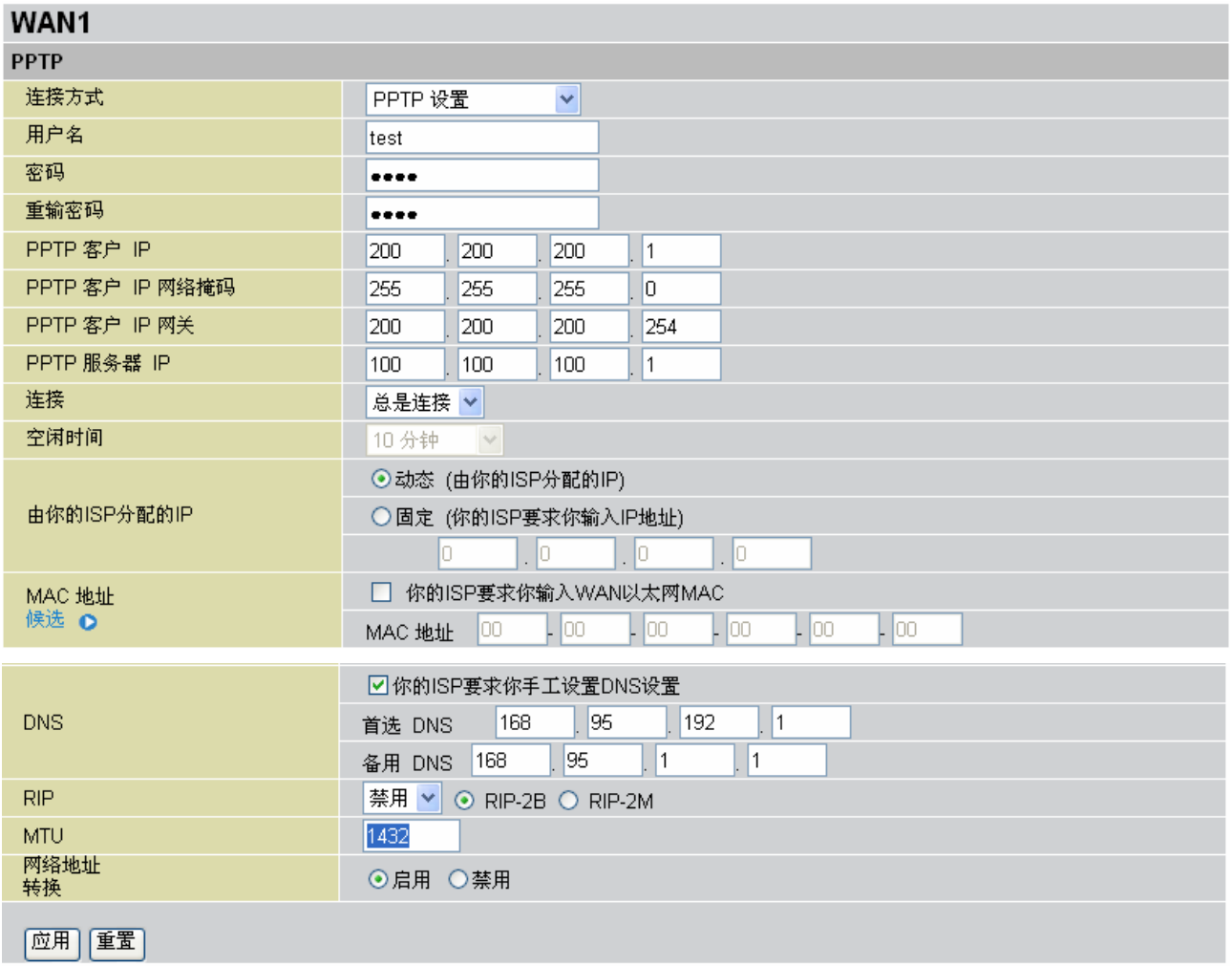


Step3: 点击“**应用**”，可以看见帐户已经成功申请；



Step4: 点击“**保存**”保存配置到闪存；

Step5: 另一台 BiGuard 作为客户端，**配置-> WAN ->设置；**



Step6: 点击“**保存**”保存配置到闪存；

7. 缩略语

AES：Advanced Encryption Standard --高级加密标准
AH：Authentication Head --验证头
ARP：Address Resolution Protocol --地址解析协议
DHCP：Dynamic Host Configuration Protocol --动态主机配置协议
DES：Data Encryption Standard --数据加密标准
DNS：Dnomain Name System --域名系统
DMZ：Demilitarized Zone --非军事区域
ESP：Encapsulating Security Payload --封装安全负荷
ICMP：Internet Control Management Protocol --互联网控制管理协议
IP：Internet Protocol --互联网协议
IPsec：IP security --互联网协议安全

ISP：Internet Service Provider --互联网服务提供商
LAN：Local Area Network --局域网
MD5：Message Digest 5 --信息摘要 5
NAT：Network Address Translation --网络地址转换协议
QoS：Quality of Service --服务质量
RIP-2：Route Infomation Protocol 2 --路由信息协议第二版本
SA：Security Association --安全联合
SHA：Standard Hash Algorithm --标准散列算法
SNMP：Simple Network Management Protocol --简单网络管理协议
PPP：Point-to-Point Protocol --点对点协议
PPTP：PPP Tunnel Protocol --点到点隧道协议
PPPoE：PPP Over Ethernet --以太网上的点对点协议
TCP：Transport Control Protocol --传输控制协议
UDP：User Datagram Protocol --用户数据报协议
VPN：Virtual Private Network --虚拟专用网络
WAN：Worldwide Area Network --广域网