Hillstone 山石网科多核安全网关

基础配置手册

version 5.0

www.hillstonenet.com.cn

目录

关于本手册

手册内容

本手册为 Hillstone 山石网科多核安全网关的基础配置手册，对 Hillstone 山石网科多核安全网关的主要功能模块配置进行介绍，帮助用户快速掌握安全网关的 WebUI 配置。适用于 StoneOS 5.0 以及以上版本。具体内容包括：

- 第 1 章：设备管理。介绍登录方式、StoneOS 升级以及许可证安装等。
- 第 2 章：基础上网配置。介绍接口、路由、策略等基本上网配置。
- 第 3 章：常用功能配置。介绍 PPPoE 拨号、动态地址分配 DHCP、DNAT 等配置。
- 第 4 章：链路负载均衡。介绍基于目的路由、源路由、策略路由的流量负载配置等。
- 第 5 章：QoS 配置。介绍 QoS 功能及配置。
- 第 6 章：网络行为控制配置。介绍 URL 过滤、网页关键字以及网络聊天控制配置。
- 第 7 章：VPN 高级配置。介绍基于 USB Key 的 SCVPN 配置以及 PnPVPN 配置。
- 第 8 章：高可靠性。介绍高可靠性（HA）的配置。

手册约定

为方便用户阅读与理解，本手册遵循以下约定：

内容约定

本手册内容约定如下：

- 提示：为用户提供相关参考信息。
- 说明：为用户提供有助于理解内容的说明信息。
- 注意：如果该操作不正确，会导致系统出错。
- 『 』：用该方式表示 Hillstone 设备 WebUI 界面上的链接、标签或者按钮。例如，“点击『登录』按钮进入 Hillstone 设备的主页”。
- < >：用该方式表示 WebUI 界面上提供的文本信息，包括单选按钮名称、复选框名称、文本框名称、选项名称以及文字描述。例如，“改变 MTU 值，选中<手动>单选按钮，然后在文本框中输入合适的值”。

第 1 章 设备管理

设备管理介绍

为方便管理员管理与配置，安全网关支持本地（Console 口）与远程（Telnet、SSH、HTTP 以及 HTTPS）两种环境配置方法，可以通过 CLI 和 WebUI 两种方式进行配置。

终端 Console 登录

通过 Console 口，用户可登录安全网关设备的 CLI，从而使用命令行对设备进行配置。在计算机上运行终端仿真程序（系统的超级终端、SecureCRT 等）建立与安全网关的连接。按照表 1 配置终端参数：

表 1：配置终端参数

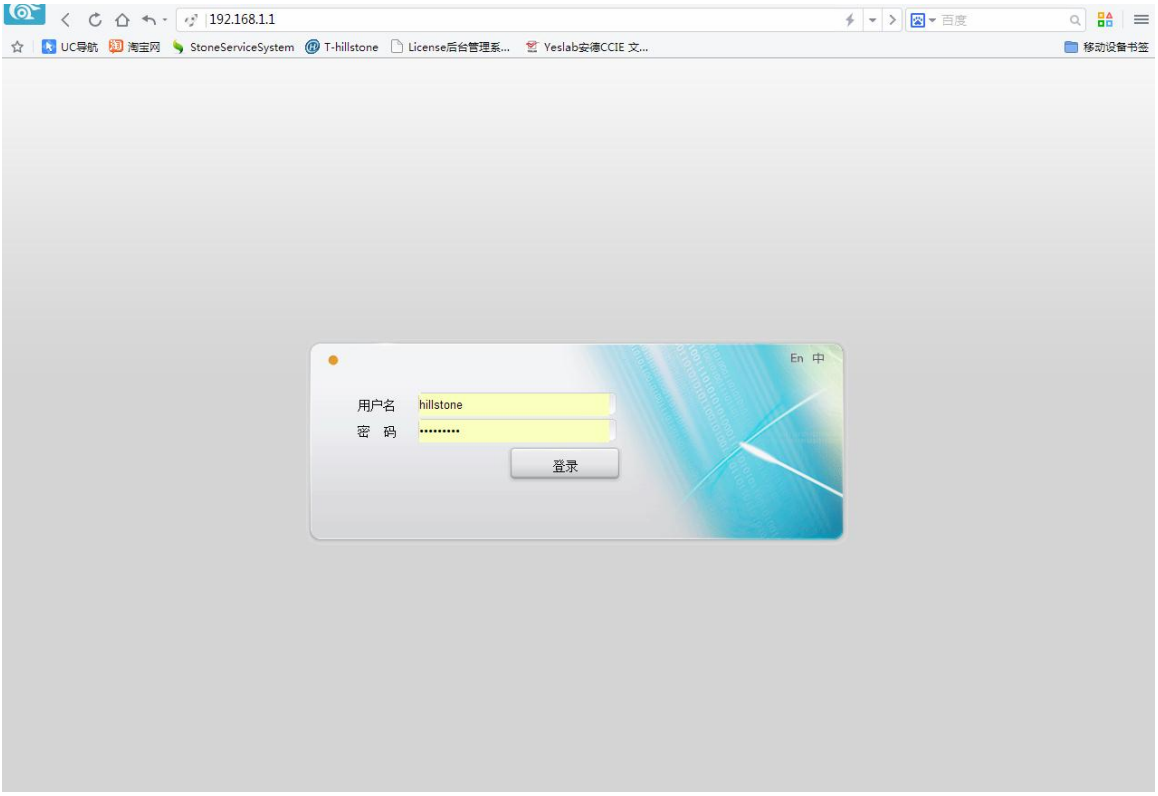
参数	数值
波特率	9600 bit/s
数据位	8
奇偶校验	无
停止位	1

WebUI 方式登录

WebUI 是最方便、直观、简单的配置方式，WebUI 同时支持 http 和 https 两种访问方式。安全网关的 ethernet0/0 接口配有默认 IP 地址 192.168.1.1/24，初次使用安全网关时，用户可以通过该接口访问安全网关的 WebUI 页面。

请按照以下步骤：

1. 将管理 PC 的 IP 地址设置为与 192.168.1.1/24 同网段的 IP 地址 ,并且用网线将管理 PC 与安全网关的 ethernet0/0 接口进行连接。
2. 在管理 PC 的 Web 浏览器中输入地址“http://192.168.1.1”并按回车键。出现登录页面如下图所示。



恢复出厂设置

Hillstone 山石网科提供三种方法恢复设备的出厂配置，分别是：

- 命令行：通过 CLI 使用命令进行恢复
- WebUI：通过 WebUI 清除配置以恢复出厂配置
- 物理方法：使用设备的 CLR 按键进行恢复

通过 CLI 方式

通过 CLI 使用命令恢复出厂设置，请按照以下步骤进行操作：

1. 在执行模式下，使用 **unset all** 命令。
2. 根据提示，选择是否保存当前配置：y/n。
3. 选择是否重启设备：y/n。
4. 系统重启后即出厂配置恢复完毕。

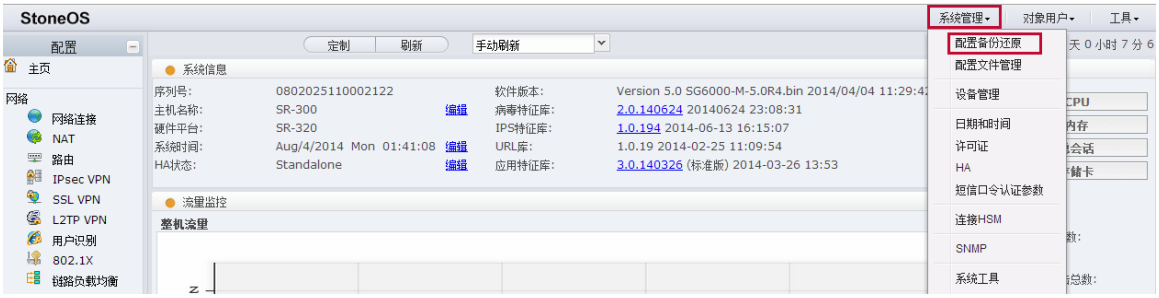
```
SG-6000# unset all
Remove all the configuration(back to factory default), are you sure? [y]/n: y
removing configuration...

System reboot, are you sure? [y]/n: y
```

通过 WebUI 方式

通过 WebUI 恢复出厂配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ,从工具栏的<系统管理>下拉菜单选择『配置备份还原』。如下图所示：



2. 在弹出的<系统配置备份还原向导>对话框，选择<恢复出厂配置>单选按钮，并点击『下一步』按钮。

3. 选择是否重启设备。为使配置生效，用户需重新启动设备。选择<是，立即重新启动设备>单选按钮，并点击『完成』按钮。

4. 所有配置将会被清除，然后设备将自动重启。

通过 CLR 按键方式

使用 CLR 按键恢复出厂配置，请按照以下步骤进行操作：

1. 关闭安全网关的电源。
2. 用针状物按住 CLR 按键的同时打开安全网关的电源。
3. 保持按住状态直到指示灯 STA 和 ALM 均变为红色常亮，释放 CLR 按键。此时系统开始恢复出厂配置。
4. 出厂配置恢复完毕，系统将会自动重新启动。

StoneOS 版本升级

通过网络迅速升级 StoneOS（TFTP）

Sysloader 可以从 TFTP 服务器获取 StoneOS，从而保证用户能够通过网络迅速升级 StoneOS。请按照以下步骤进行操作：

1. 给设备上电根据提示按 ESC 键并且进入 Sysloader。参照以下操作提示：

```
HILLSTONE NETWORKS
Hillstone Bootloader 1.3.2 Aug 14 2008-19:09:37

DRAM:  2048 MB
BOOTROM: 512 KB
```

```
Press ESC to stop autoboot:  4          5 秒倒计时结束前按“ESC”键
Run on-board sysloader? [y]/n: y        键入字母“y”或者敲回车键
Loading: ##########################
```

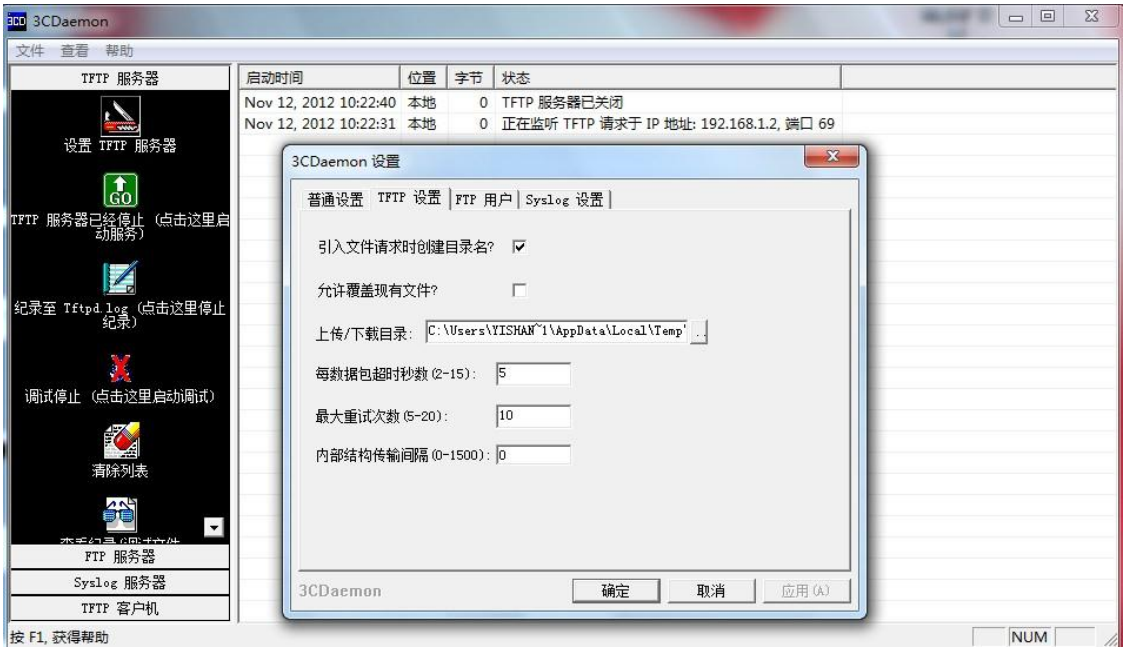
2. 从 Sysloader 的操作选择菜单选择通过 TFTP 升级 StoneOS。参照以下操作提示：

```
Sysloader 1.2.13 Aug 14 2008 - 16:53:42

1       Load firmware via TFTP
2       Load firmware via FTP
3       Load firmware from USB disks (not available)
4       Select backup firmware as active
5       Show on-board firmware
6       Reset

Please select: 1 在此处键入“1”并敲回车键
```

3. 确保设备与控制主机的连通性，并将需升级的 StoneOS 拷贝到指定目录下。



4. 依次配置 Sysloader 的 IP 地址、TFTP 服务器的 IP 地址、网关 IP 地址以及 StoneOS 名称。参照以下操作提示：

```
Local ip address     [     ]: 10.2.2.10/16   输入 Sysloader 的 IP 地址并敲回车键
Server ip address    [     ]: 10.2.2.3       输入 TFTP 服务器的 IP 地址并敲回车键
Gateway ip address   [     ]: 10.2.2.1       如果 Sysloader 与 TFTP 服务器的 IP 地址不属于同一个网段，输入网关的 IP 地址并敲回车键；否则直接敲回车键
File name  : StoneOS-3.5R2   输入 StoneOS 名称并敲回车键，系统开始通过 TFTP 获取 StoneOS
```

```
##################################################################################################################################
```

5. 保存 StoneOS。参照以下操作提示：

```
File total length 10482508
Checking the image...
Verified OK
Save this image? [y]/n: y   键入字母“y”或者敲回车键，保存获得的 StoneOS
Saving ..........................................
Set StoneOS-3.5R2 as active boot image
```

6. 重启。系统将使用新的 StoneOS 启动。参照以下操作提示：

```
Please reset board to boot this image
1       Load firmware via TFTP
2       Load firmware via FTP
3       Load firmware from USB disks (not available)
4       Select backup firmware as active
5       Show on-board firmware
6       Reset

Please select: 6 在此处键入“6”并敲回车键，系统开始重启
```

设备的 Flash 中最多可以储存两个 StoneOS。如果 Flash 中已经保存了两个 StoneOS，请根据提示对储存的 StoneOS 进行删除。

通过 WebUI 方式升级 StoneOS

1. 通过 WebUI 方式登录 StoneOS，从工具栏的<系统管理>下拉菜单选择『版本升级』。如下图所示：

2. 在弹出的<版本升级向导>对话框，选择<升级到最新的软件版本>单选按钮，并点击『下一步』按钮。

3. 在<选择备份软件版本>下拉菜单中选择一个软件版本做为备份，然后点击<上传新的软件文件>后的『浏览』按钮并在本地 PC 选择新的软件版本文件。

4. 点击『下一步』。根据需要，选择<是，立即重新启动设备>单选按钮，并点击『完成』按钮。为使配置生效，用户需重新启动设备。

注意：如果选择暂不重新启动设备，将会在下次重新启动设备后加载新版本 StoneOS。

许可证安装

通过 CLI 方式安装

通过 CLI 使用命令安装许可证，请按照以下步骤进行操作：

1. 登录 StoneOS，在执行模式下，使用 **exec license install** *license-string* 命令（*license-string* – 要安装的许可证字符串。输入“license：”后的字符串）。如下图所示：

```
SG-6000# exec license in
SG-6000# exec license install license:MBvPXiU8nWYoITvsovRJSSEqJABvQNeJIFdUQZRtbmwLpRWeJVTyMp1ga6pICcjEnyUjI71hDdOZ1KUdMskhlbdMI70YvS
L2DwPKqchcyYreajADsBbb+wIGda08BFZ6rxy5E+cnelYjytdxMIO8iP0y+Te3EtGnqKuZfL19BMLtYZQYPFp7CoZfSMONoYL19vuPpZwJLlDGrVKPleHBWWRI9xZCIFoQmL
Fl3ssrwjjN3OxgXVbtMyQOw+C8O8CNERxPYNm0dKspmVWgzoaX4bAFAqLdkrYLFmnqAQ9biJ9gZhqCnW0u+3CVo8Dx7mpMy+4BAmS2g2IJ5NcCMPE2KQ==
2014-08-04 03:16:51, Event WARNING@MGMT: license plat140804110416 installation succeeded

Info: Successfully install the license

SG-6000#
```

2. 根据系统提示重启后即完成许可证安装。

通过 WebUI 方式安装

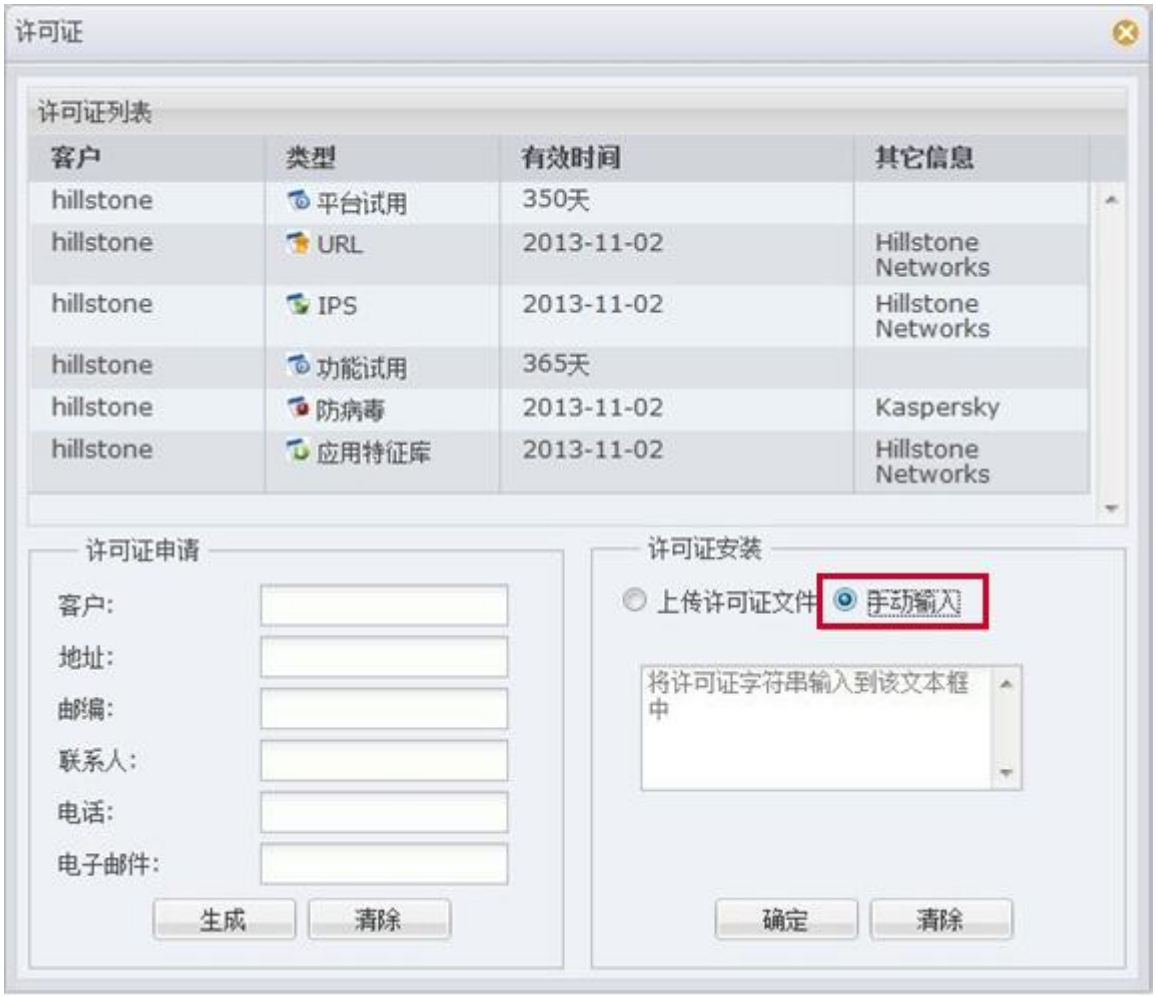
通过 WebUI 安装许可证，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS，从工具栏的<系统管理>下拉菜单选择『许可证』。如下图所示：

2. 在弹出的<许可证>对话框中，许可证列表可查看当前系统许可证的类型和有效时间。

3. 在<许可证安装>处，用户可根据需要，选择手动输入许可证请求或选择上传本地文件。

- **上传许可证文件**：选中<上传许可证文件>单选按钮（许可证为纯文本.txt 文件），点击『浏览』按钮，并且选中许可证文件；
- **手动输入**：选中<手动输入>单选按钮，然后将许可证字符串内容（包含“license：”及之后内容）输入到对应的文本框。



4. 点击『确定』按钮保存所做配置，并且重启设备完成许可证的安装。

第 2 章 基础上网配置

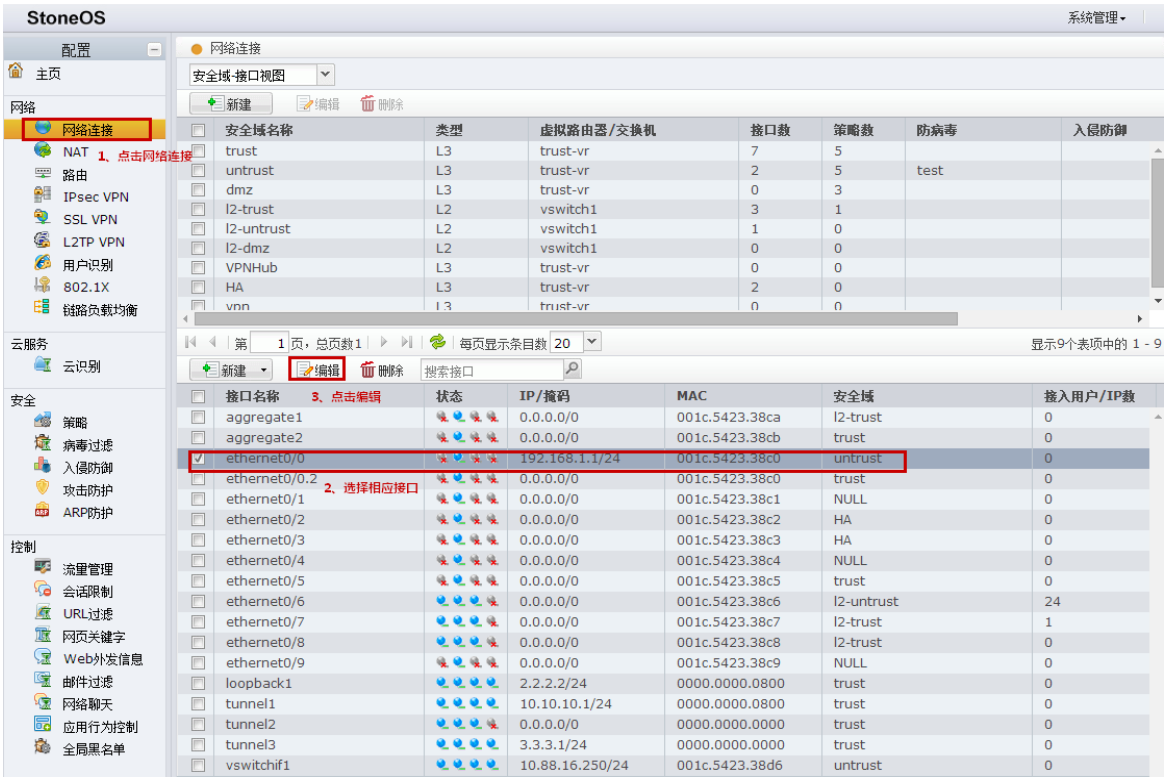
基础上网配置介绍

为使设备实现正常上网，基本配置包括接口、路由、策略以及源 NAT 的配置。

接口配置

接口配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ，从页面左侧导航树选择并点击“配置->网络->网络连接”，进入网络连接页面。



2. 从接口列表中选中需要编辑的接口，双击或者点击列表右上方的『编辑』按钮。

3. 在弹出的<接口配置>对话框对接口进行编辑：

- **绑定安全域**：指定接口的安全域类型。三层接口选择三层安全域，二层接口选择二层安全域；
- **安全域**：选择安全域名称。一般情况下，内网选择 trust 或 l2-trust；外网选择 untrust 或 l2-untrust。

- **IP 配置**：为接口配置 IP 地址相关信息。
- **管理方式**：指定接口的管理方式。在<管理方式>部分选中需要的管理方式的复选框。

提示：如果外网接口使用 PPPoE 拨号方式接入，关于接口的配置请参阅 PPPoE 配置。

路由配置

路由配置，请按照以下步骤进行操作：

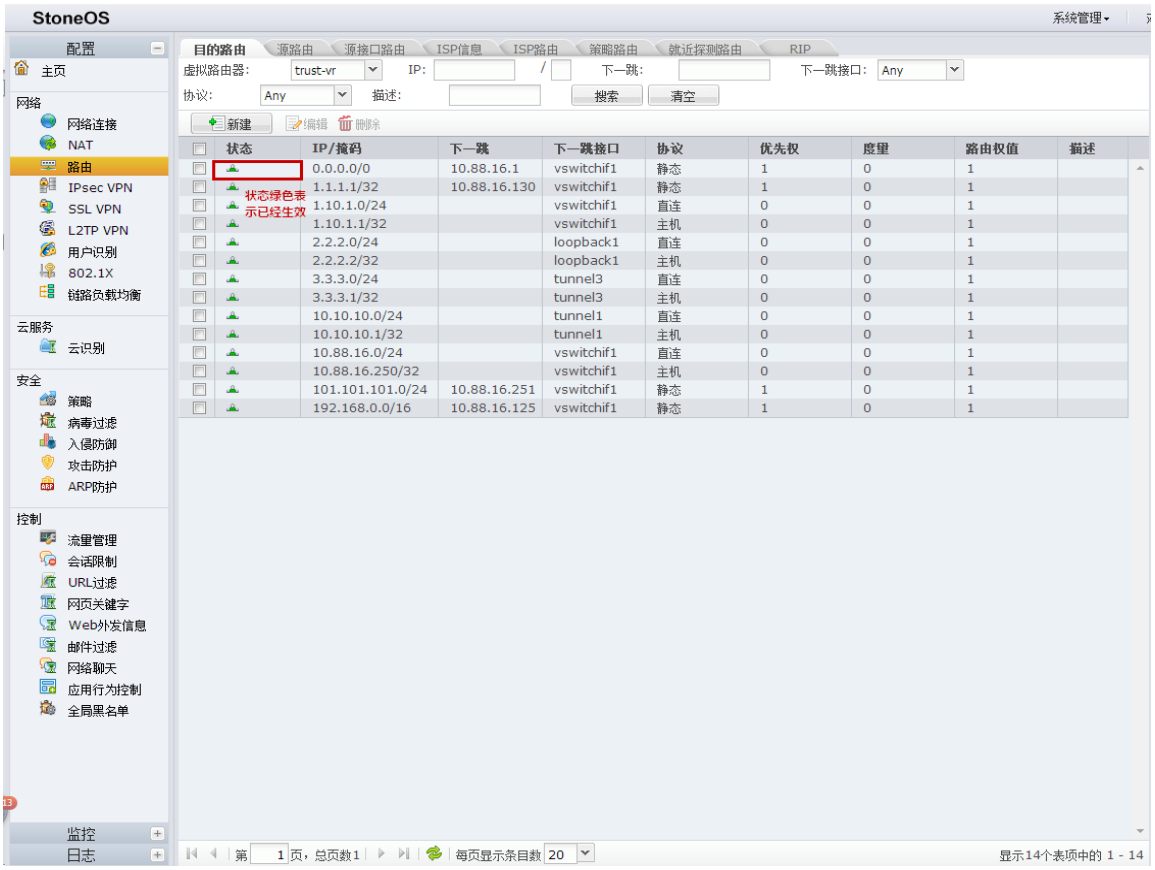
1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->网络->路由”，进入路由页面。
2. 点击『目的路由』标签，进入目的路由页面。
3. 从<虚拟路由器>下拉菜单选择一个 VR，新建的路由将属于该 VR，默认为“trust-vr”。
4. 点击目的路由列表左上角的『新建』按钮，弹出<目的路由配置>对话框，在该对话框对目的路由进行编辑：
   - **目的地**：指定路由条目的目的 IP。
   - **子网掩码**：指定路由条目的目的 IP 对应的子网掩码。
   - **下一跳**：指定下一跳类型，选中<网关>或<接口>单选按钮。若选择<网关>，需在<网关>文本框中输入网关 IP 地址。若选择<接口>，需在<接口>下拉菜单中选择接口名称。如果该接口为 tunnel 的时候，需要在可选栏输入 tunnel 对端的网关地址。如：下一跳网关指定为 122.193.30.97（由运营商提供网关地址）。
   - **优先权**：该参数取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由

会被优先使用。取值范围是 1 到 255，默认值为 1。当优先级为 255 时，该路由无效。

- **路由权值**：路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。

5. 用户可以根据需要，在<描述>文本框中指定目的路由的描述信息。

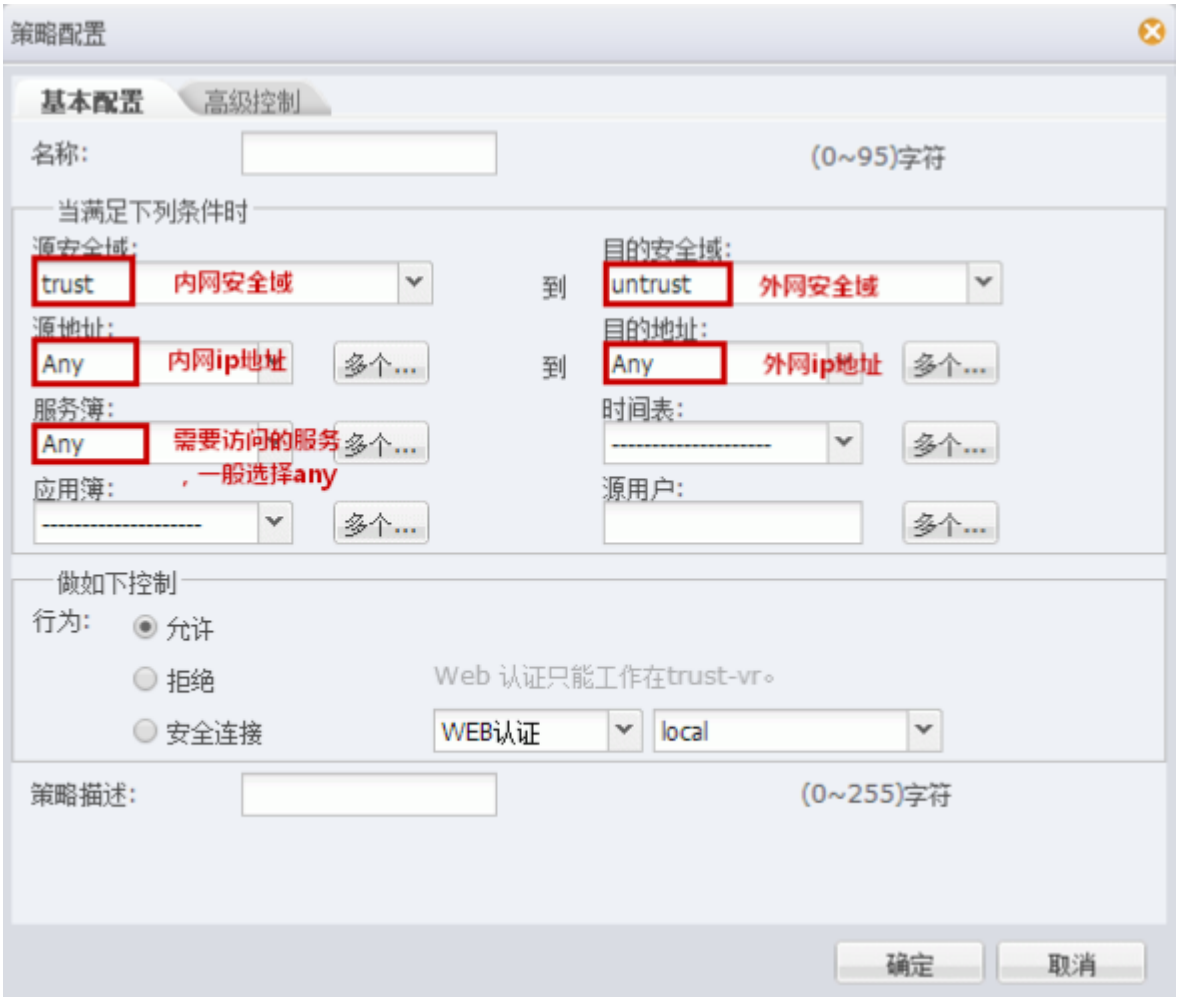
6. 点击『确定』按钮，完成新建目的路由。



策略配置

策略配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->安全->策略”，进入策略页面。
2. 点击列表左上角的『新建』按钮，弹出<策略配置>对话框，在该对话框对策略规则进行编辑。基本选项包含策略的源/目的安全域和源/目的地址的选择，以及服务、时间表、用户、行为和策略描述的指定。



3. 配置完成后，点击『确定』按钮保存所做配置并返回策略页面。

源 NAT 配置

源 NAT 配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->网络->NAT”，进入源 NAT 页面。
2. 点击源 NAT 列表中的『新建』按钮，弹出<新建源 NAT>对话框。在该对话框对源 NAT

规则进行编辑。

3. 配置完成后，点击『确定』按钮保存所做配置。

第 3 章 常用功能配置

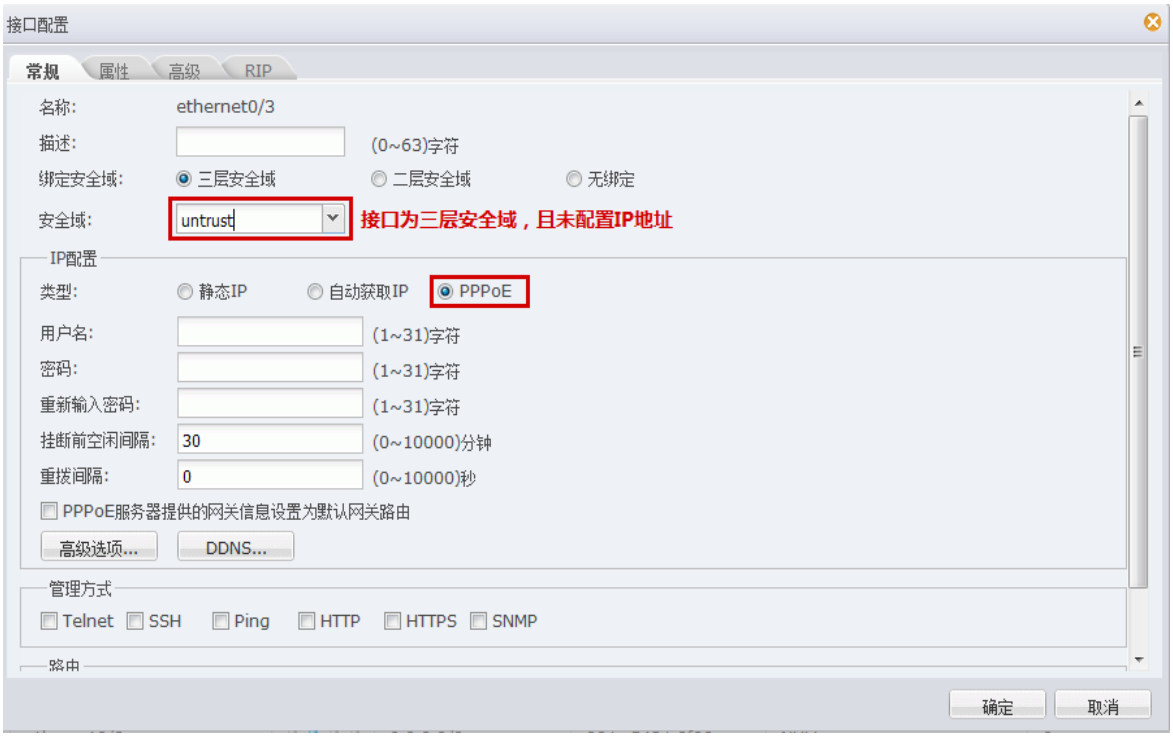
常用配置介绍

本章介绍 Hillstone 山石网科多核安全网关的一些常用功能配置，包括 PPPoE、DHCP、IP-MAC 绑定、端到端 IPsec VPN、SCVPN、DNAT 等配置。

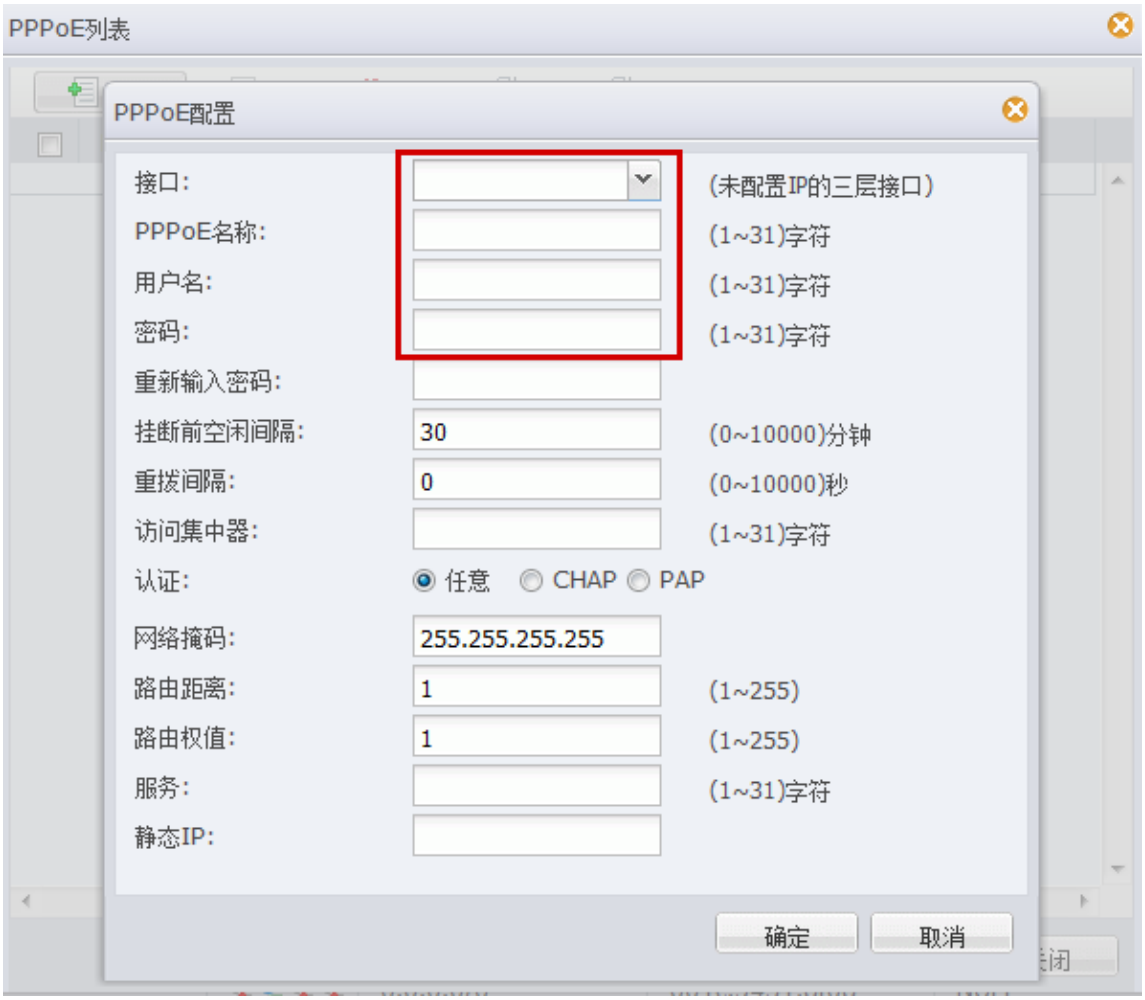
PPPoE 配置

PPPoE 配置，请按照以下步骤进行操作：

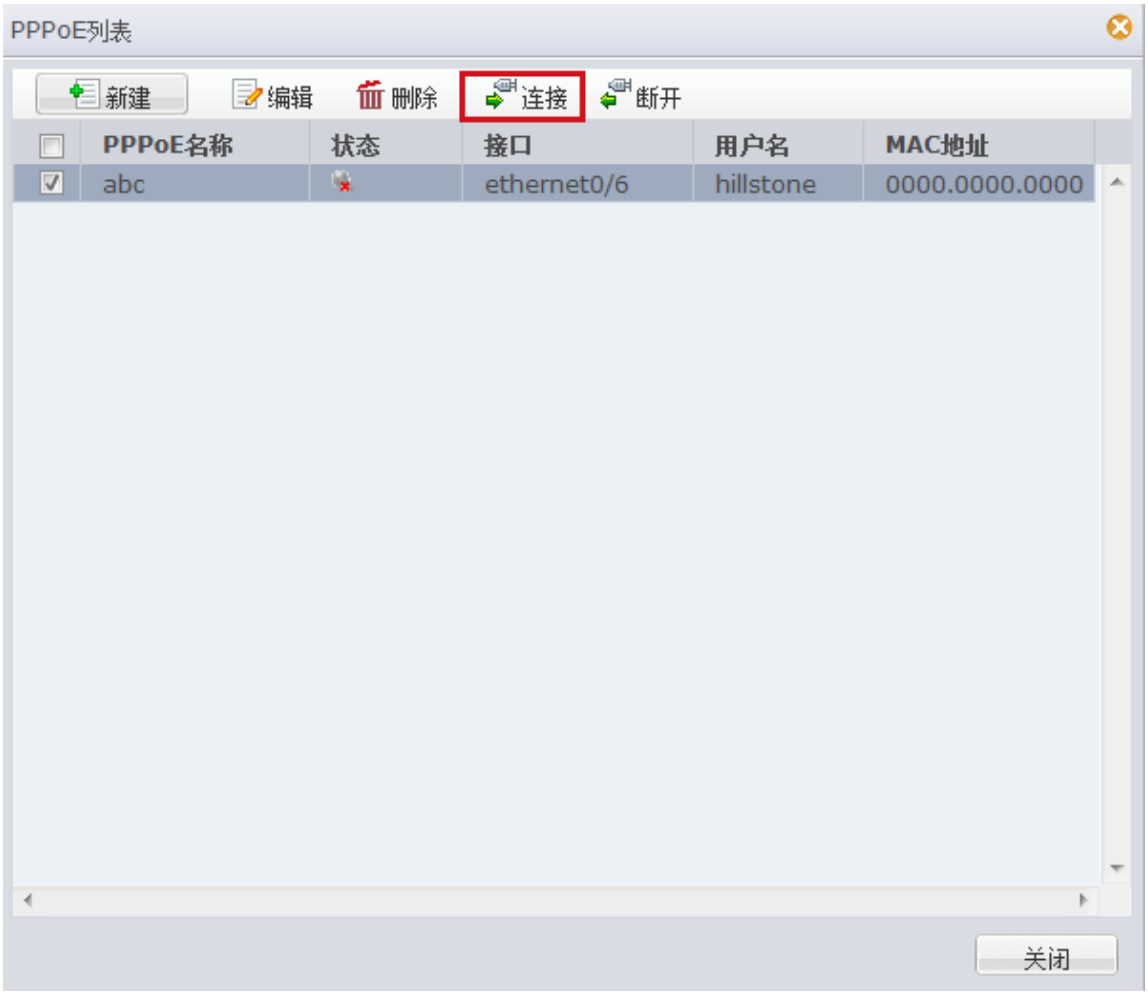
1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->网络->网络连接”，进入网络连接页面。
2. 从接口列表中选中需要编辑的接口，双击或者点击列表右上方的『编辑』按钮。
3. 在弹出的<接口配置>对话框对接口进行编辑。



4. 点击『确定』按钮保存所做配置并返回网络连接页面。
5. 从页面右侧辅助栏的<任务>区选择『PPPoE 列表』链接，弹出<PPPoE 列表>对话框。
6. 点击页面左上角的『新建』按钮，弹出<PPPoE 配置>对话框。在该对话框进行配置。



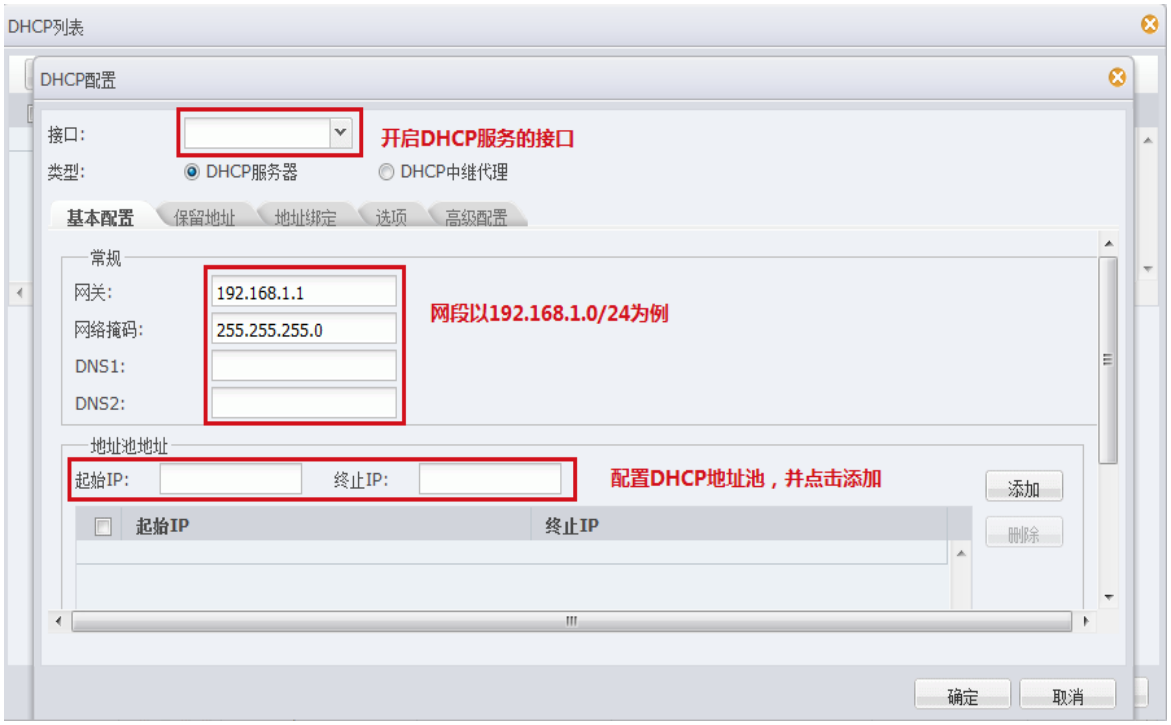
7. 配置完成点击『确定』按钮并返回 PPPoE 列表对话框。选中需要连接/断开的 PPPoE 实例，然后点击页面左上角的『连接』按钮。



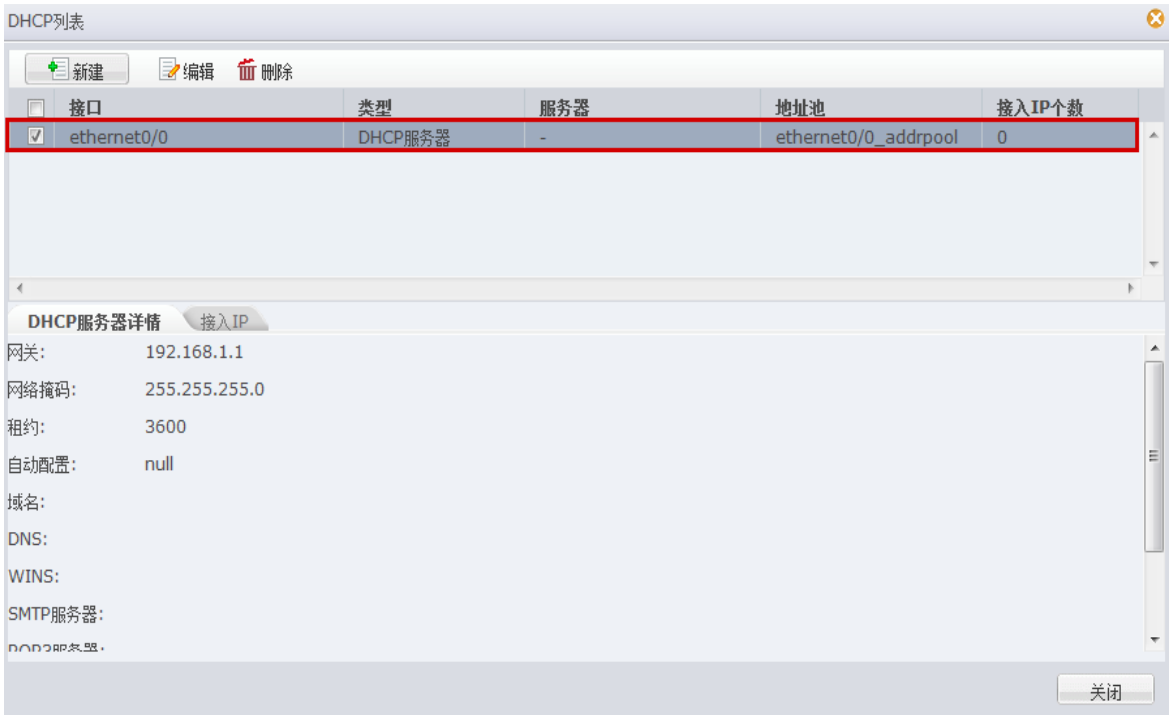
DHCP 配置

DHCP 配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击“配置->网络->网络连接”，进入网络连接页面。
2. 从页面右侧辅助栏的<任务>区选择『DHCP 列表』链接，弹出<DHCP 列表>对话框。在该对话框对 DHCP 进行编辑：
   - **接口**：选择应用 DHCP 服务器功能的接口。
   - **类型**：选中<DHCP 服务器>单选按钮。
   - **基本配置**：在<基本配置>标签页对 DHCP 的基本属性进行配置。



3. 配置完成点击『确定』按钮并返回 DHCP 列表对话框。并且将用户 pc 或者交换机连接在相应端口，即可获取 IP 地址。



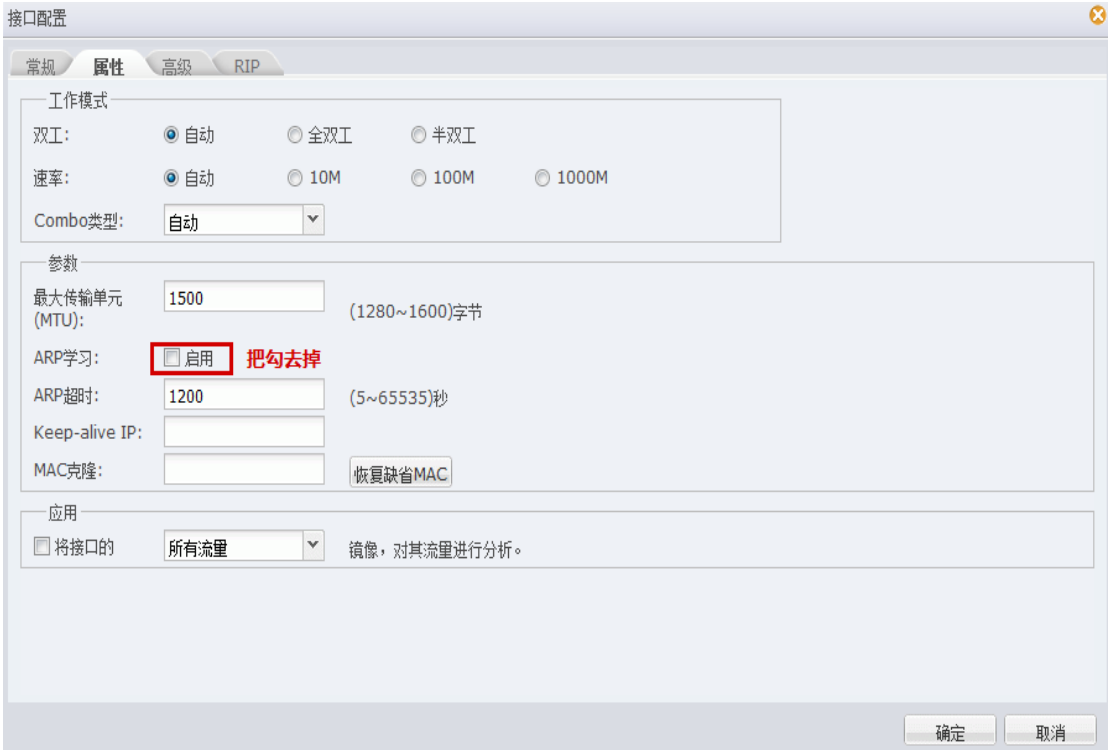
IP-MAC 绑定配置

IP-MAC 绑定配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击“配置->安全->ARP 防护”，进入 ARP 防护页面。

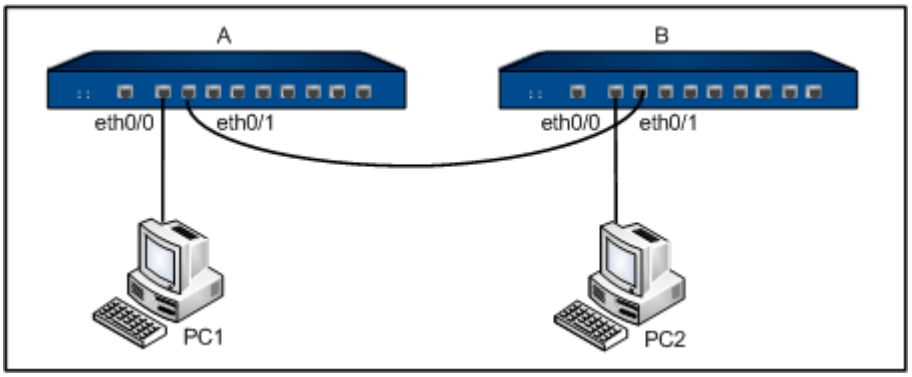
2. 从静态 IP-MAC 绑定条目列表中选中需要绑定的 IP-MAC 条目，双击或者点击列表上方的『编辑』按钮，弹出<IP-MAC 绑定>对话框。
3. 在<IP-MAC 绑定>对话框中 ,选中<IP-MAC 绑定>复选框开启 IP-MAC 绑定 ,并点击『确定』按钮保存配置。

4. 默认情况下，安全网关的 ARP 学习功能是开启的，IP-MAC 绑定成功后，还需要关闭接口的 ARP 学习功能。
5. 从页面左侧导航树选择并点击"配置->网络->网络连接"，进入网络连接页面，从接口列表中选中需要编辑的接口，双击或者点击列表右上方的『编辑』按钮。
6. 在弹出的<接口配置>对话框中，点击『属性』标签，在<参数>部分取消选中 ARP 学习后的『启用』复选框开启接口的 ARP 学习功能。



端到端 IPsec VPN 配置

在 Hillstone 安全网关 A 和 Hillstone 安全网关 B 之间建立一个安全隧道，PC1 作为 Hillstone 安全网关 A 端的主机，PC2 作为 Hillstone 安全网关 B 端的主机，两端的公网 IP 都是固定的情况下，配置端到端的 IPsec VPN，拓补图如下：

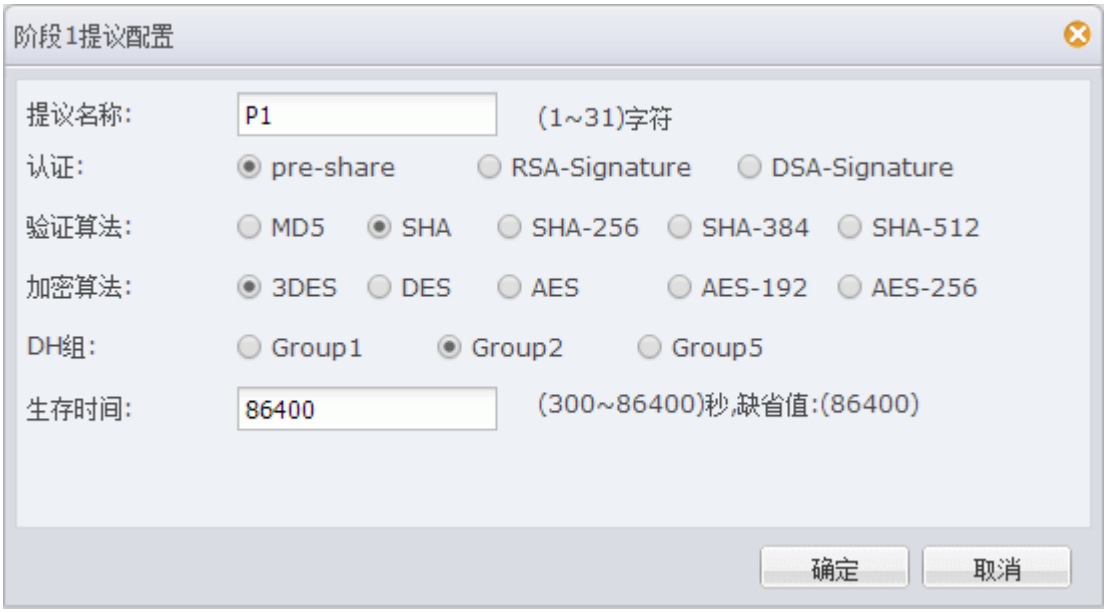


使用 IKE VPN 即自动协商方式配置 IPsec VPN，配置包括：

- 配置 P1 提议
- 配置 VPN 对端
- 配置 P2 提议
- 配置隧道
- 绑定接口到隧道
- 配置隧道路由和策略

具体配置。请按照以下步骤进行操作：

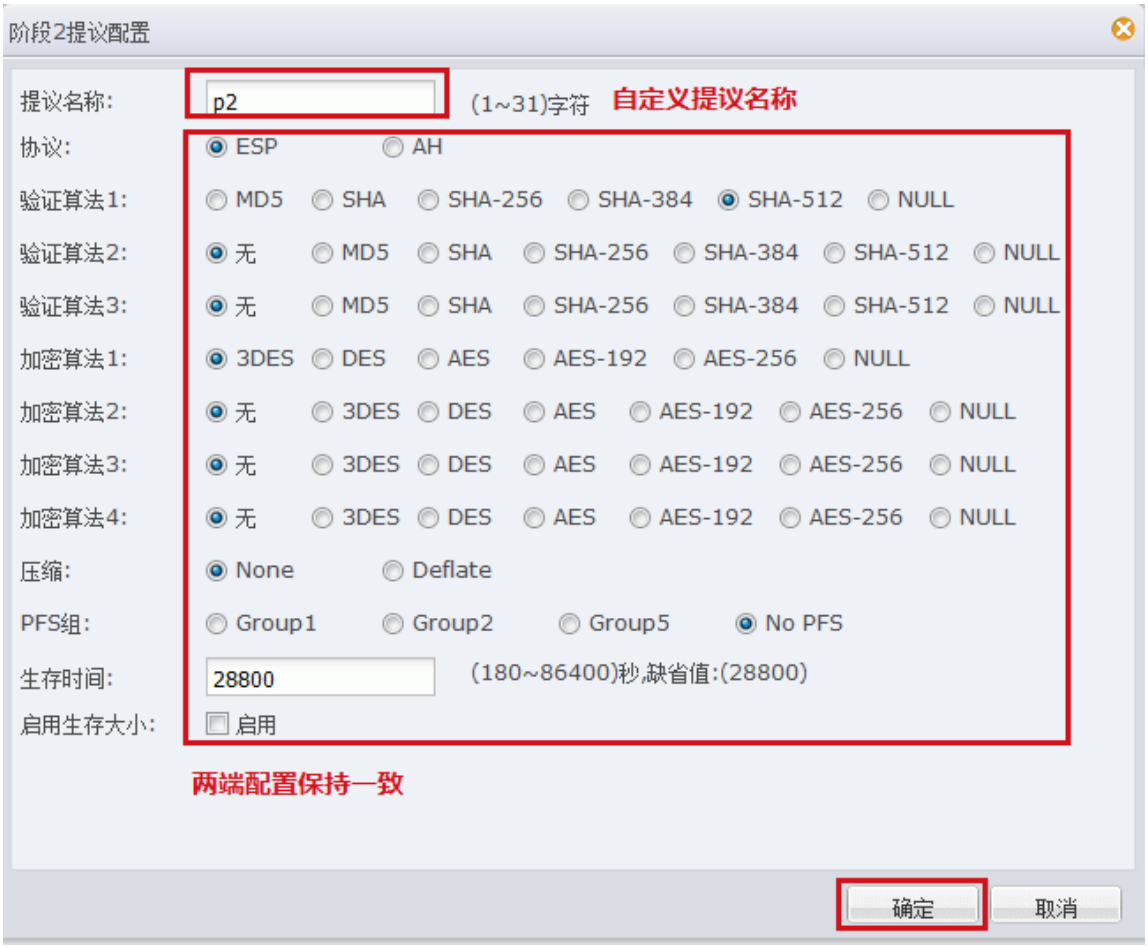
1. **配置 P1 提议**。通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击"配置->网络->IPsec VPN"，进入 IPsec VPN 页面。点击『P1 提议』标签，进入 P1 提议标签页。
2. 点击 P1 提议列表左上方的『新建』按钮，弹出<阶段 1 提议配置>对话框。在该对话框进行编辑：
   - **提议名称**：指定或者显示 P1 提议的名称。
   - **认证**：指定 IKE 身份认证的方式。
   - **验证算法**：为 P1 提议指定验证算法。选中所需验证算法的单选按钮。
   - **加密算法**：为 P1 提议指定加密算法。
   - **DH 组**：为 P1 提议选择 DH 组。
   - **生存时间**：指定 SA 第一阶段的生命周期长度，单位为秒。默认 86400 秒。



3. **配置 VPN 对端**。在 IPsec VPN 页面，点击『VPN 对端列表』标签，进入 VPN 对端列表标签页。
4. 点击 VPN 对端列表左上方的『新建』按钮，弹出<VPN 对端配置>对话框。在该对话框对 VPN 对端进行基本配置。

注意：如果在设备前还有其他 NAT 设备，需在<高级配置>标签下配置 NAT 穿越功能。

5. **配置 P2 提议**。在 IPsec VPN 页面，点击『P2 提议』标签，进入 P2 提议标签页。
6. 点击 P2 提议列表左上方的『新建』按钮，弹出<阶段 2 提议配置>对话框。在该对话框进行 P2 提议配置。



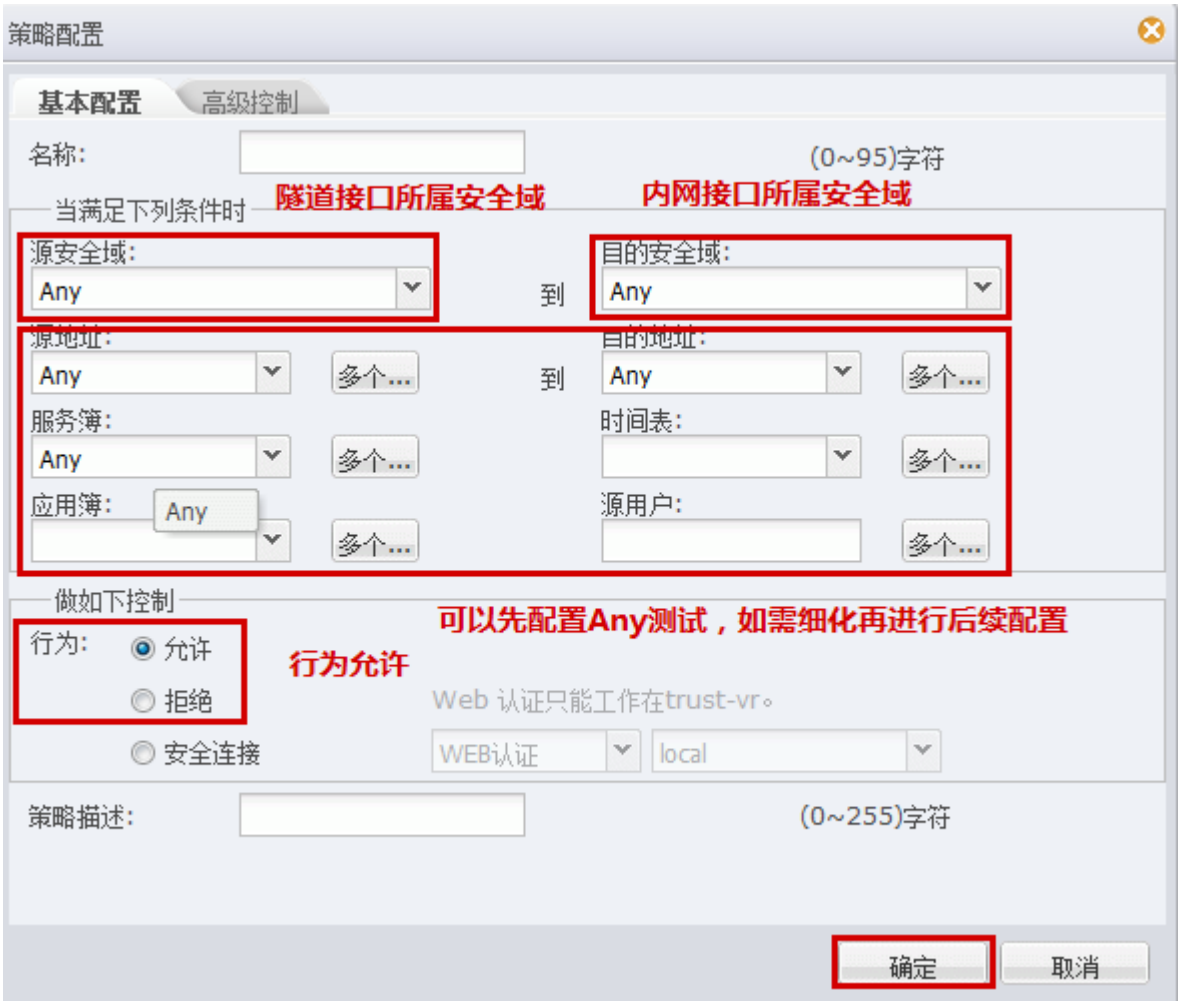
7. **配置隧道。**在 IPsec VPN 页面，点击 IKE VPN 列表左上方的『新建』按钮，弹出<IKE VPN 配置>对话框。
8. 在<步骤 1：对端>部分配置各选项。点击后面的『导入』按钮，并在<对端名称>下拉菜单选择已配置的 VPN 对端名称，导入系统中已配置的 VPN 对端参数。
9. 点击<步骤 2：隧道>，配置隧道相关选项。

注意：隧道配置完成后，需要流量触发 VPN 连接。如果需要自动连接，请在<高级配置>标签下配置自动连接功能。

10. **绑定接口到隧道。**从主页面左侧导航树选择并点击"配置->网络->网络连接"，进入网络连接页面。点击接口列表左上角的『新建』按钮，从下拉菜单中选择并点击<隧道接口>，系统弹出<接口配置>对话框。在该对话框绑定接口到隧道。

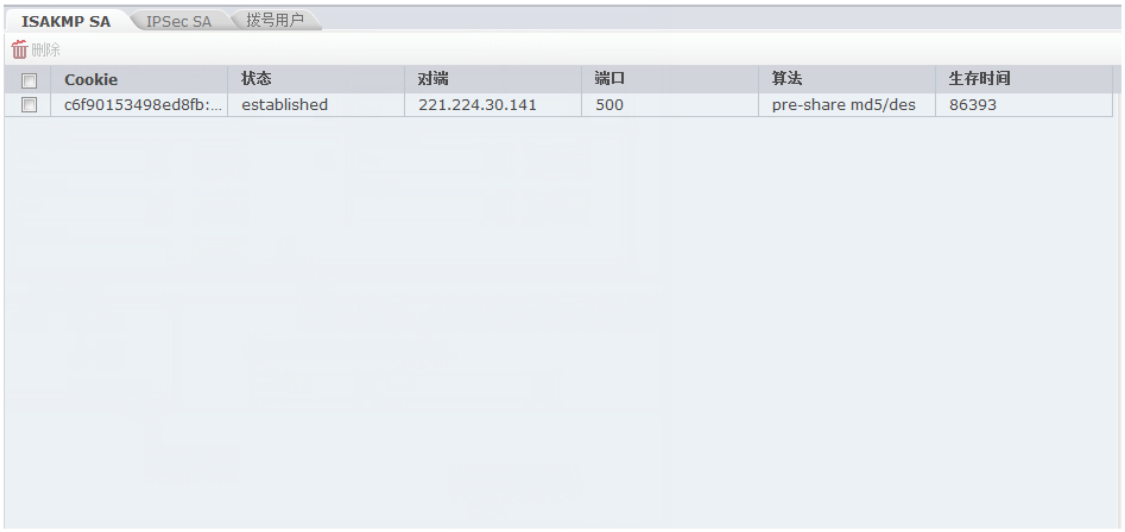
11. **配置隧道路由和策略**。从页面左侧导航树选择并点击"配置->网络->路由"，进入目的路由页面。点击目的路由列表左上角的『新建』按钮，弹出<目的路由配置>对话框，在该对话框对目的路由进行编辑。

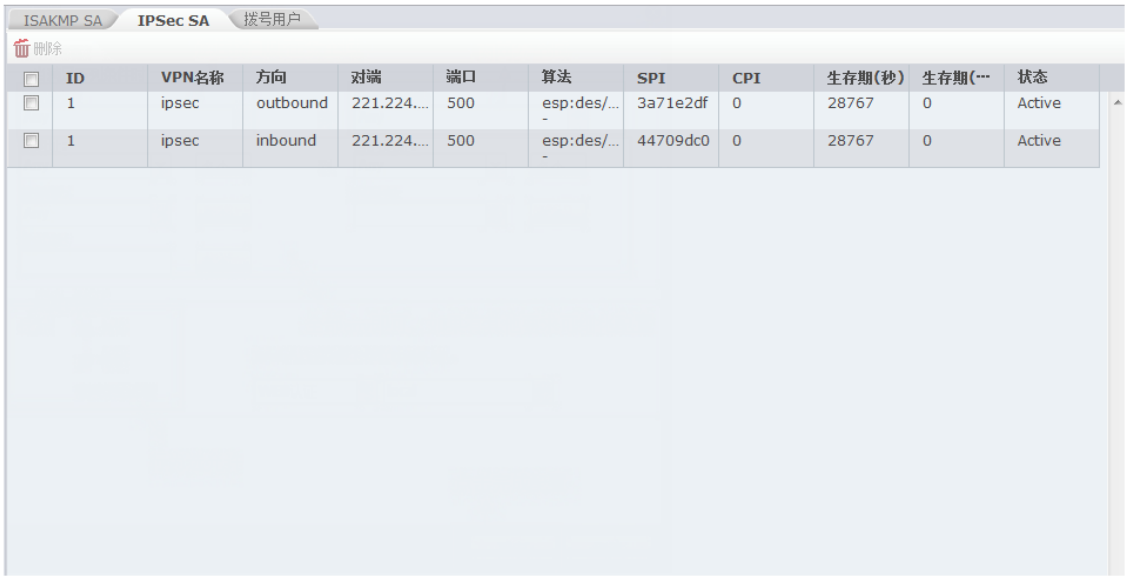
12. 从页面左侧导航树选择并点击"配置->安全->策略"，进入策略页面。点击列表左上角的『新建』按钮，弹出<策略配置>对话框，在该对话框对策略规则进行编辑。



13. 配置完成后，安全网关 B 也按照步骤 1-12 进行配置。

14. 完成以上配置后，安全网关 A 和安全网关 B 之间的安全隧道便建立成功了。从 IPsec VPN 页面右侧辅助栏的<任务>区选择『ISAKMP SA』/『IPsec SA』/链接，查看 VPN 监控结果。





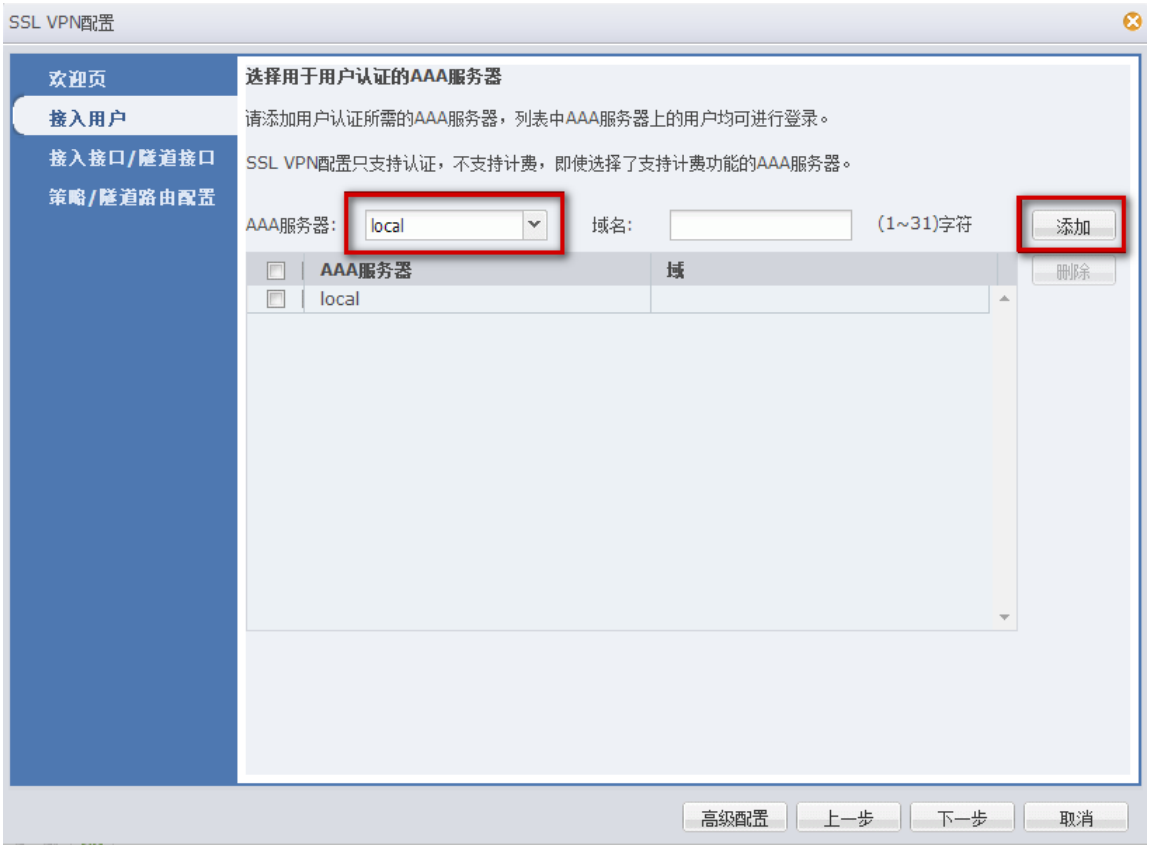
SCVPN 配置

为解决远程用户安全访问私网数据的问题，安全网关提供基于 SSL 的远程登录解决方案——Secure Connect VPN，简称为 SCVPN。SCVPN 功能可以通过简单易用的方法实现信息的远程连通。

SCVPN 配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击"配置->网络-> SSL VPN"，进入 SCVPN 页面。
2. 点击 SCVPN 列表左上角的『新建』按钮或者从页面右侧辅助栏的<任务>区选择『新建 SSL VPN』链接，弹出<SSL VPN 配置>对话框。
3. 阅读<欢迎页>内容，并在<SSL VPN 名称>文本框中指定 SCVPN 名称。

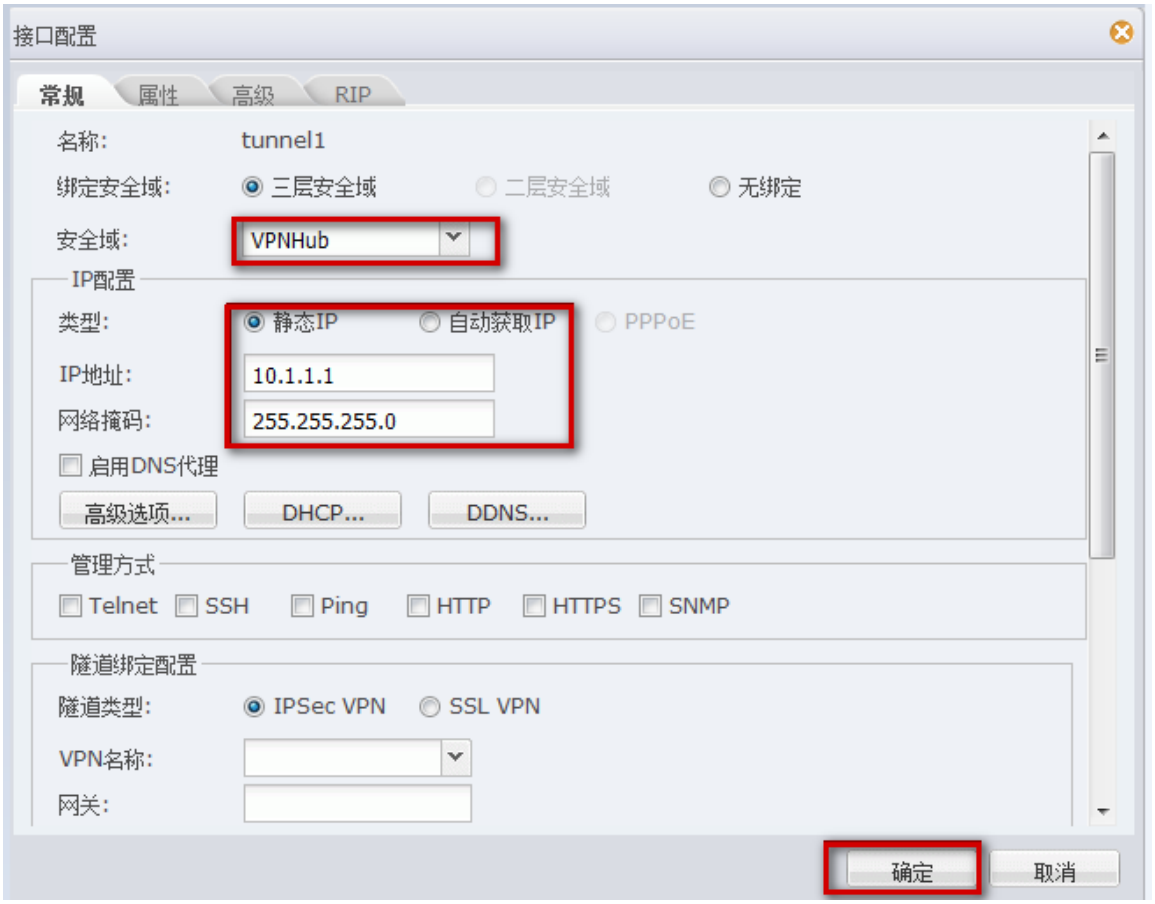
4. 点击『下一步』按钮进入<接入用户>配置页面。在该页面配置用于客户端用户身份认证的 AAA 服务器。



5. 点击『下一步』按钮进入<接入接口/隧道接口>配置页面。在该页面配置设备端接口、隧道接口和地址池。

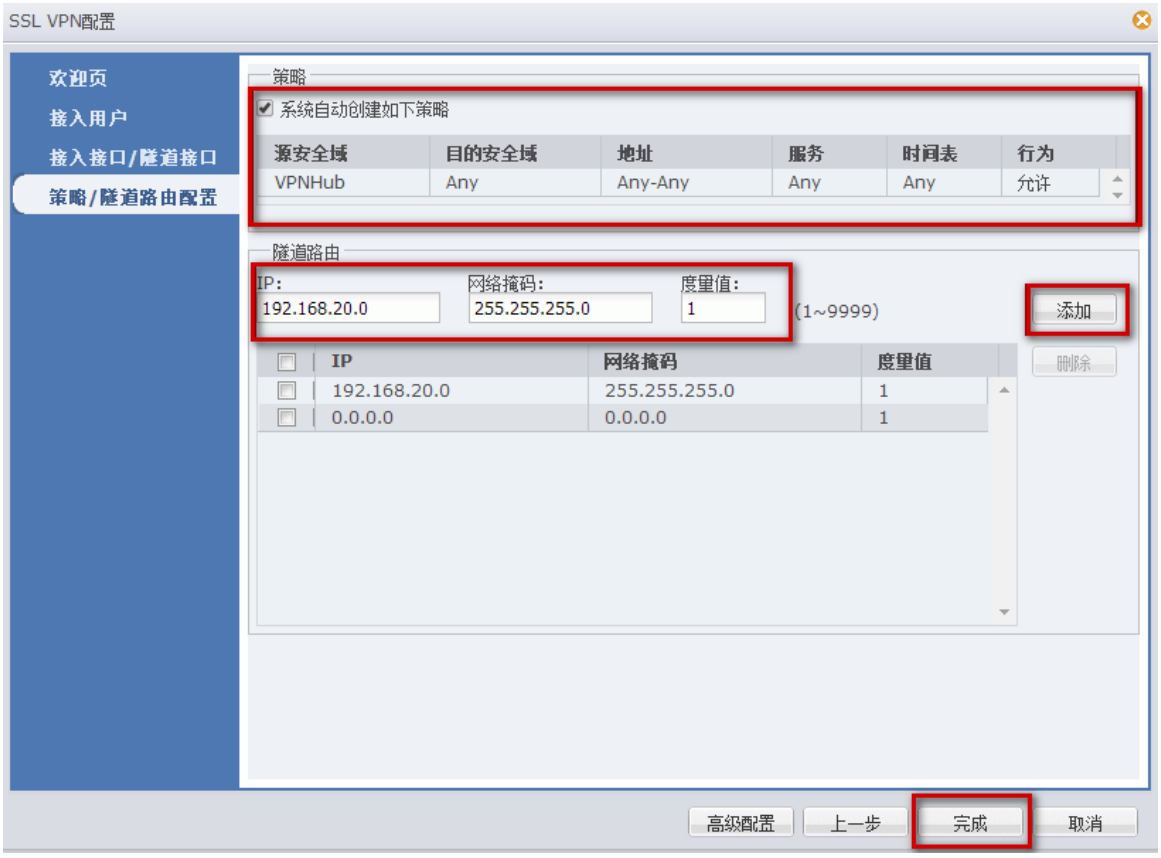
注意：隧道接口地址和地址池必须在同一网段，且地址池地址段中不能包含隧道接口地址。

6. 在<接入接口/隧道接口>配置页面<隧道接口>下拉菜单中选择系统中已配置的隧道接口；或者选中下拉菜单中的<新建>选项，在弹出的<接口配置>对话框中新建隧道接口；还可以在下拉菜单中选中系统中已配置的隧道接口，然后点击『配置』按钮，在弹出的<接口配置>对话框中编辑该隧道接口。



7. 在<接入接口/隧道接口>配置页面<地址池>下拉菜单中选择系统中已配置的地址池；或者，选中下拉菜单中的<新建>选项，在弹出的<地址池配置>对话框中新建地址池；还可以在下拉菜单中选中系统中已配置的地址池，然后点击『配置』按钮，在弹出的<地址池配置>对话框中编辑该地址池。

8. 点击『下一步』按钮进入<策略/隧道路由配置>页面。在该页面配置策略规则和隧道路由。

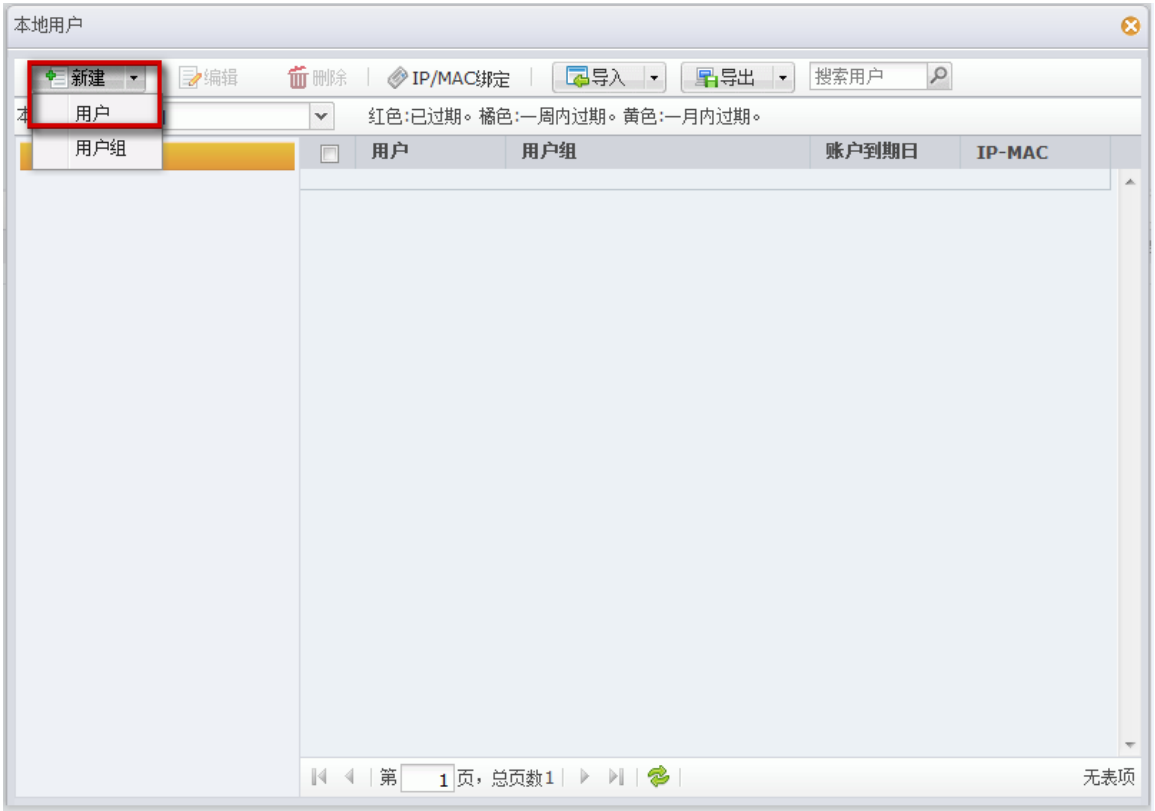


注意：系统会自动创建一条源安全域是 VPNHub，目的安全域是 Any 的策略；隧道路由即为远程拨入用户需要访问的内网资源网段。

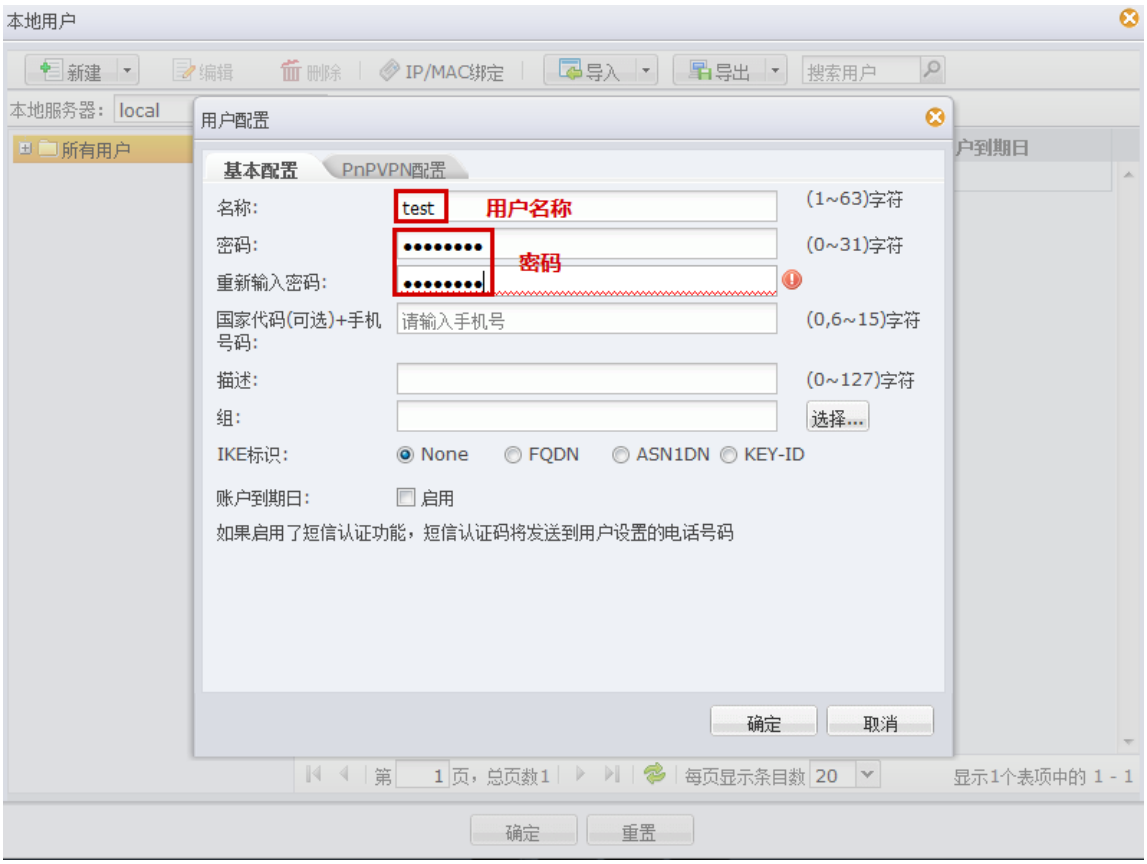
9. 如需要，点击页面右下方的『高级配置』按钮，进行 SCVPN 高级参数配置，包括参数配

置、客户端/USB Key 配置、主机检测/绑定配置、短信口令认证配置和最优路径检测配置。参数配置保持默认即可。

10. **建立登录用户**。从工具栏的<对象用户>下拉菜单选择『本地用户』，弹出<本地用户>对话框。



11. 选中<新建>下拉菜单中的『用户』按钮，弹出<用户配置>对话框。在『基本配置』标签页，进行用户名称和密码的配置。



12. **Web 方式（用户名/密码）启动 SCVPN**。在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number（默认为 4433）。

13. 浏览器转到登录页面，输入用户名和密码，并点击『登录』按钮。

14. **下载并启动 SCVPN 客户端（用户名/密码）**。使用 Web 方式登录后，下载并安装客户端程序 Hillstone Secure Connect。

15. 完成安装后，双击桌面的 Hillstone Secure Connect 快捷方式，或者点击"开始菜单"中的"所有程序 Hillstone Secure Connect Hillstone Secure Connect"，系统弹出登录对话框，点击对话框中的『模式』按钮，系统弹出<登录模式>对话框（如下图所示）。选中<用户名/密码>单选按钮，点击『确定』按钮。

16. 在弹出的"用户名/密码"登录模式客户端程序登录对话框，依次填写服务器地址、端口号、用户名以及密码，然后点击『登录』按钮。

DNAT 配置

目的地址映射主要用于将内网的服务器对外进行发布（如 HTTP 服务，FTP 服务，数据库服务等），使外网用户能够通过外网地址访问需要发布的服务。

常用的 DNAT 映射有一对一 IP 映射，一对一端口映射，多对多端口映射，一对多映射。

一对一 IP 映射

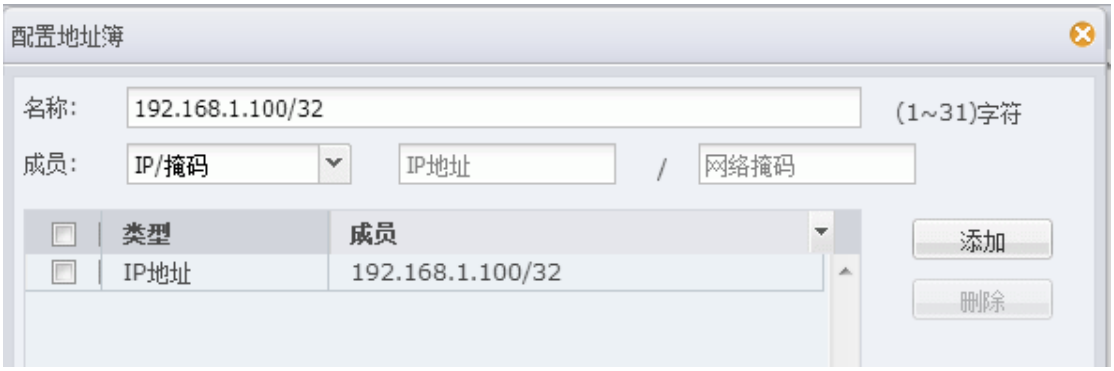
配置举例：将公网地址 60.0.0.1 映射到内网地址 192.168.1.100

请按照以下步骤进行配置：

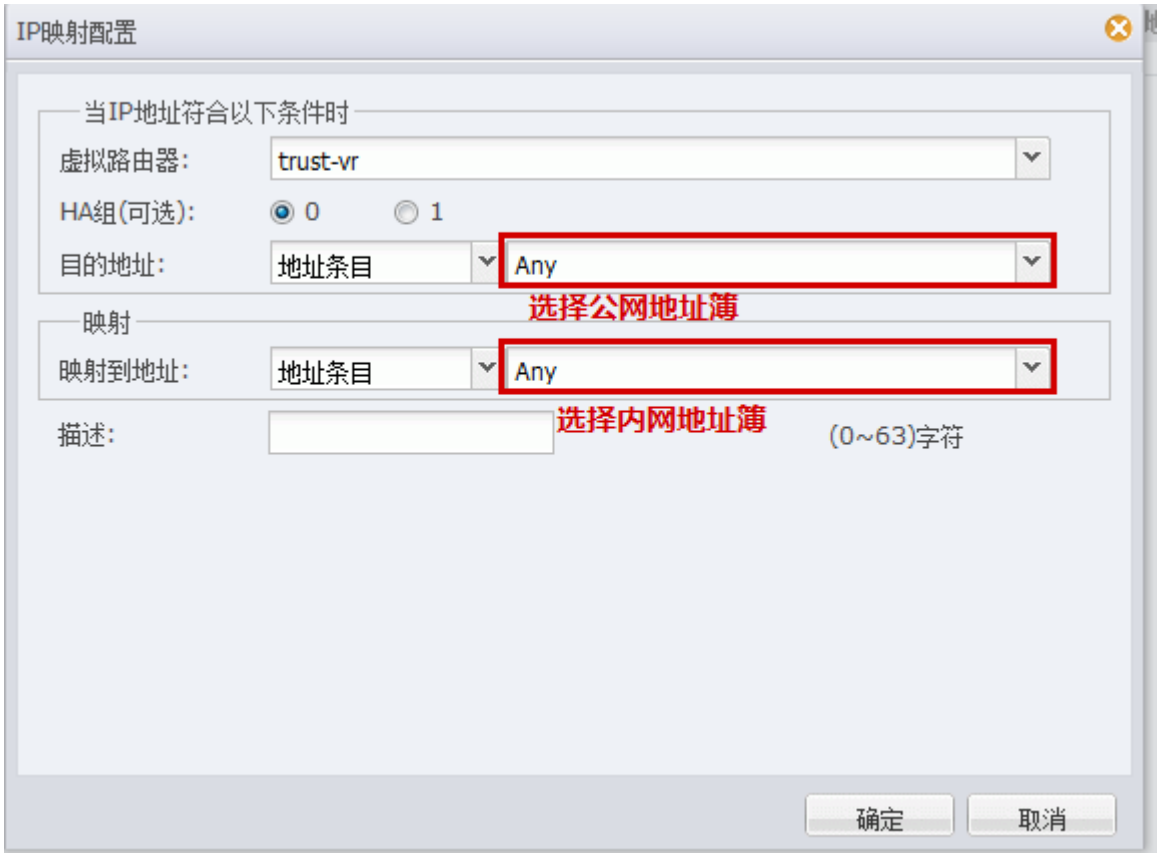
1. **创建两个地址簿(内网地址和外网地址)。**从工具栏的<对象用户>下拉菜单选择『地址簿』，弹出<地址簿>对话框。点击『新建』按钮，弹出<配置地址簿>对话框。

注意：针对此配置举例，掩码必须填写 32。

2. 同步骤 1，创建内网地址簿。

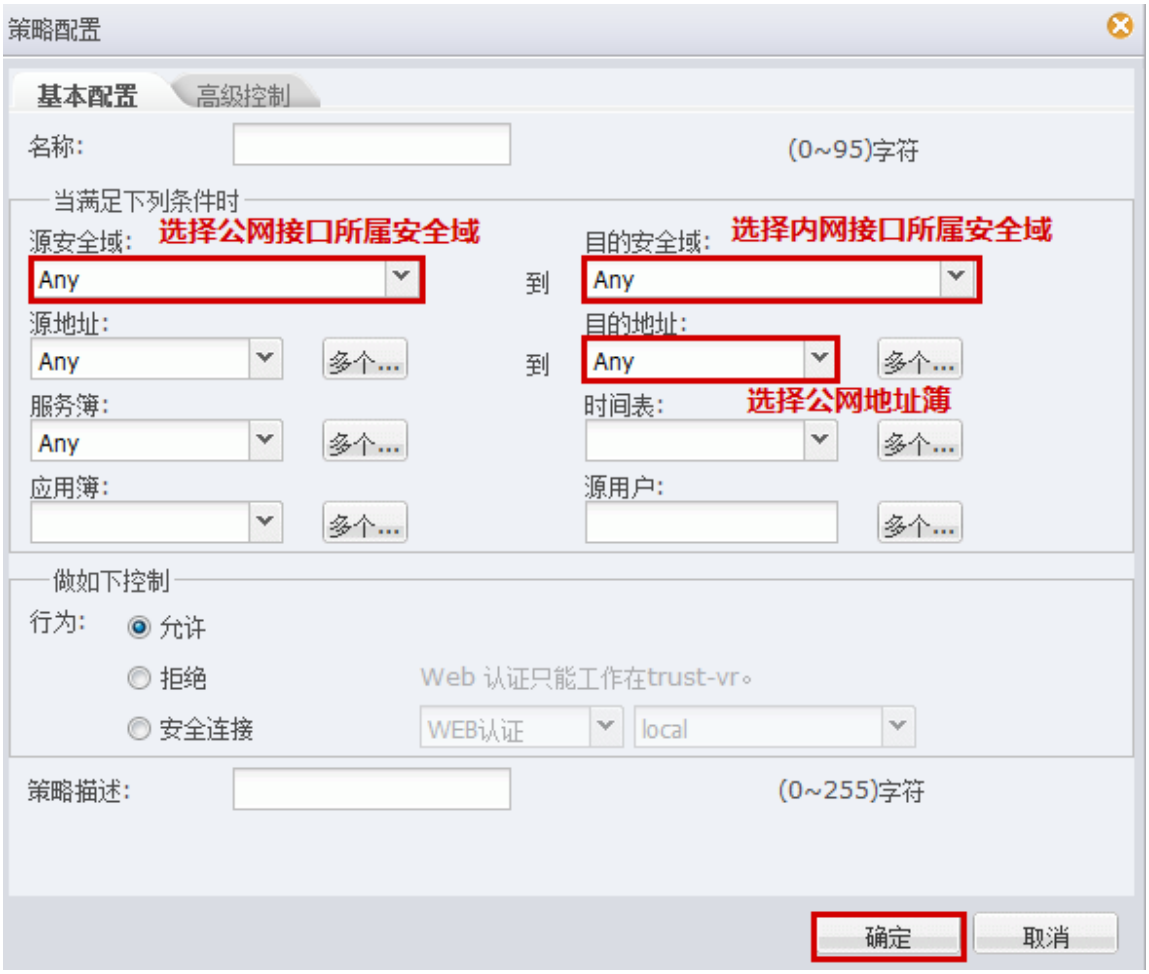


3. **新建目的 NAT IP 映射规则**。从页面左侧导航树选择并点击"配置->网络->NAT"，进入源 NAT 页面。点击『目的 NAT』标签，进入目的 NAT 页面。点击目的 NAT 列表中的『新建』按钮，并在弹出的下拉菜单中选择『IP 映射』，弹出<IP 映射配置>对话框。



4. **查看接口所在安全域。**点击目的 NAT 列表中的『新建』按钮，并在弹出的下拉菜单中选择『IP 映射』，弹出<IP 映射配置>对话框。从页面左侧导航树选择并点击"配置->网络->网络连接"，进入网络连接页面，在接口列表查看接口所在安全域。

5. 创建 untrust -> trust 的策略规则。从页面左侧导航树选择并点击"配置->安全->策略"，进入策略页面。点击列表左上角的『新建』按钮，弹出<策略配置>对话框，在该对话框对策略规则进行编辑。

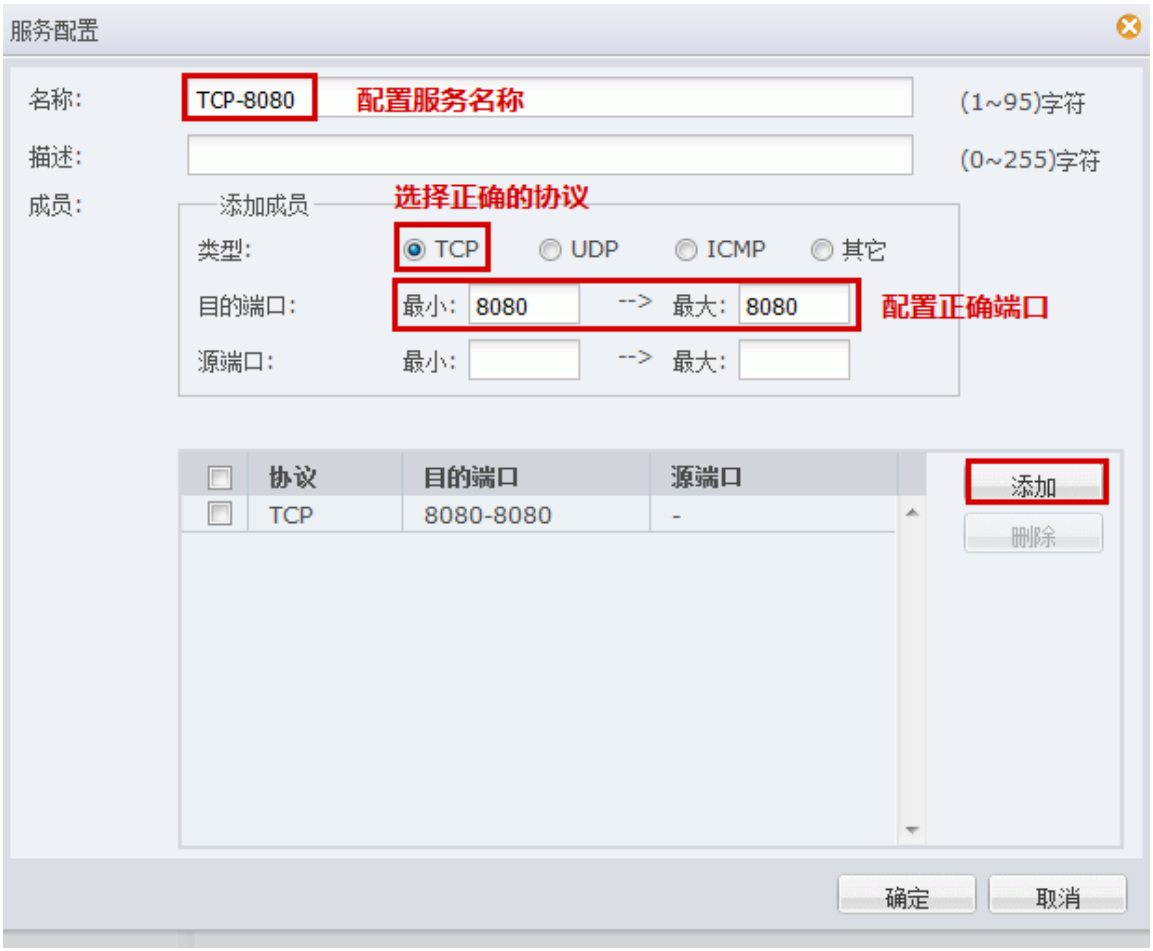


一对一端口映射

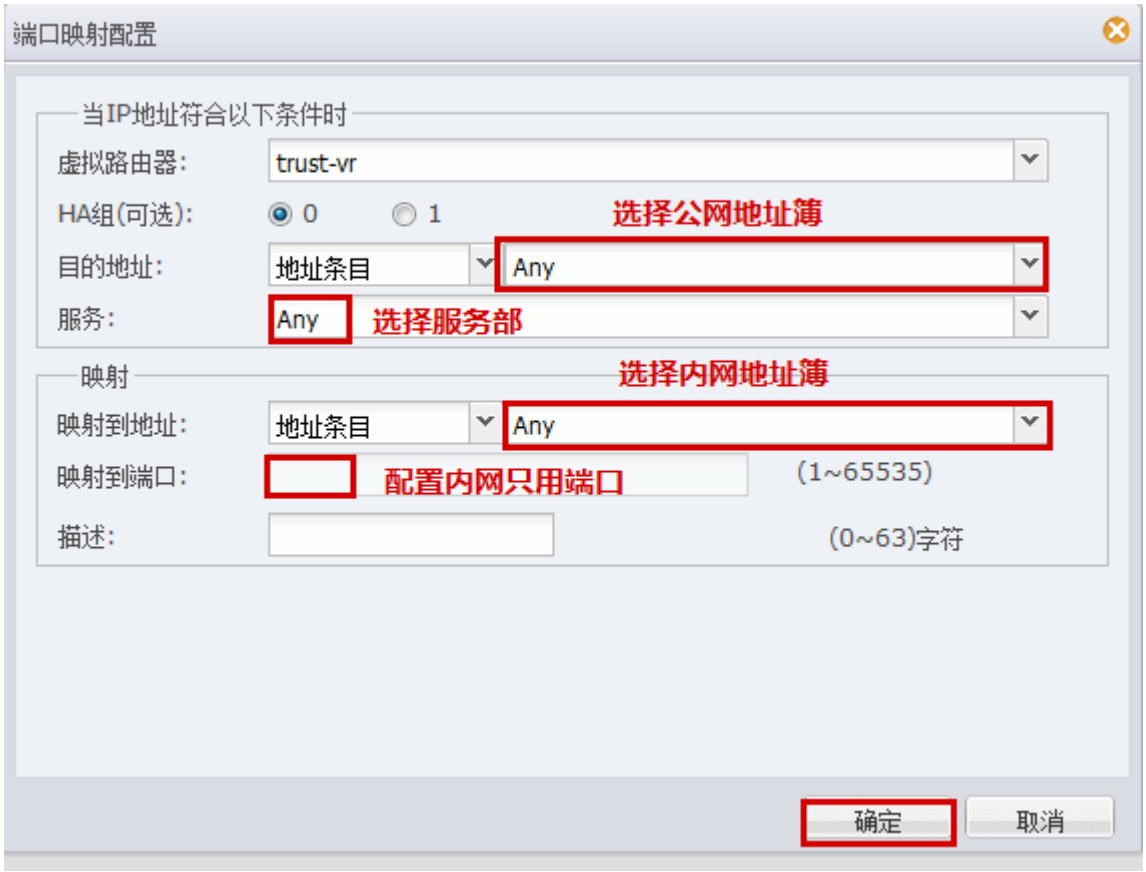
配置举例：将公网地址 60.0.0.1 的 TCP 8080 端口映射到内网地址 192.168.1.100 的 80 端口。

请按照以下步骤进行配置：

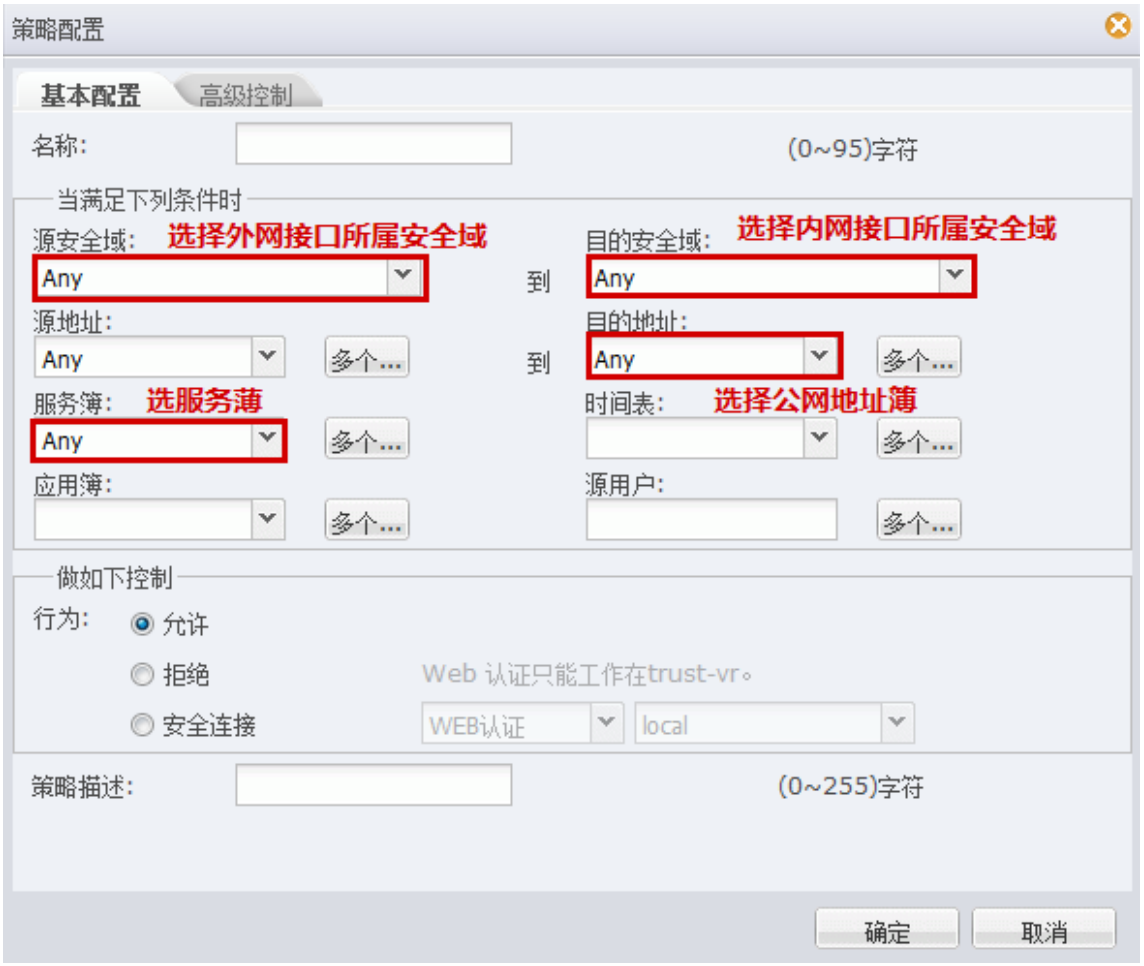
1. **创建两个地址簿（内网地址和外网地址）**。请参阅一对一 IP 映射步骤 1-2。
2. 根据所需映射的公网地址端口（8080），创建服务。从工具栏的<对象用户>下拉菜单选择『服务簿』，弹出<服务簿>对话框。选中<新建>下拉菜单中的『服务』按钮，弹出<服务配置>对话框。



3. **新建目的 NAT 端口映射规则**。从页面左侧导航树选择并点击“配置->网络->NAT”，进入源 NAT 页面。点击『目的 NAT』标签，进入目的 NAT 页面。点击目的 NAT 列表中的『新建』按钮，并在弹出的下拉菜单中选择『端口映射』，弹出<端口映射配置>对话框。



4. **查看接口所在安全域。**请参阅一对一 IP 映射步骤 4-5。



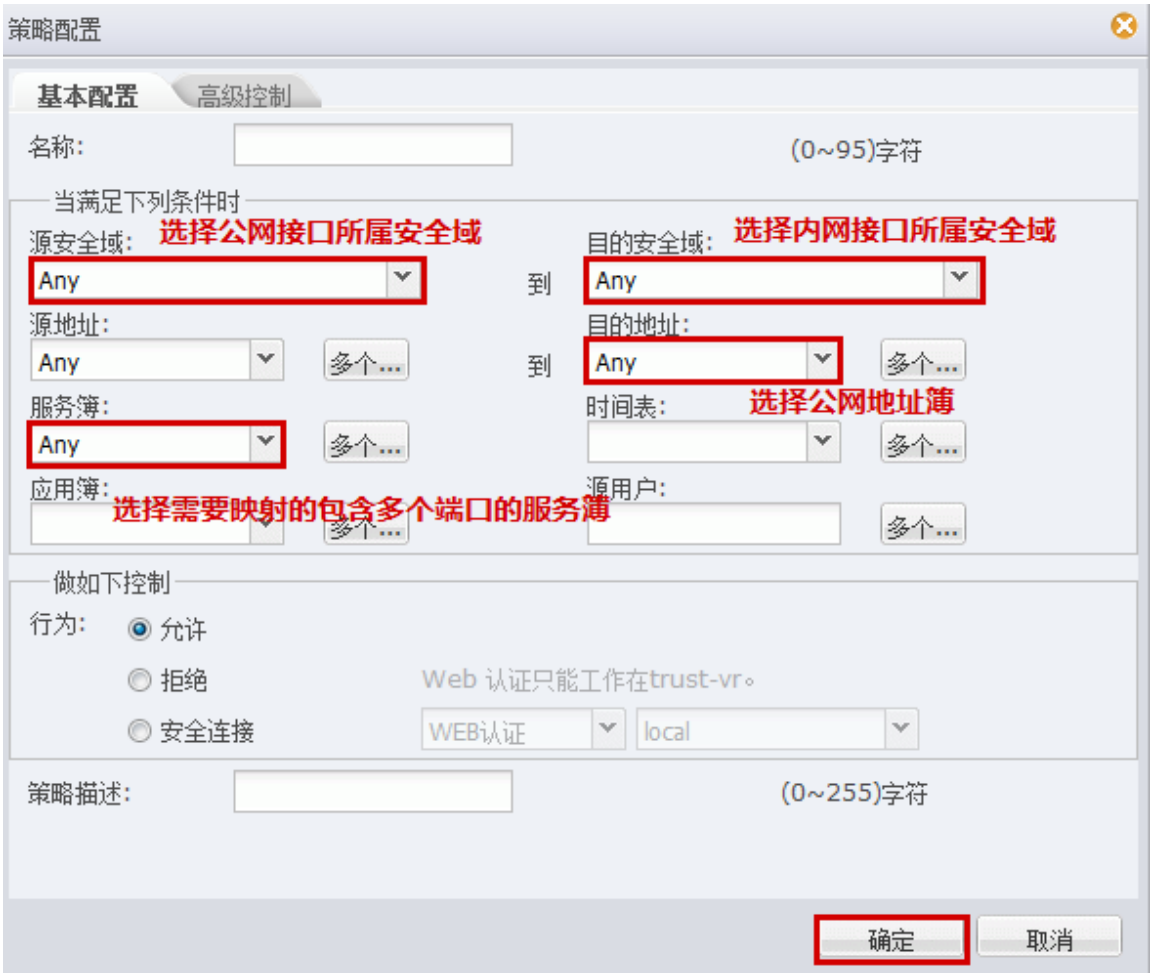
一对多映射（包含服务器负载均衡）

配置举例：将公网地址 60.0.0.1 的 tcp 80 端口映射到内网地址 192.168.1.1 和 192.168.1.3 的 80 端口，多台服务器进行负载均衡。

请按照以下步骤进行配置：

1. **创建两个地址簿（内网地址和外网地址）**。请参阅一对一 IP 映射步骤 1-2。
2. 根据所需映射的公网地址端口（80），创建服务。请参阅一对一端口映射步骤 2。
3. **目的 NAT 高级配置**。从页面左侧导航树选择并点击“配置->网络->NAT”，进入源 NAT 页面。点击『目的 NAT』标签，进入目的 NAT 页面。点击目的 NAT 列表中的『新建』按钮，并在弹出的下拉菜单中选择『高级配置』，弹出<目的 NAT 配置>对话框。

4. **查看接口所在安全域**。请参阅一对一 IP 映射步骤 4-5。



第 4 章 链路负载均衡

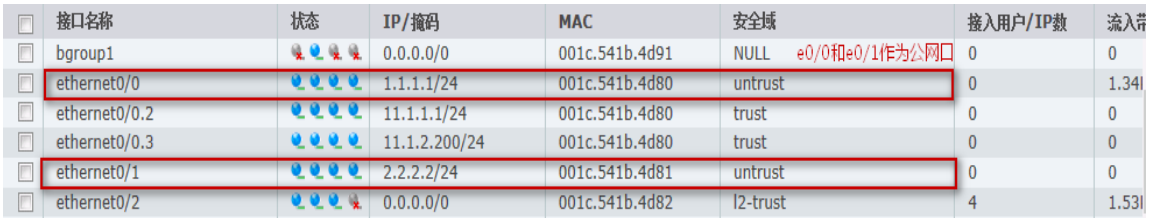
链路负载均衡介绍

对于多 ISP 链路用户，链路负载均衡功能可以通过动态链路探测技术将流量合理分发到不同链路，从而达到充分利用各条链路资源的目的。可以对内网的流量根据源地址、目的地址或者服务进行流量的负载分摊，以便保证流量的负载分担。

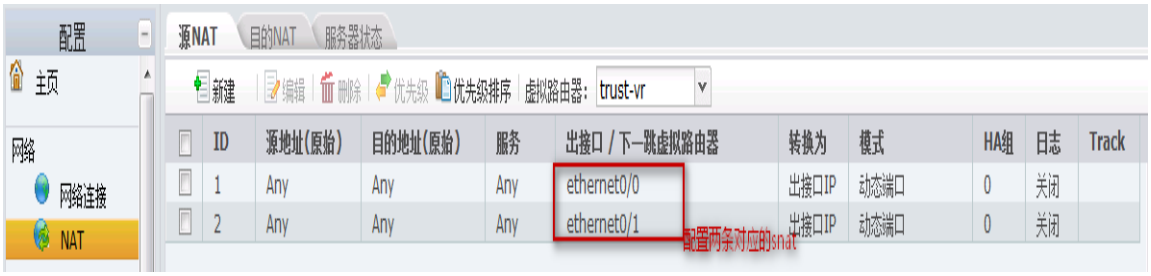
在配置源地址，目的地址的负载均衡后，可以实现冗余，当某一条路由失效时，可以保证正常的流量转发。

在配置链路负载均衡之前，先确保设备的接口、SNAT 和策略都已配置完成。

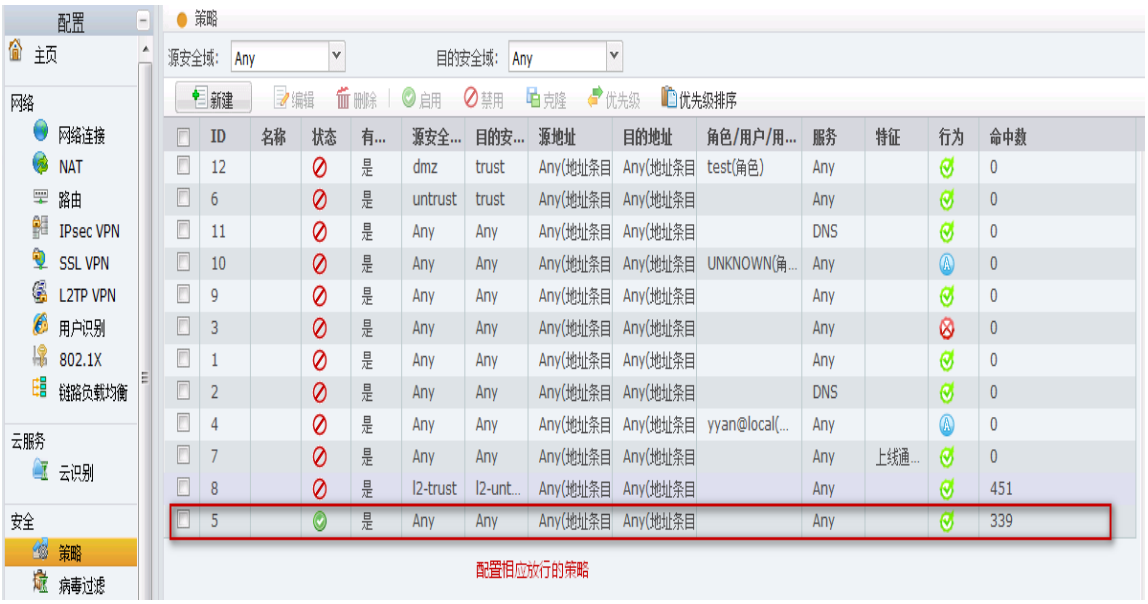
1. 接口的 IP 地址和掩码配置完成（掩码位数需要跟运营商确认）



2. SNAT 规则配置完成，使内网的流量可以分别 NAT 成对应公网出口地址池的地址，能够访问 Internet。



3. 策略规则配置完成。允许流量通过设备。



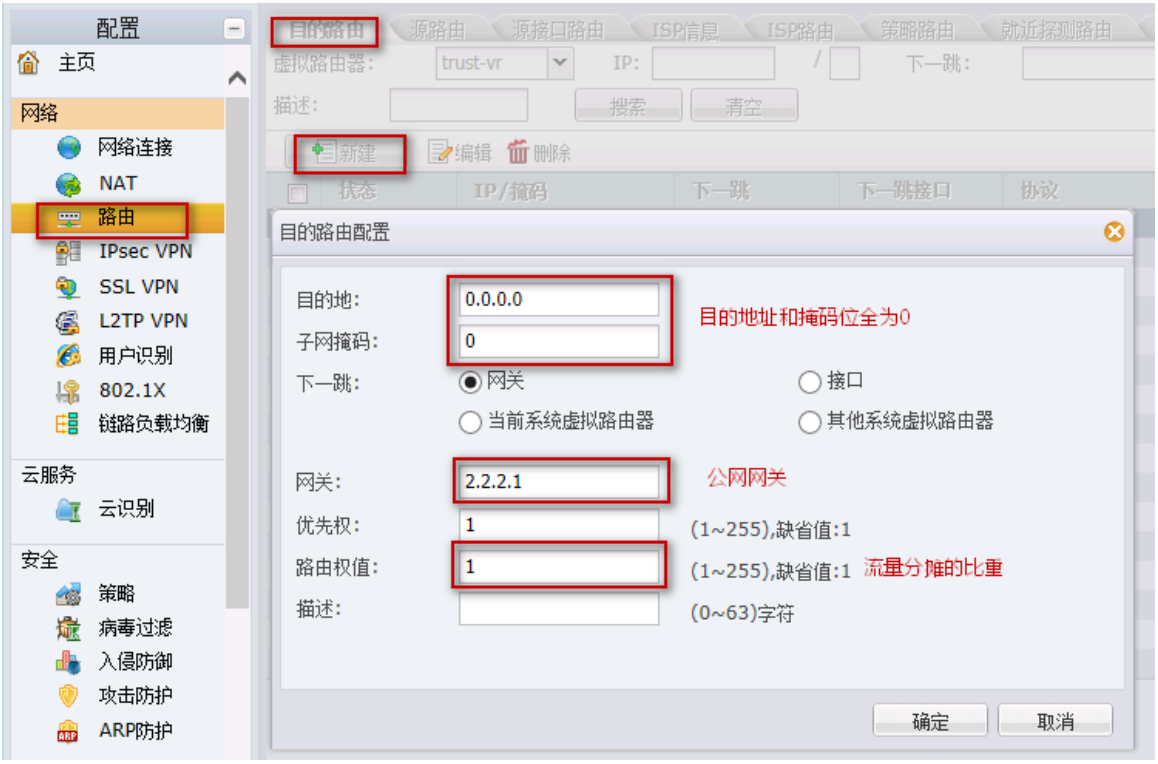
基于目的路由的负载均衡

配置举例：ethernet0/1 口接入 10M 带宽的运营商 A 链路，ethernet0/2 接入 20M 带宽的运营商 B 链路；实现所有访问公网的流量按 1：2 的比例分别从 ethernet0/1 口和 ethernet0/2 口转发出去。即当设备总共转发 3 数值的流量时，ethernet0/1 转发 1 数值；ethernet0/2 口转发 2 数值。

请按照以下步骤进行配置：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->网络->路由”，进入路由页面。点击『目的路由』标签，进入目的路由页面。点击目的路由列表左上角的

『新建』按钮，弹出<目的路由配置>对话框，在该对话框对目的路由进行编辑。



2. 再创建一条路由权值为 2 的路由条目，方法同步骤 1。

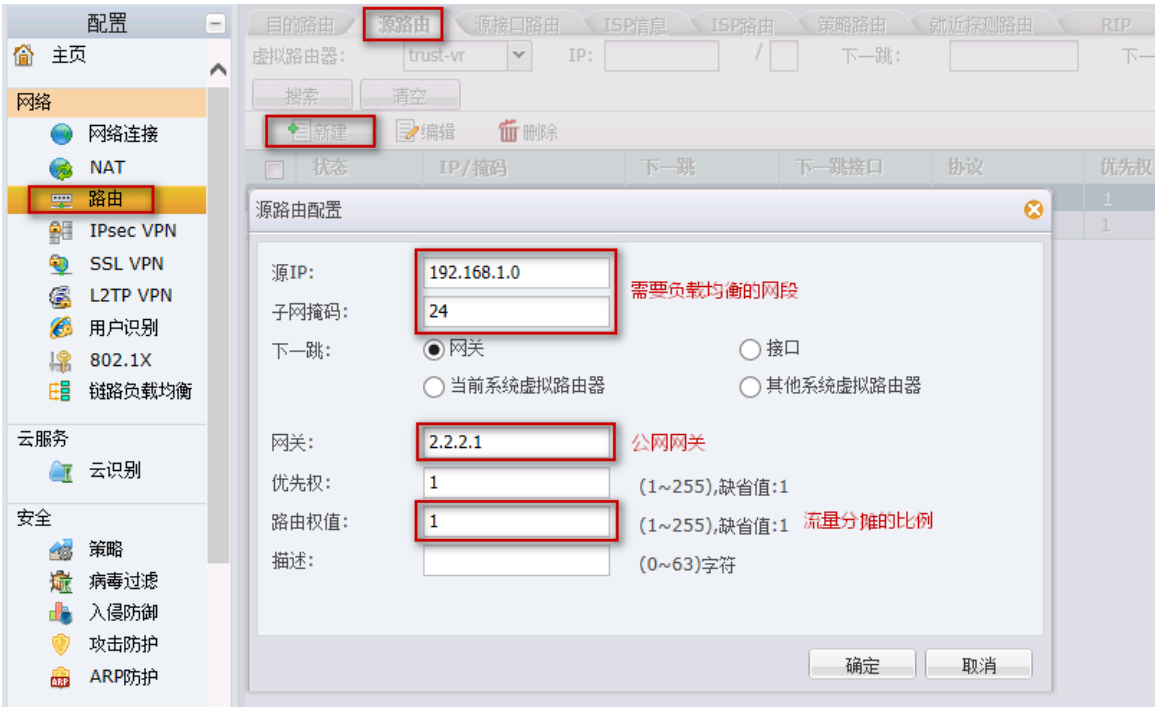
3. 完成配置后，即可实现流量从 ethernet 0/1 转发和从 ethernet 0/2 转发的比是 10：20 即流量的 1：2 负载均衡。具体比例可根据出口带宽的大小以及实际使用率确定。

基于源路由的负载均衡

配置举例：负载均衡来自 192.168.1.1/24 网段的流量。

请按照以下步骤进行配置：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->网络->路由”，进入路由页面。点击『源路由』标签，进入源路由页面。点击源路由列表左上角的『新建』按钮，弹出<源路由配置>对话框，在该对话框对源路由进行编辑。



2. 再创建一条网关为 3.3.3.1、路由权值为 2 的路由条目，方法同步骤 1。

3. 完成配置后，即可实现来自 192.168.1.1/24 网段的流量从 e0/1 转发和从 e0/2 转发的比是 1：2，具体比例可根据出口带宽的大小以及实际使用率确定。

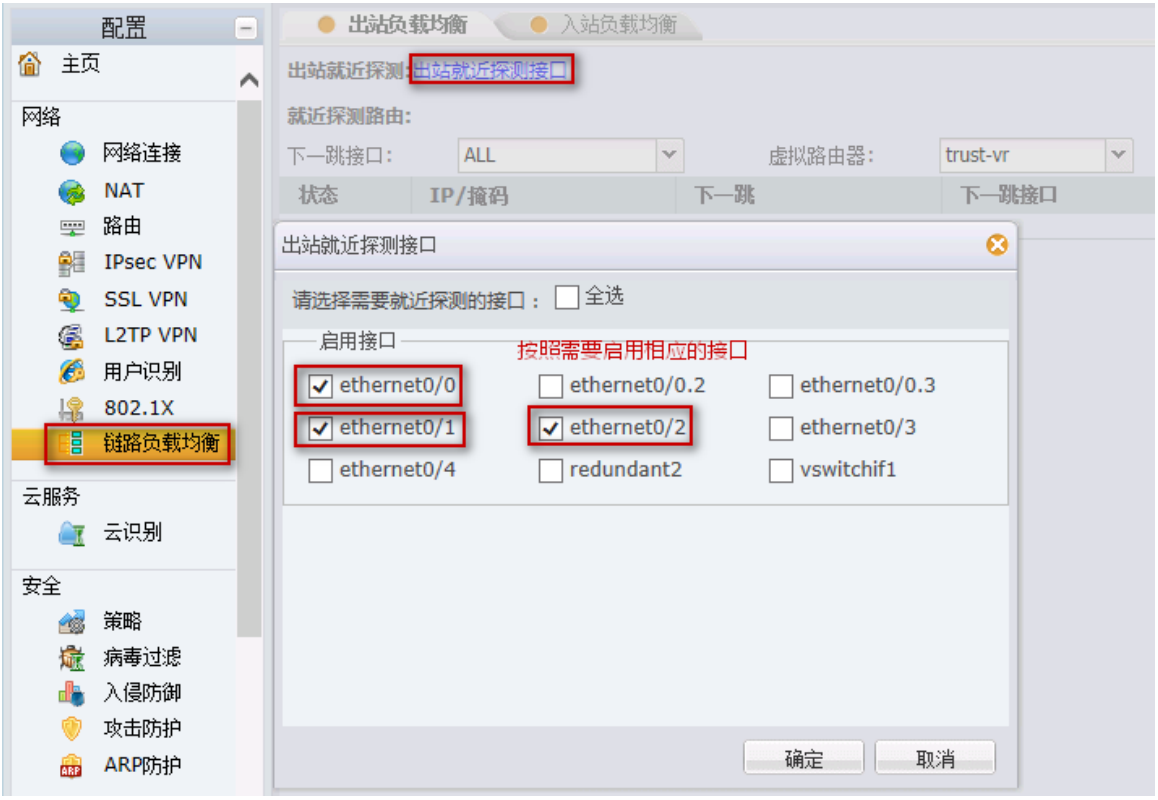
智能链路负载均衡

当内网用户向外网目标地址首次发起访问时，系统对匹配到默认路由的流量在符合条件的链路上进行探测，对响应相对快速的接口生成静态路由，后续报文将直接按照路由转发不再探测；如果生成的静态路由在一定时间内不被命中，则自动老化。

请按照以下步骤进行配置：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击“配置->网络->链路负载均衡”，进入链路负载均衡页面。
2. 点击『出站负载均衡』标签，进入出站负载均衡页面。
3. 在页面左上角点击『出站就近探测接口』，弹出<出站就近探测接口>配置对话框。
4. 选择需要启用出站就近探测的接口（即启用出站负载均衡功能的接口）。并点击『确定』按

钮。



5. 在页面右侧辅助栏的<任务>区对就近探测路由进行配置：

- **老化时间**：指定就近探测路由的老化时间，单位为分钟。取值范围是 1 到 1440 分钟，默认值为 10 分钟。如果在老化时间结束后仍没有流量匹配该路由，系统认为该路由已经老化失效，并从路由表中删除；
- **子网掩码**：指定就近探测路由的掩码。安全网关支持两种格式：*A.B.C.D* 和 *num*。*A.B.C.D* 的取值范围是 255.0.0.0 到 255.255.255.255 默认值为 255.255.255.0；*num* 的取值范围是 8 到 32，默认值为 24。

第 5 章 QoS 配置

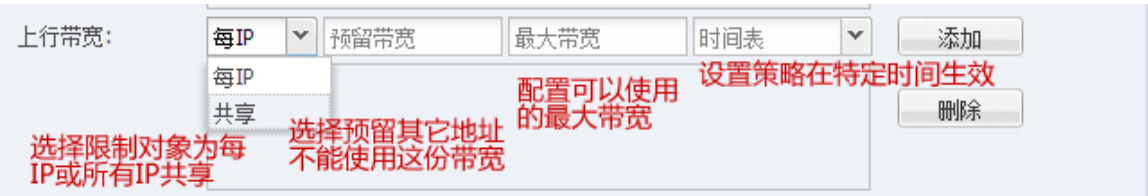
QoS 介绍

QoS（Quality of Service）即"服务质量"。它是指网络为特定流量提供更高优先服务的同时控制抖动和延迟的能力，并且能够降低数据传输丢包率。当网络过载或拥塞时，QoS 能够确保重要业务流量的正常传输。QoS 是网络中管理数据流的可用带宽、延迟、抖动以及分组丢失的技术集合。所有的 QoS 机制的目的就是影响这些特征中的至少一个，某些情况下甚至是全部。

IP QoS 配置

IP QoS 配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS，从页面左侧导航树选择并点击"配置->控制->流量管理"，进入 QoS 配置页面。
2. 点击『IP QoS』标签，页面将出现 IP QoS 列表。
3. 点击 IP QoS 列表上方的『新建』按钮，弹出<IP QoS>对话框。
4. 在『基本配置』标签页，进行 IP QoS 规则的基本配置。



5. 在『高级配置』标签页，可根据需要，配置如下功能：

- **配置弹性 QoS**。可设置最大弹性带宽，当接口存在闲置带宽时可暂时突破 QoS 的闲置以避免资源浪费，必须在主页开启全局弹性 QoS 时才能生效。用户可选择为上行流量或下行流量配置该功能。

  启用 - 选中该复选框开启弹性 QoS 功能。

  最大弹性带宽 - 开启弹性 QoS 功能后，该选项用来指定最大弹性带宽，即带宽上涨的最大限制 单位为 Kbps。默认值是 IP 配置带宽的 100 倍。取值范围是 64 到 1000000。；

- **配置细粒度控制**。为 IP QoS 规则嵌套应用 QoS 规则，系统将为不同 IP 按照指定的应用 QoS 规则分配应用带宽，实现 IP QoS 的细粒度控制。用户可选择为上行流量或下行流量配置该功能。点击『嵌套应用 QoS 规则』链接，弹出<嵌套应用 QoS 配置>对话框，配置方式与配置应用 QoS 规则的方式相同。用户可在嵌套应用 QoS 规则列表中点击『编辑』或『删除』按钮，进行相应的编辑或删除操作

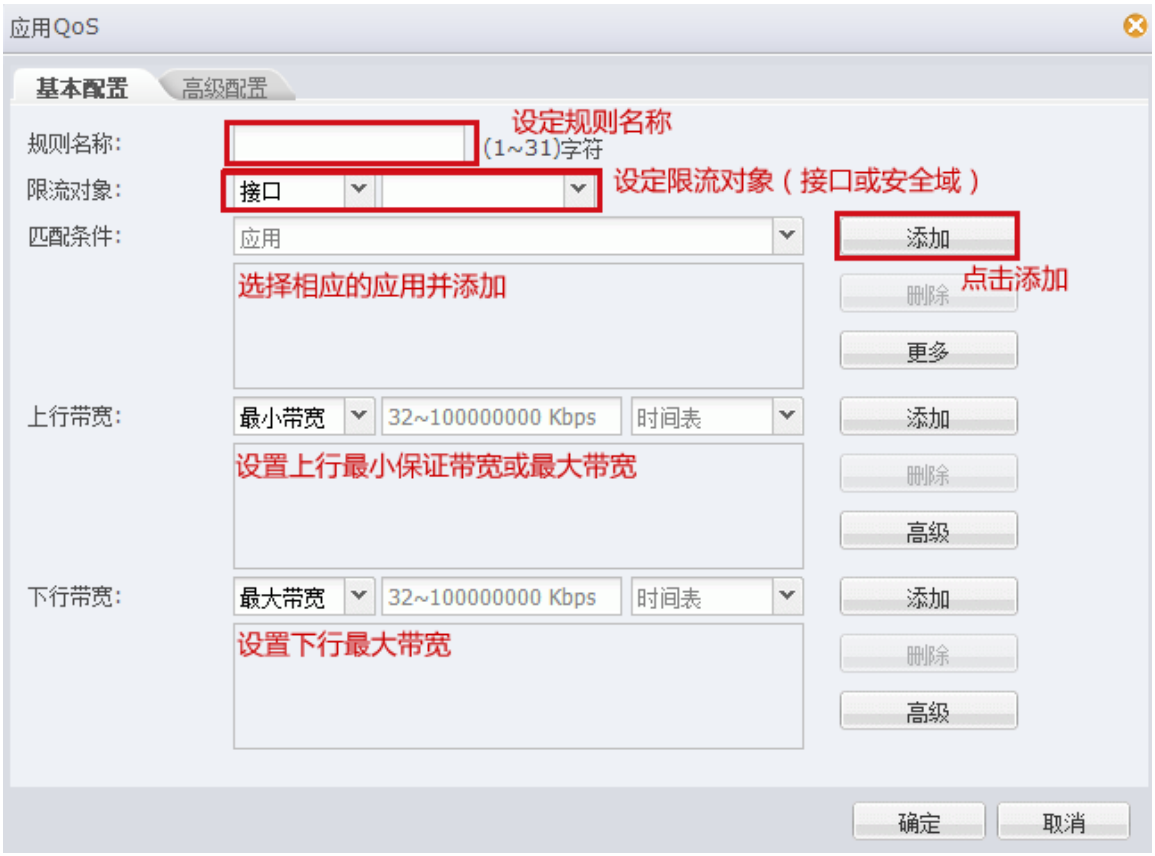
注意：使用应用 QoS 需要打开相应安全域的应用识别以及安装应用特征库许可证。

配置举例 :配置 192.168.1.2 至 192.168.1.200 范围内 IP 在 ethernet0/2 每 IP 上下行预留带宽 200K，最大带宽 1M，如下图所示：

应用 QoS 配置

应用 QoS 配置，请按照以下步骤进行操作：

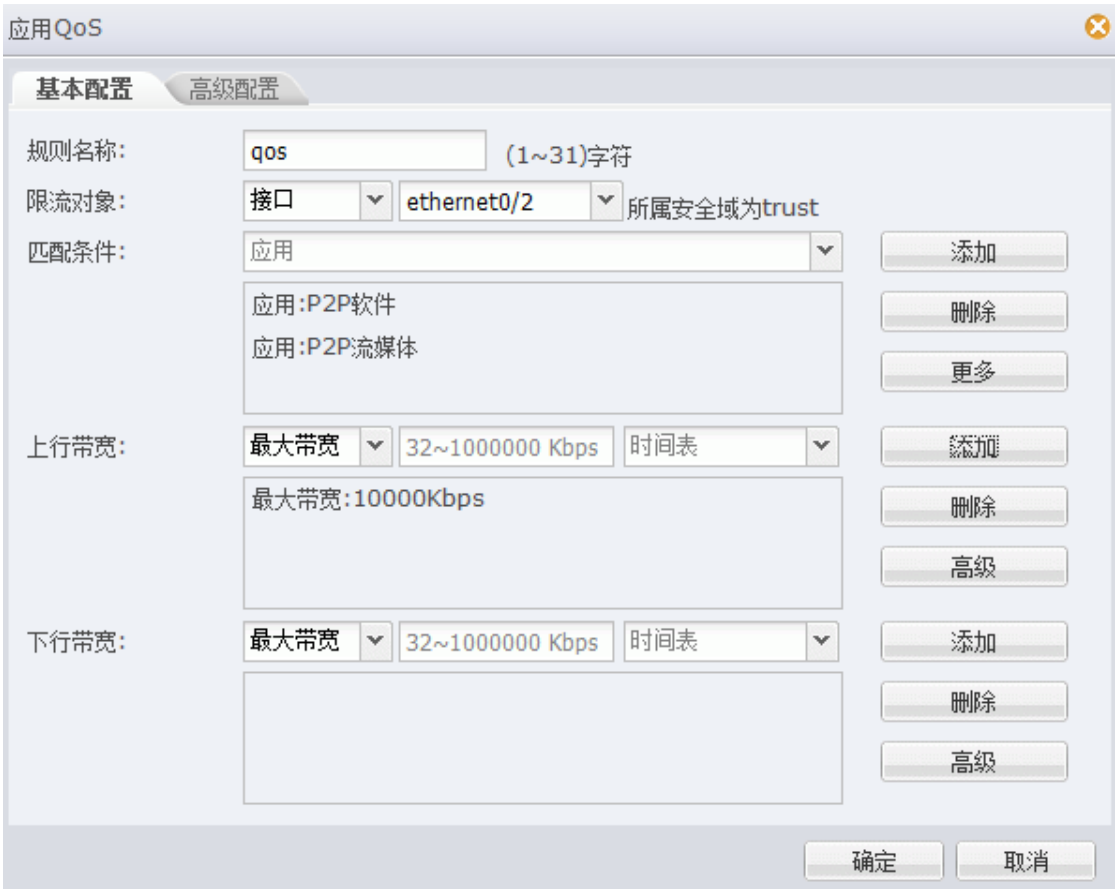
1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击“配置->控制->流量管理”，进入 QoS 配置页面。
2. 点击应用 QoS 列表上方的『新建』按钮，弹出<应用 QoS>对话框。
3. 在『基本配置』标签页，进行应用 QoS 规则的基本配置。



4. 在『高级配置』标签页，可根据需要，配置细粒度控制。在<嵌套 QoS 类型>下拉菜单中选择 IP QoS，然后点击『嵌套 IP QoS 规则』链接，弹出<嵌套 IP QoS 配置>对话框，配置方式与 IP QoS 配置相同。

注意：使用应用 QoS 需要打开相应安全域的应用识别以及安装应用特征库许可证。

配置举例：限制 P2P 软件及 P2P 流媒体在 ethernet0/2 接口上行最大流量为 10M，如下图所示：

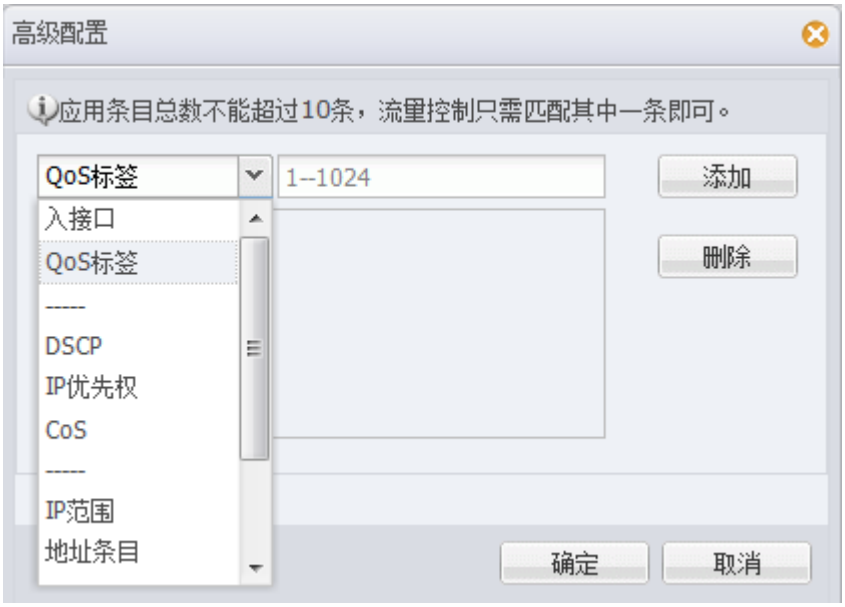


混合 QoS 配置

Hillstone 山石网科安全网关中的 QoS 除了有针对 IP 和应用外 ,还可以针对地址条目 ,角色，QoS 标签，IP 优先权以及 DSCP 等多项条件进行混合 QoS 配置以达到更精确的带宽管理。

混合 QoS 配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击“配置->控制->流量管理”，进入 QoS 配置页面。
2. 点击应用 QoS 列表上方的『新建』按钮，弹出<应用 QoS>对话框。
3. 在『基本配置』标签页，点击<匹配条件>右侧『更多』按钮，弹出<高级配置>对话框，可添加多项匹配条件。可针对策略标签，IP 优先权，IP 范围，地址条目等进行控制。



QoS 白名单配置

QoS 功能支持配置 IP 地址白名单。配置后，系统将对指定的流量不进行 QoS 控制。

配置 IP 地址白名单，请按照以下步骤进行操作：

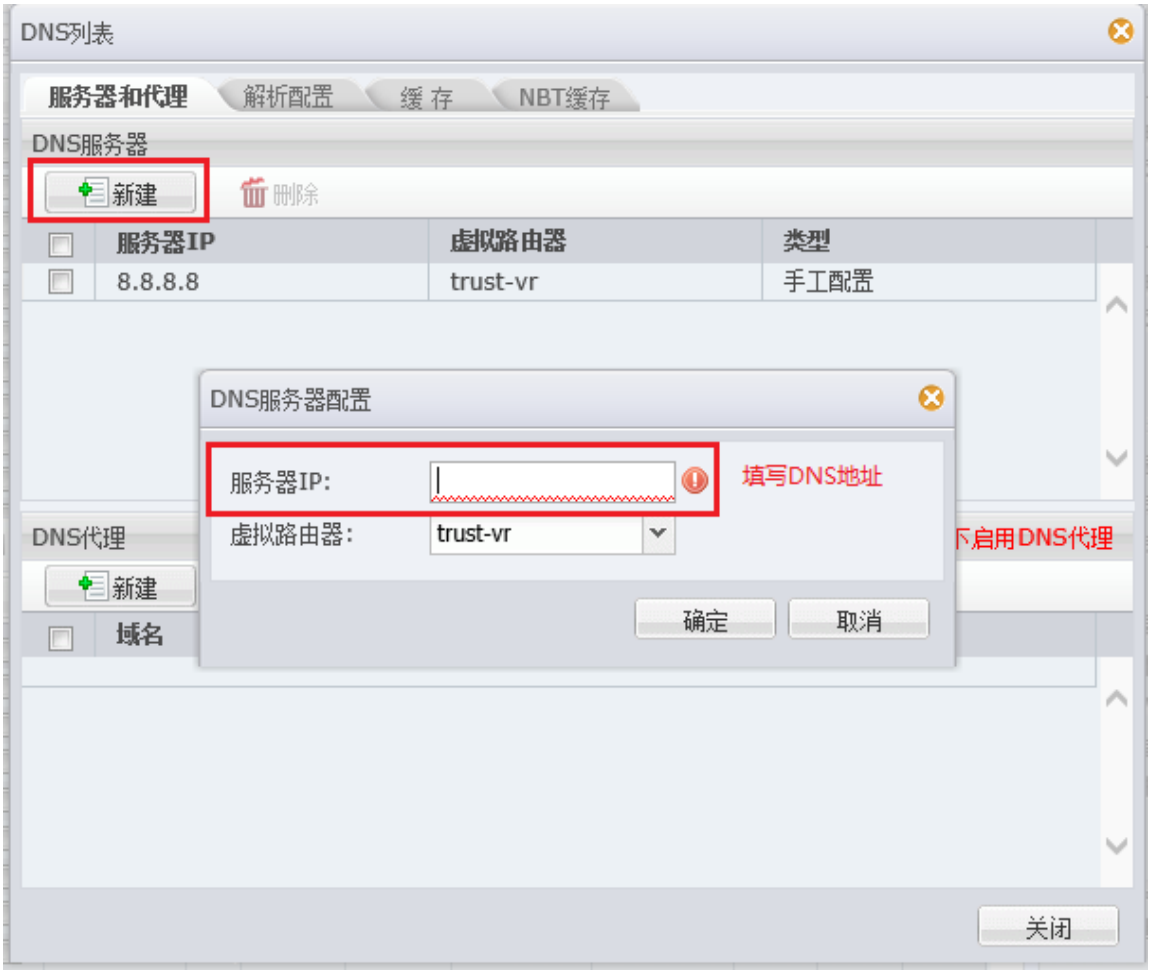
1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->控制->流量管理"，进入 QoS 配置页面。
2. 在『应用 QoS』标签下的<白名单>处指定不受 QoS 规则流量限制的 IP。可以选择指定 IP 范围或地址簿条目：
   - **IP 范围**：在文本框中输入起始 IP 地址和终止 IP 地址；
   - **地址条目**：在组合框中输入或选择地址簿中的地址条目。

第 6 章 网络行为控制

配置网络行为控制功能中的 URL 过滤、bypass 域名以及应用行为控制等与网络域名有关的功能时 ,需要现在设备上上进行 DNS 配置 ,并且尽量保证设备使用的 DNS 与内部电脑的 DNS 一致。

DNS 配置，，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->网络->网络连接"，进入网络连接页面。
2. 从页面右侧辅助栏的<任务>区选择『DNS 列表』链接，弹出<DNS 列表>对话框。
3. 选中『服务器和代理』标签，在<DNS 服务器>部分点击『新建』按钮，弹出<DNS 服务器配置>对话框。

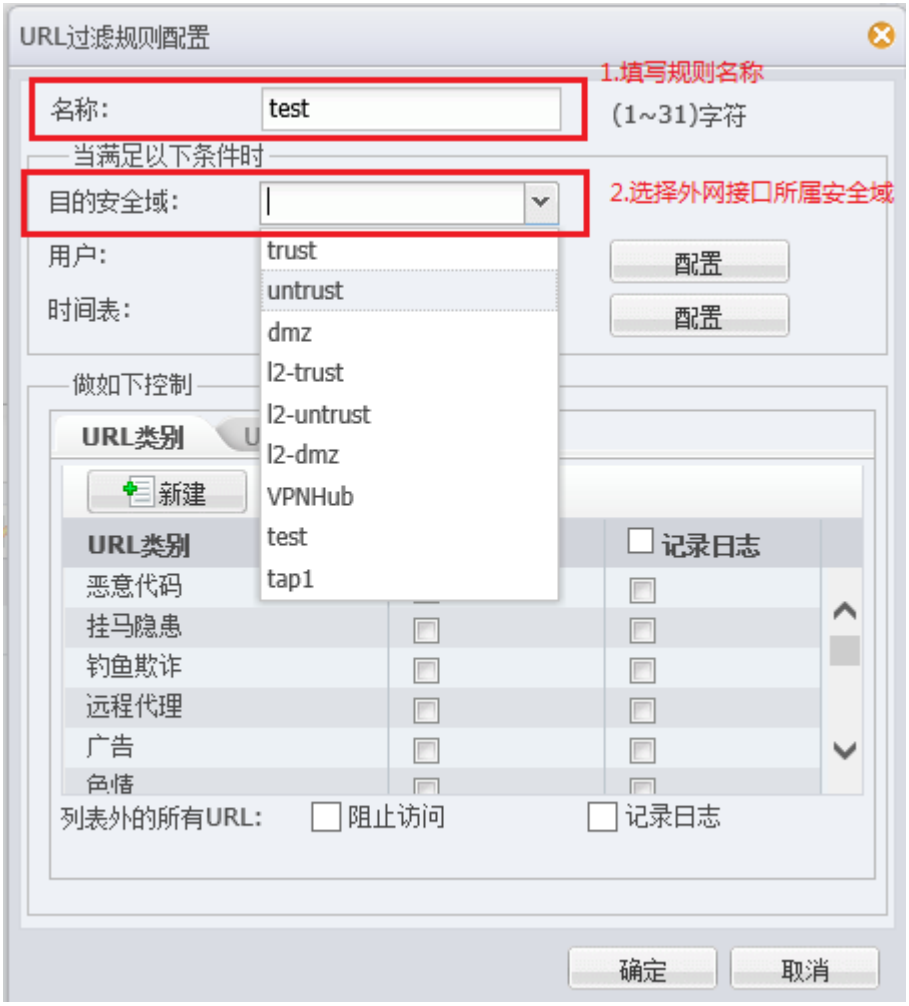


URL 过滤（有 URL 许可证）

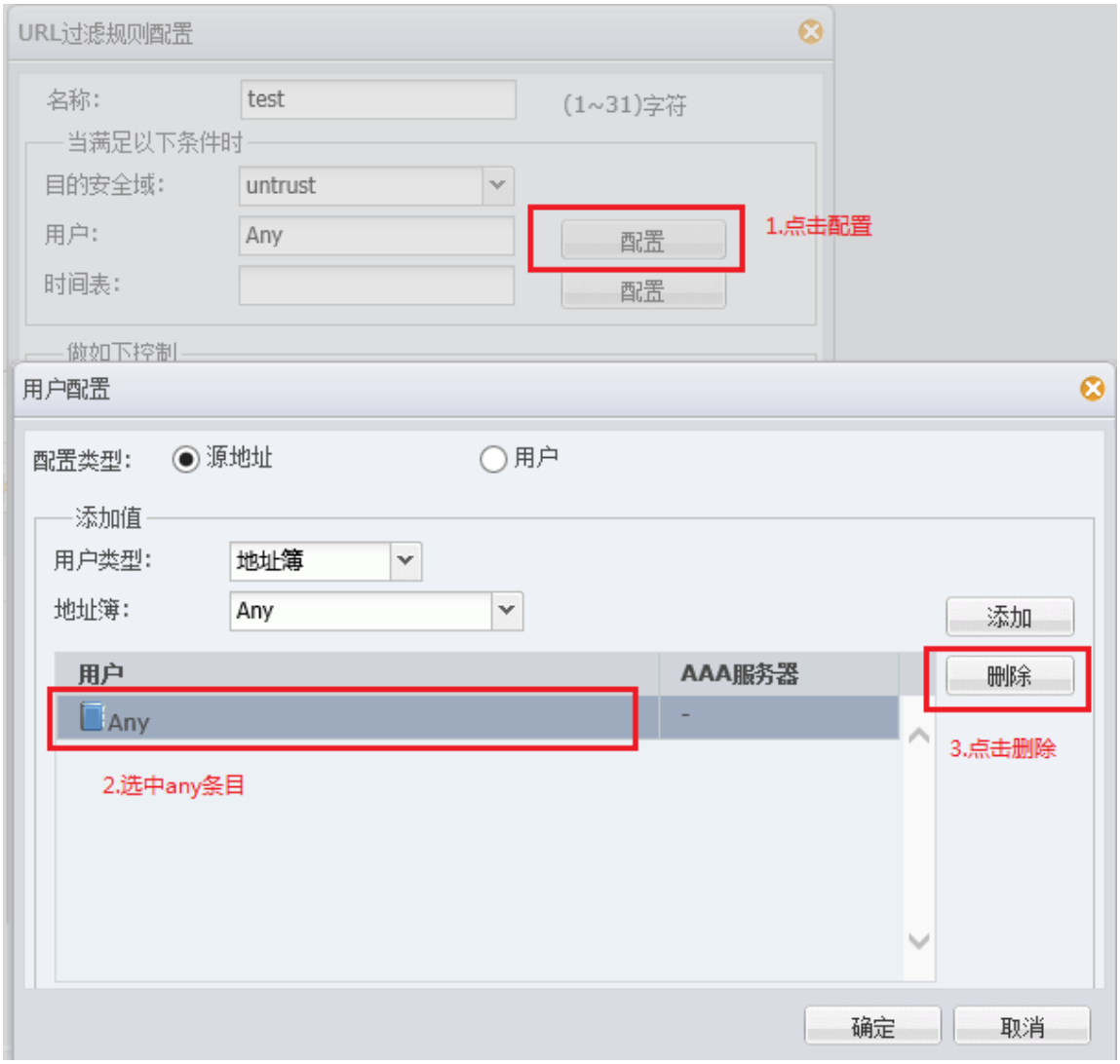
URL 过滤配置，请按照以下步骤进行操作：

1. 通过 WebUI 方式登录 StoneOS ,从页面左侧导航树选择并点击"配置->控制->URL 过滤"，进入 URL 过滤页面。

2. 点击『新建』按钮，弹出<URL 过滤规则配置>对话框。



3. 指定规则的用户，该用户可以为地址簿地址条目、IP 地址、IP 地址范围、角色、用户或用户组。系统默认用户为 Any，即对任意用户都有效，如果要修改，则先删除 any 用户。点击后面的『配置』按钮，在弹出的<用户配置>对话框中对用户进行修改。



4. 配置实际所需要限制的内网 IP 用户，注意掩码 32 表示单个主机 IP，如需整个网段则填写相应的网络掩码。在<用户类型>下拉菜单选中“IP”，需要在<IP 地址>文本框输入 IP 地址和网络掩码。

5. 在<做如下控制>部分配置规则的控制内容(URL 类别和 URL 关键字类别)和控制动作(阻止访问和记录日志)。（可选）

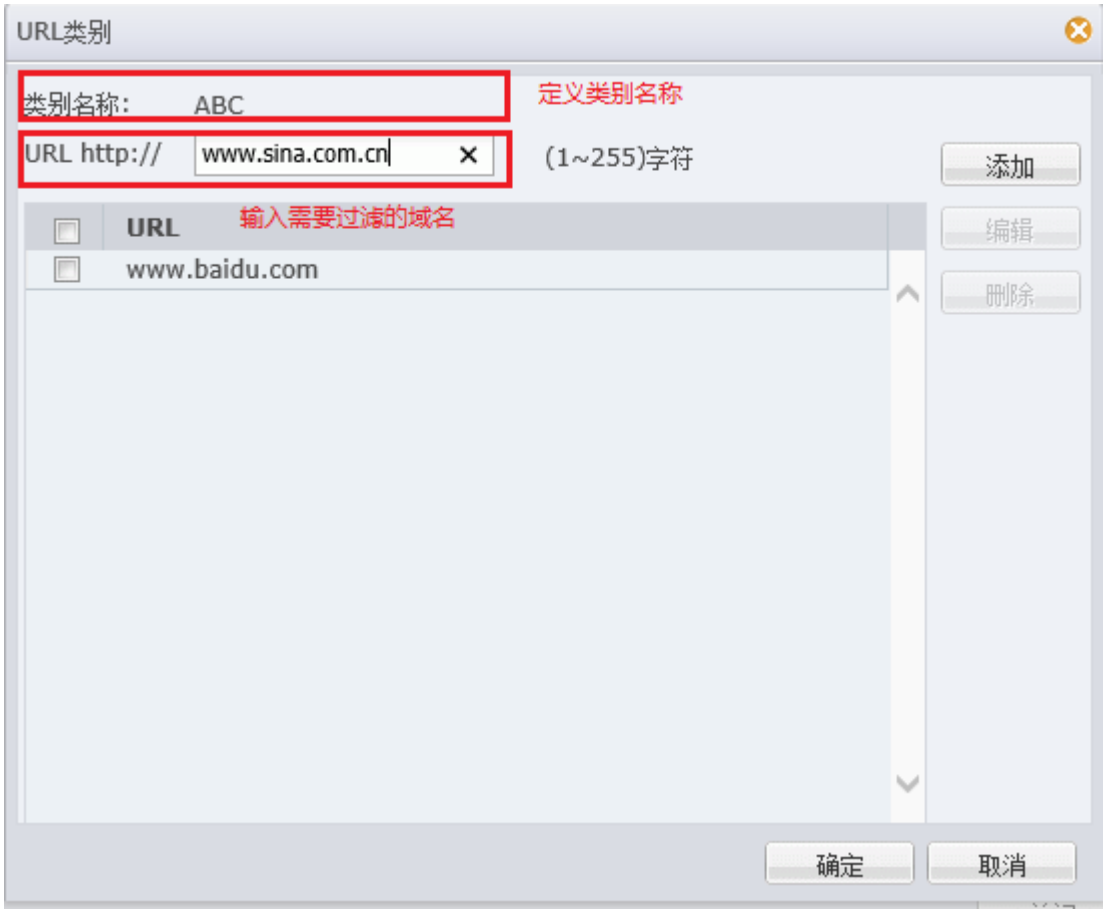
6. 完成上述配置，即可实现阻止内网 192.168.1.2 这个 IP 访问“恶意代码”和“挂马隐患”这两类网站。

配置自定义 URL 库

用户可以根据需要自定义 URL 类别。与预定义 URL 类别相同，自定义 URL 库能够为 URL 过滤功能配置、网页关键字过滤功能配置和 Web 外发信息控制功能配置提供 URL 类别。

新建 URL 类别，请按照以下步骤进行操作：

1. 从页面左侧导航树选择并点击“配置->控制->URL 过滤/网页关键字/Web 外发信息”，进入功能页面。
2. 从页面右侧辅助栏的<任务>区选择『自定义 URL 库』链接，弹出<自定义 URL 库>对话框。
3. 点击『新建』按钮，弹出<URL 类别>对话框。输入自定义 URL 类别名称和需要过滤的域名。



4. 点击『确定』按钮，保存所做配置。即可在配置 URL 过滤时找到自定义的 URL 类别，选择控制动作。

URL 过滤（无 URL 许可证）

URL 过滤配置，请按照以下步骤进行操作：

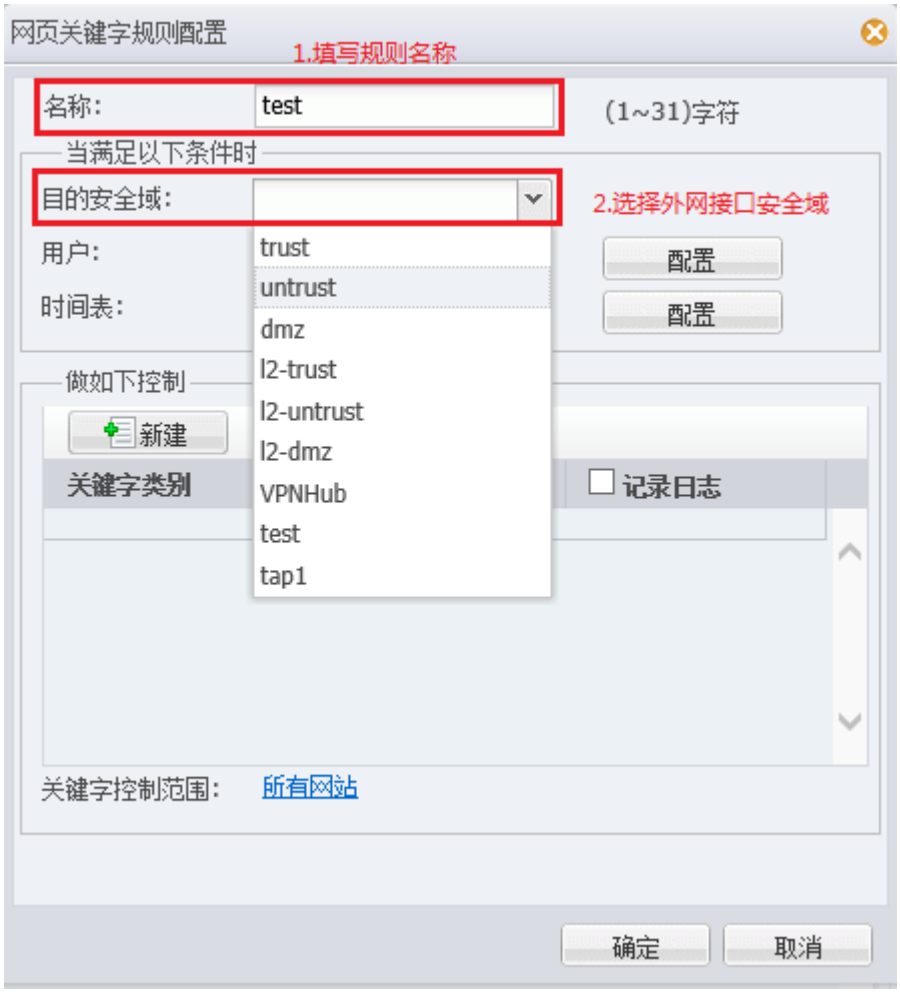
1. 新建 URL 过滤规则，步骤请参阅 URL 过滤（有 URL 许可证）步骤 1-4。
2. 在<URL 过滤规则配置>对话框中的<做如下控制>部分点击<HTTP 控制>，添加要阻止的网站，*号表示通配符，这样该网站的子域名也会一起被禁止，如果是仅需阻止单个域名，则填写该域名全称，也可以在用户访问该网站的时记录日志。（可选）

3. 完成上述配置，即实现了阻止内网 192.168.1.2 这个 IP 地址访问带 baidu.com 的所有网站。

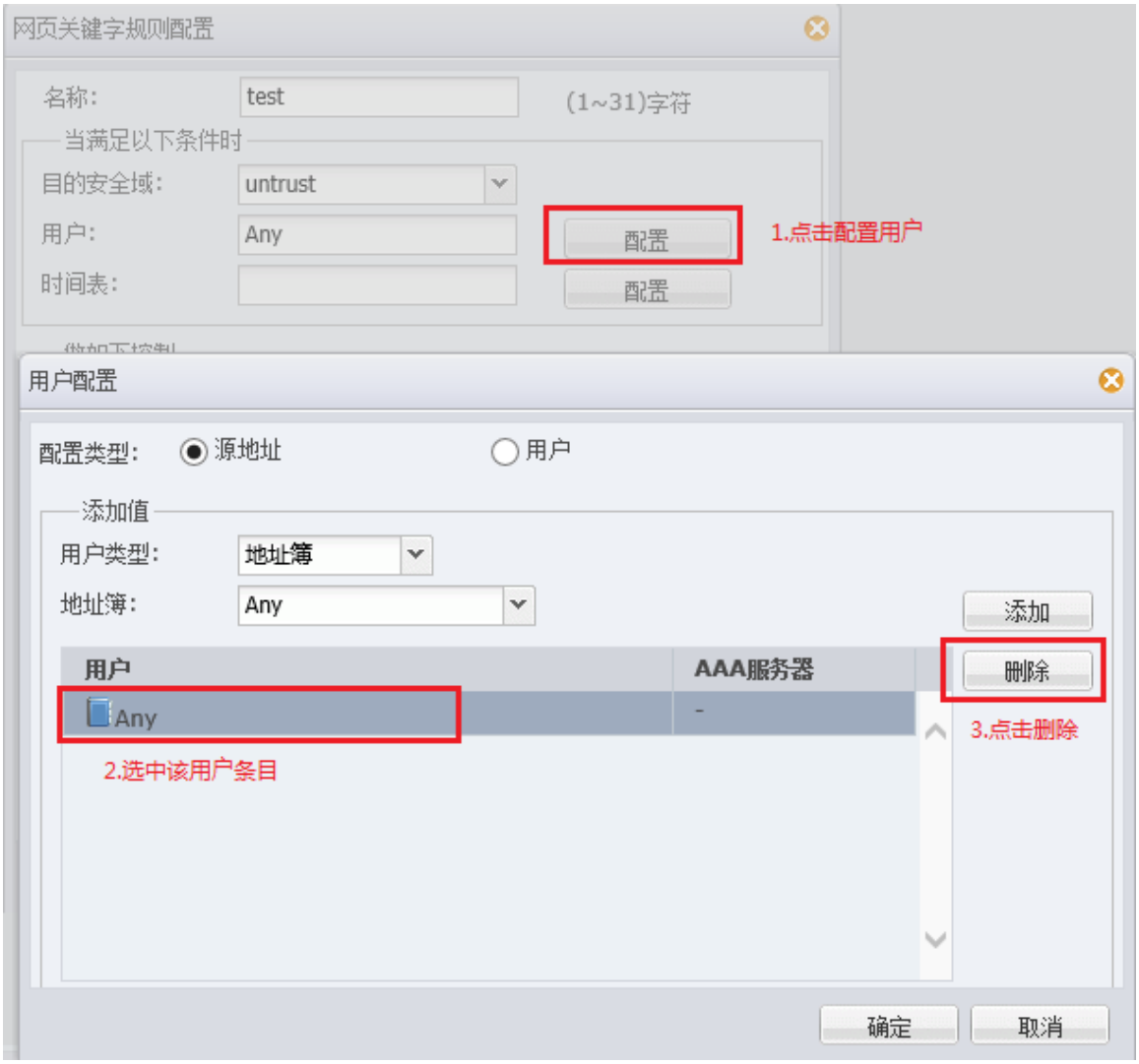
网页关键字过滤

新建网页关键字规则，请按照以下步骤进行操作：

1. 从页面左侧导航树选择并点击"配置->控制->网页关键字"，进入网页关键字页面。
2. 点击『新建』按钮，弹出<网页关键字规则配置>对话框。



3. 指定规则的用户，该用户可以为地址簿地址条目、IP 地址、IP 地址范围、角色、用户或用户组。系统默认用户为 Any，即对任意用户都有效，如果要修改，则先删除 any 用户。点击后面的『配置』按钮，在弹出的<用户配置>对话框中对用户进行修改。



4. 配置实际所需要限制的内网 IP 用户，注意掩码 32 表示单个主机 IP，如需整个网段则填写相应的网络掩码。在<用户类型>下拉菜单选中“IP”，需要在<IP 地址>文本框输入 IP 地址和网络掩码。

5. 在<做如下控制>部分配置规则的控制内容（网页关键字类别）和控制动作（阻止访问、记录日志和记录内容）。点击『新建』按钮，弹出<关键字类别配置>对话框。

6. 点击『新建』按钮，弹出<关键字类别>对话框进行新建关键字类别。并点击『确定』按钮保存所做配置并返回上一级对话框/页面。

7. 在<做如下控制>部分配置规则的控制内容。

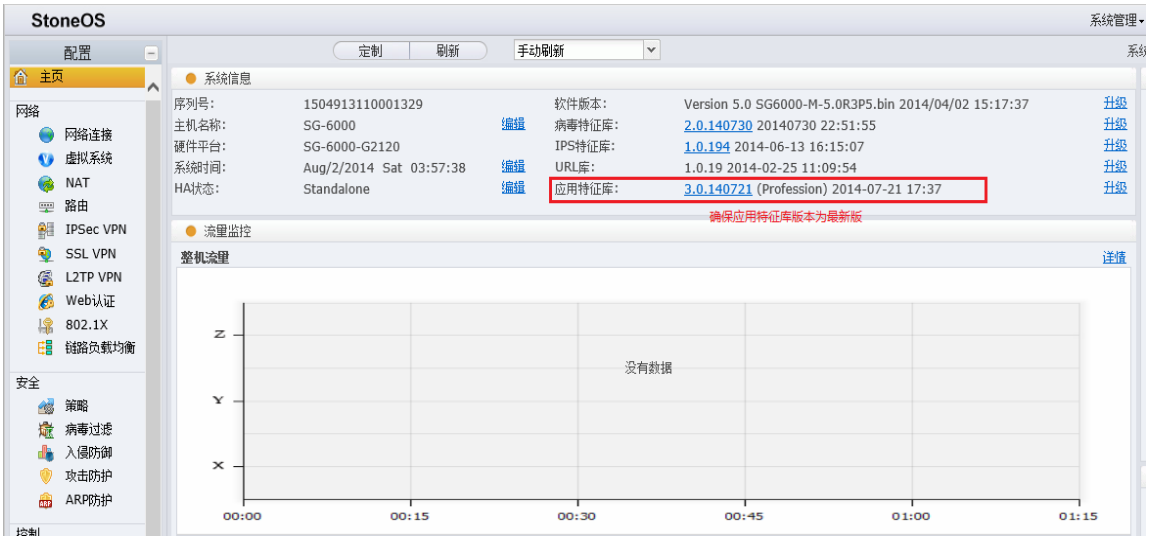
8. 完成上述配置，即实现了阻止内网 192.168.1.2 这个 ip 地址访问带有“赌博”关键字的网页。

网络聊天控制

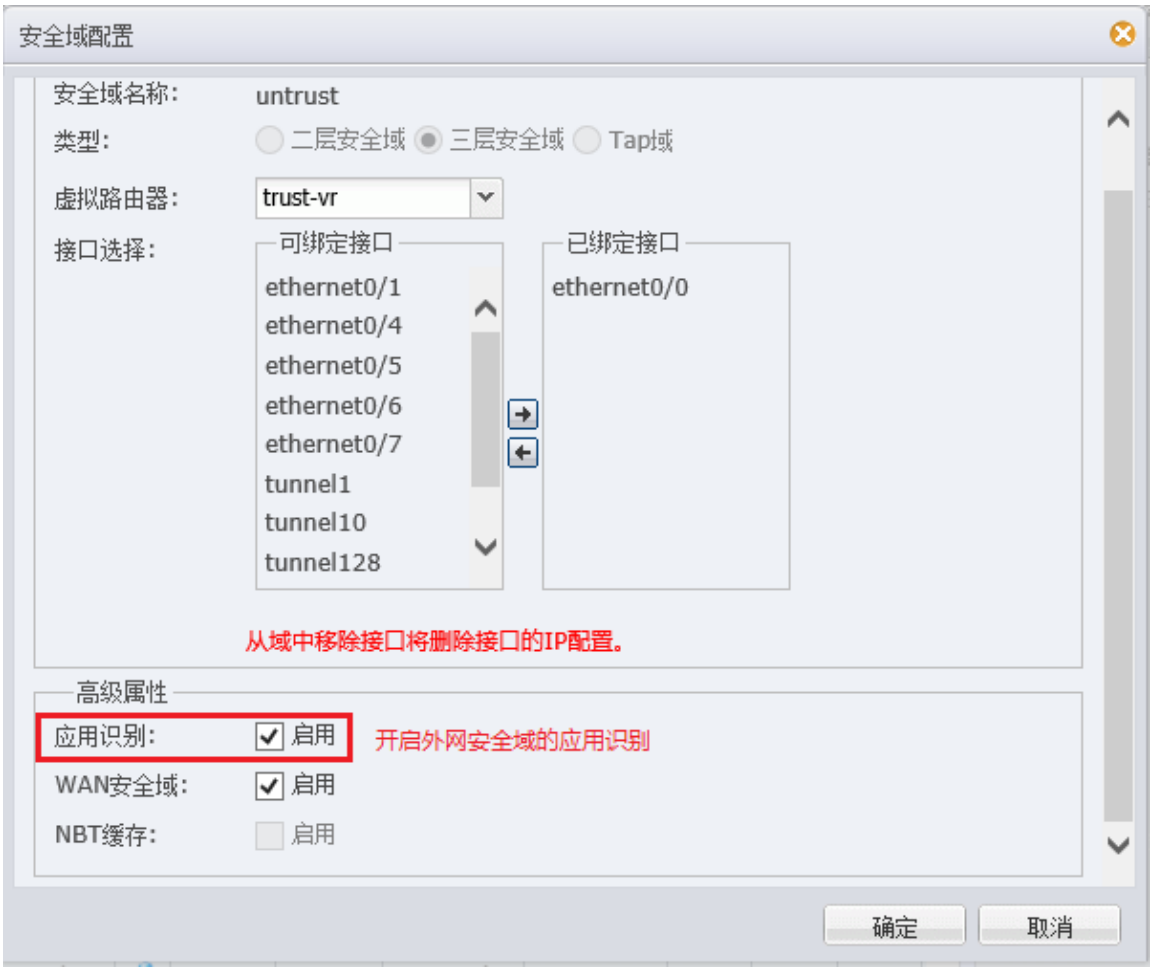
网络聊天功能可以通过聊天软件的账号控制用户使用 MSN、QQ 和雅虎通聊天的行为，并记录上下线日志。

以 QQ 为例，网络聊天控制配置，请按照以下步骤进行操作：

1. 确认设备已经安装了最新的应用特征库。



2. 开启内外安全域的应用识别功能。从页面左侧导航树选择并点击“配置->网络->网络连接”，进入网络连接页面。
3. 从安全域列表中选中安全域，然后双击或者点击列表左上方的『编辑』按钮。
4. 在弹出的<安全域配置>对话框的<高级属性>部分，选中<应用识别>复选框开启安全域的应用识别功能。



5. 新建网络聊天规则。从页面左侧导航树选择并点击“配置->控制->网络聊天”，进入网络聊天页面。点击『新建』按钮，弹出<网络聊天规则配置>对话框。

6. 如果想要阻止所有的 qq 账号都无法登录，则可以勾选<列表外的所有 QQ 账号>部分的<阻止使用>复选框，或者直接通过设备的策略规则进行对 qq 应用的阻止。

第 7 章 VPN 高级配置

基于 USB Key 的 SCVPN 配置

本节介绍基于 USB-KEY 的 SSL VPN 配置，其他 SSL VPN 配置请参阅 SCVPN 配置。

基于 UEB Key 的 SCVPN 配置包括：

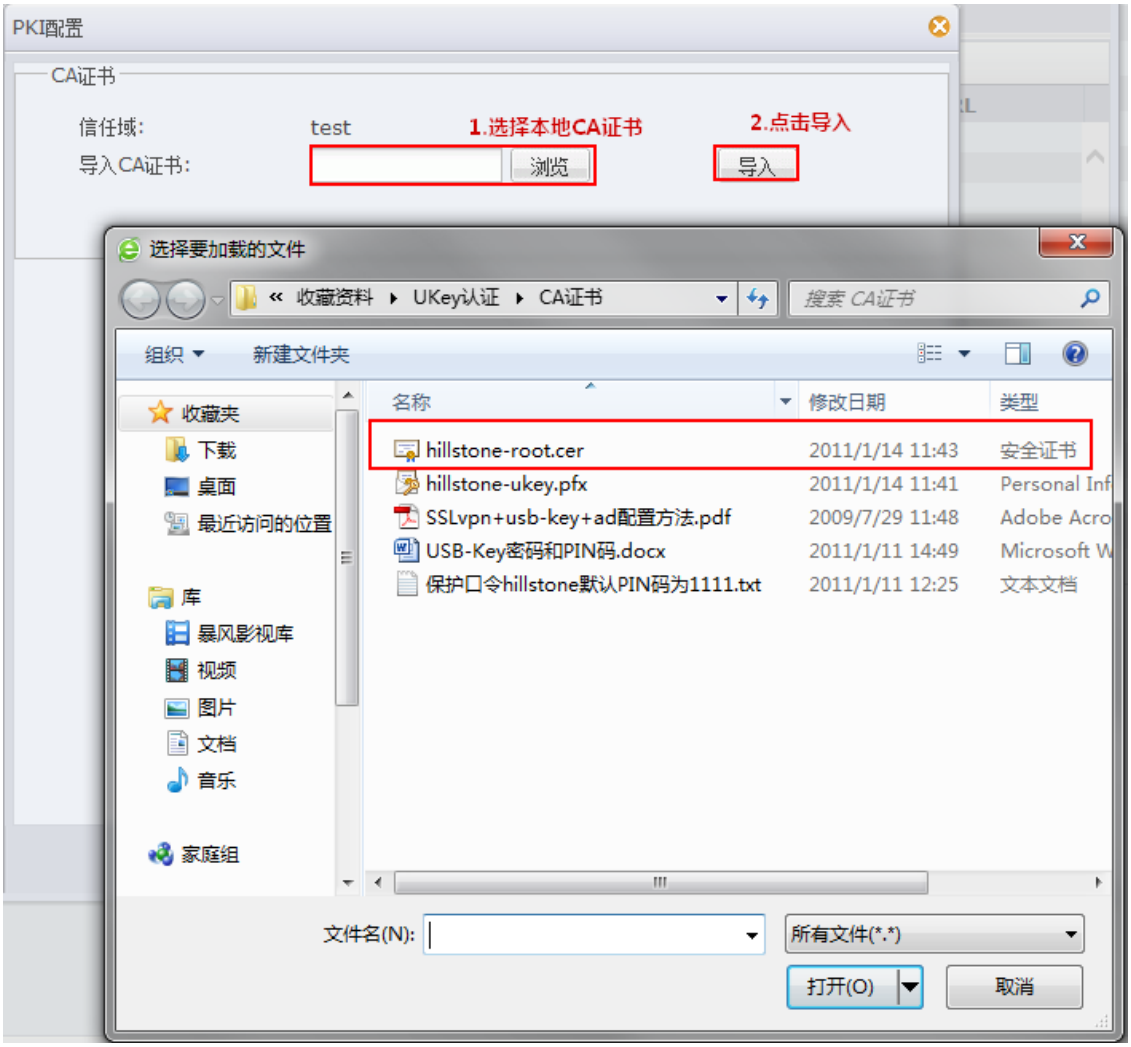
- 新建 PKI 信任域
- 配置 SCVPN
- 制作 USB Key
- 使用 USB Key 方式登录 SCVPN

新建 PKI 信任域

新建 PKI 信任域，请按照以下步骤进行配置：

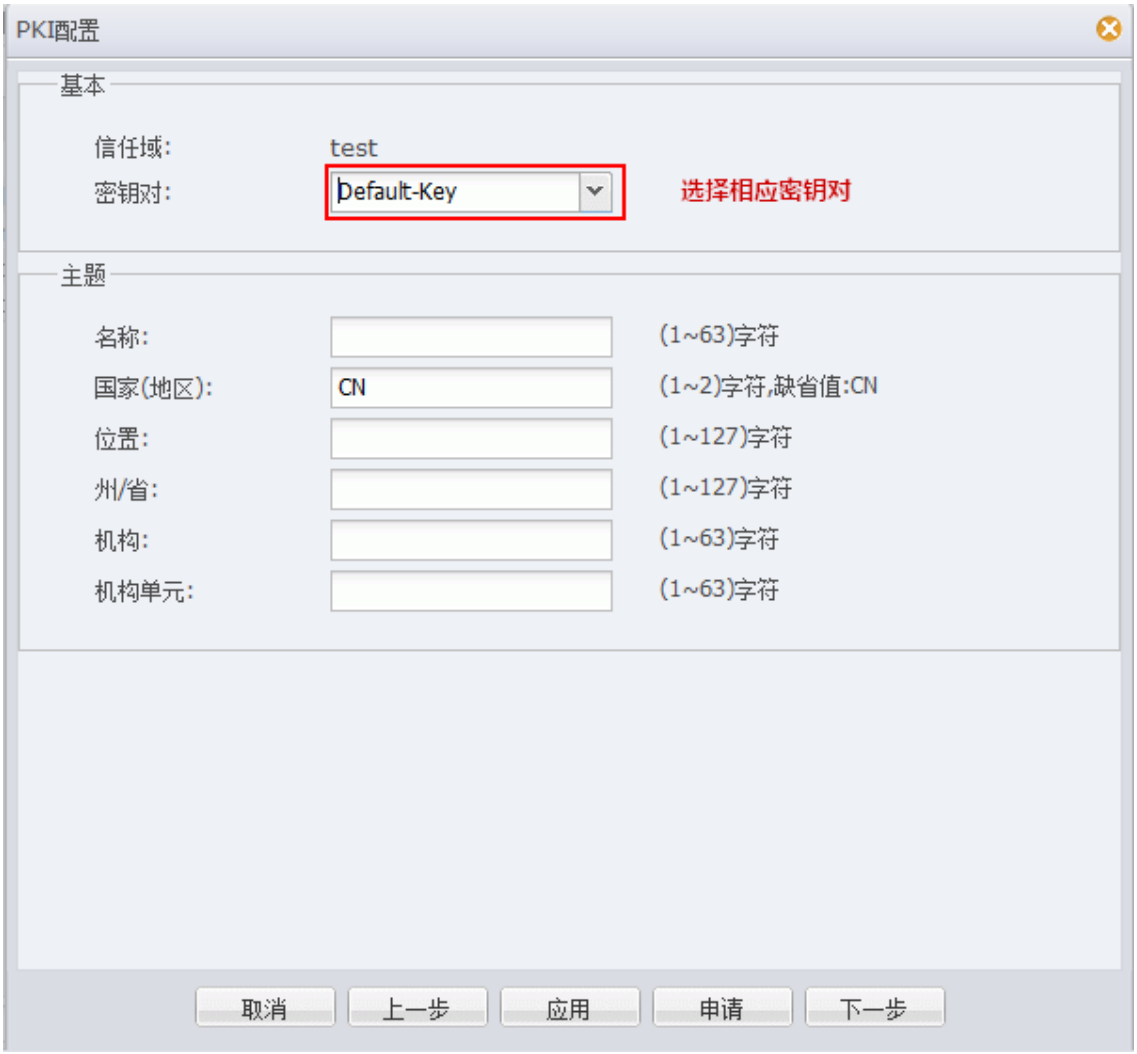
1. 从工具栏的<对象用户>下拉菜单选择『PKI』，弹出<PKI 管理>对话框。点击『信任域』标签，进入信任域标签页。
2. 点击信任域列表左上方的『新建』按钮，弹出<PKI 配置>对话框。
3. 在<信任域>文本框输入信任域的名称并选择证书获取方法，然后点击『下一步』按钮。选择<手动输入>方法获取证书，点击后进入<CA 证书>页面，在该页面导入 CA 证书（点击『浏览』按钮选择证书，然后点击『导入』按钮）。获取证书方法包括以下两种：
   - **手动输入**：使用终端（剪切和粘贴）的获得方法；
   - **自签名证书**：使用自签名的获得方法。

4. 导入需要使用的 CA 证书。

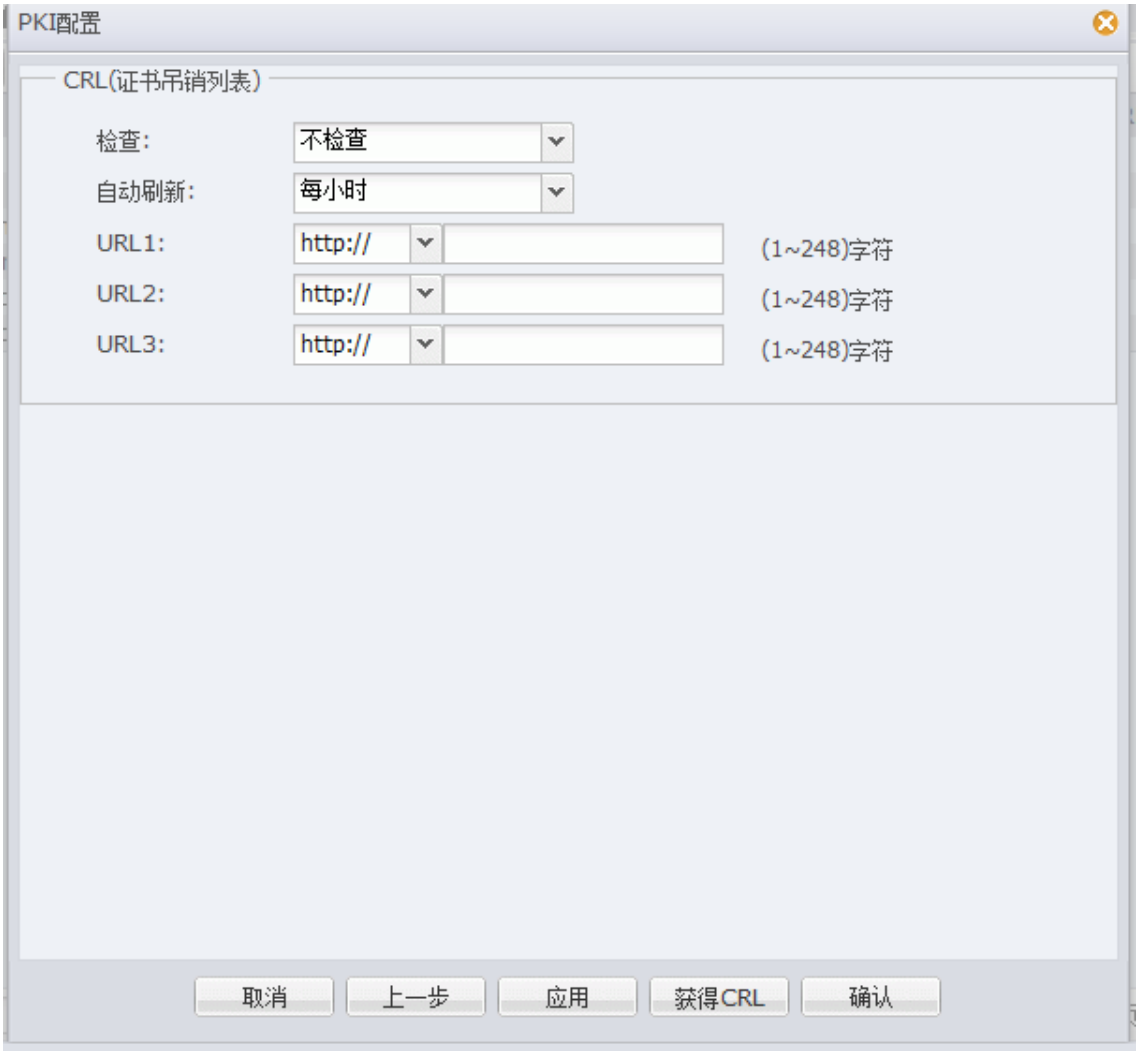


5. 导入成功后可看到 CA 证书相关信息。

6. 点击『下一步』按钮，从<密钥对>下拉菜单为信任域指定密钥对，其他信息可选填。



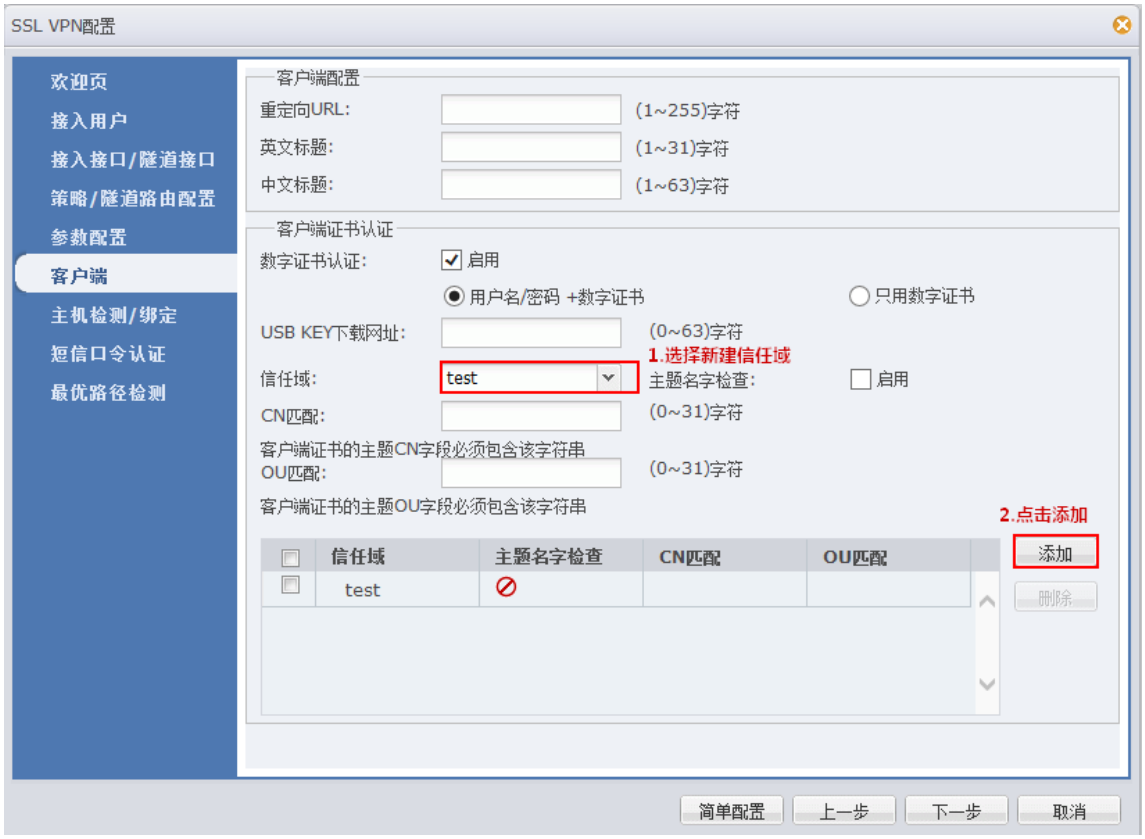
7. 点击『下一步』，在新页面配置 CRL 相关选项。



配置 SCVPN

请按照以下步骤进行操作：

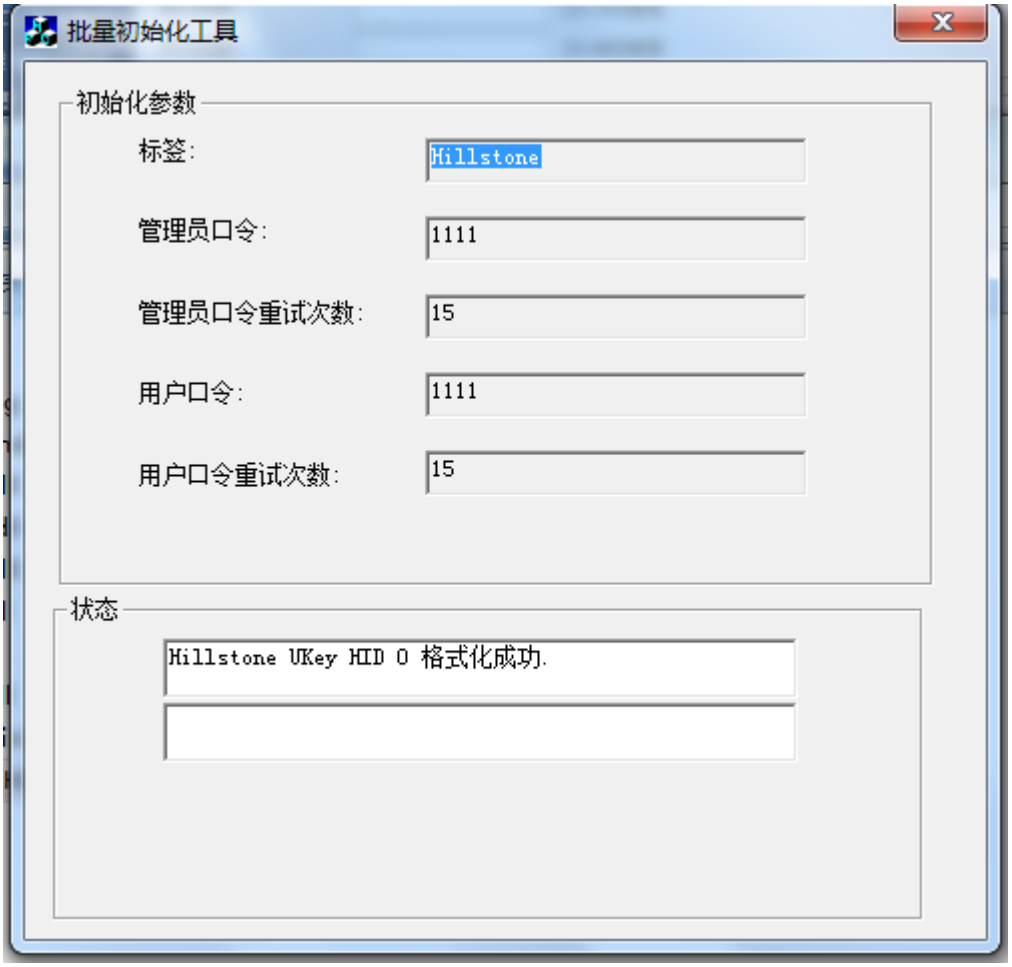
1. 配置 SCVPN 名称、用户身份认证的 AAA 服务器、设备端接口、隧道接口、地址池以及策略规则和隧道路由，请参阅 SCVPN 配置步骤 1-9。
2. 在<客户端>页面，进行客户端和客户端证书认证配置：
   - **USB Key 证书认证**：选中<启用>复选框开启客户端证书认证功能。该功能支持"用户名/密码 + USB Key"和"只用 USB Key"两种认证方式；
   - **信任域：**在<信任域>下拉菜单中选中之前创建的信任域。



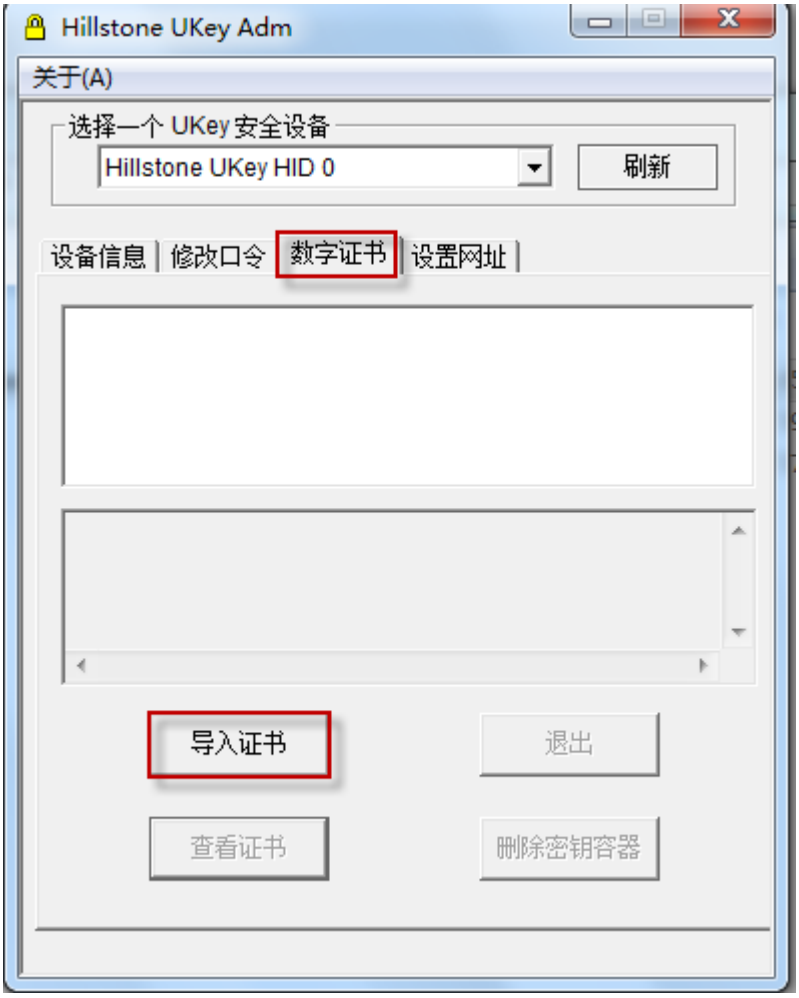
制作 USB Key

请按照以下步骤进行配置：

1. 格式化 USB Key，打开“Hillstone 初始化工具”，插入 USB Key，系统将进行自动格式化。



2. 导入认证证书，打开“Hillstone ukey admin 管理工具”，点击<数字证书>标签，然后点击<导入证书>按钮，输入保护口令（默认为 hillstone）。



使用 USB Key 方式登录 SCVPN

请按照以下步骤通过启动文件直接启动客户端，完成客户端与设备端的连接：

1. 将 USB Key 插入 PC 的 USB 接口。
2. 在 IE 浏览器的地址栏输入以下 URL 访问设备端：https://IP-Address:Port-Number。
3. 浏览器弹出<选择数字证书>对话框。选中需要的数字证书，点击『确定』按钮。在弹出的<请输入用户口令>对话框（如下图所示）中输入 UKey 的用户口令（默认为"1111"），并点击『确定』按钮。

4. 浏览器转到登录页面（如下图所示），输入用户名和密码，并点击『登录』按钮。此处的用户名和密码为安全网关中配置的用户及其相应的密码。

5. 成功登录后，如果使用 IE 浏览器，系统将自动完成下载任务，用户只需按照提示安装即可；如果使用 Firefox 等浏览器，请点击『下载』按钮下载客户端程序 scvpn.exe，下载完成，双击 scvpn.exe，按照安装向导提示进行安装。
6. 安装成功后，双击桌面的 Hillstone Secure Connect 快捷方式，或者点击"开始菜单"中的"所有程序 Hillstone Secure Connect Hillstone Secure Connect"，系统弹出登录对话框。
7. 点击对话框中的『模式』按钮，系统弹出<登录模式>对话框（如下图所示）。选中<用户名/密码>单选按钮，点击『确定』按钮。

8. 系统弹出"用户名/密码"登录模式客户端程序登录对话框（如下图所示）。依次填写登录对话框中的各项，然后点击『登录』按钮。

PnPVPN

IPSec VPN 配置复杂，维护成本高，对网管人员技术要求高，针对该问题，Hillstone 为企业用户提供了一种简单易用的 VPN 技术——PnPVPN，即即插即用 VPN。PnPVPN 由两部分组成，分别是 PnPVPN Server 和 PnPVPN Client，各自功能描述如下：

- PnPVPN Server：通常放置于企业总部，由总部 IT 工程师负责维护，客户端的大多数配置由服务器端下发。PnPVPN Server 通常由 Hillstone 设备充当，一台 Hillstone 设备可充当多个 PnPVPN Server。
- PnPVPN Client：通常放置于企业分支机构（如办事处），可由总部工程师远程维护，只需要做简单配置（如客户端 ID、密码和服务器端 IP 地址），和 Server 端协商成功后即可从 Server 端获取配置信息（如 DNS、WINS、DHCP 地址池等）。

用户需要在以下模块进行配置：

- 用户配置
- IKE VPN 配置
- 隧道接口配置
- 策略配置
- PnPVPN 客户端配置

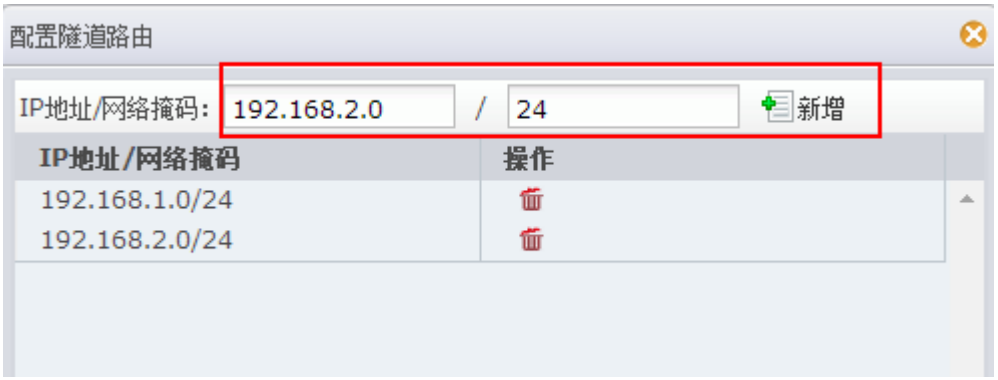
用户配置

请按照以下步骤进行用户配置：

1. 从工具栏的<对象用户>下拉菜单选择『本地用户』，弹出<本地用户>对话框。
2. 在<本地服务器>下拉菜单中选择需要的本地服务器名称，然后点击对话框左上角的『新建』下拉菜单，选择<用户>，弹出<用户配置>对话框。

3. 按照上图完成配置后，点击<PnPVPN 配置>，展开具体配置选项，包括 DHCP 相关选项、DNS、WINS 以及隧道路由。当该用户不使用隧道下已经配置的 DNS、WINS 和隧道路由选项或者新建隧道页面未配置这些选项时，这些选项必须在本页面完成配置。

4. 根据需要对该页面的其它选项进行配置。
5. 配置完成，点击『确定』按钮保存所做配置。然后需要重新编辑该用户，进入<PnPVPN配置>，用于指定客户端的 VPN 路由。如果有多个分支客户端可重复上述步骤。



IKE VPN 配置

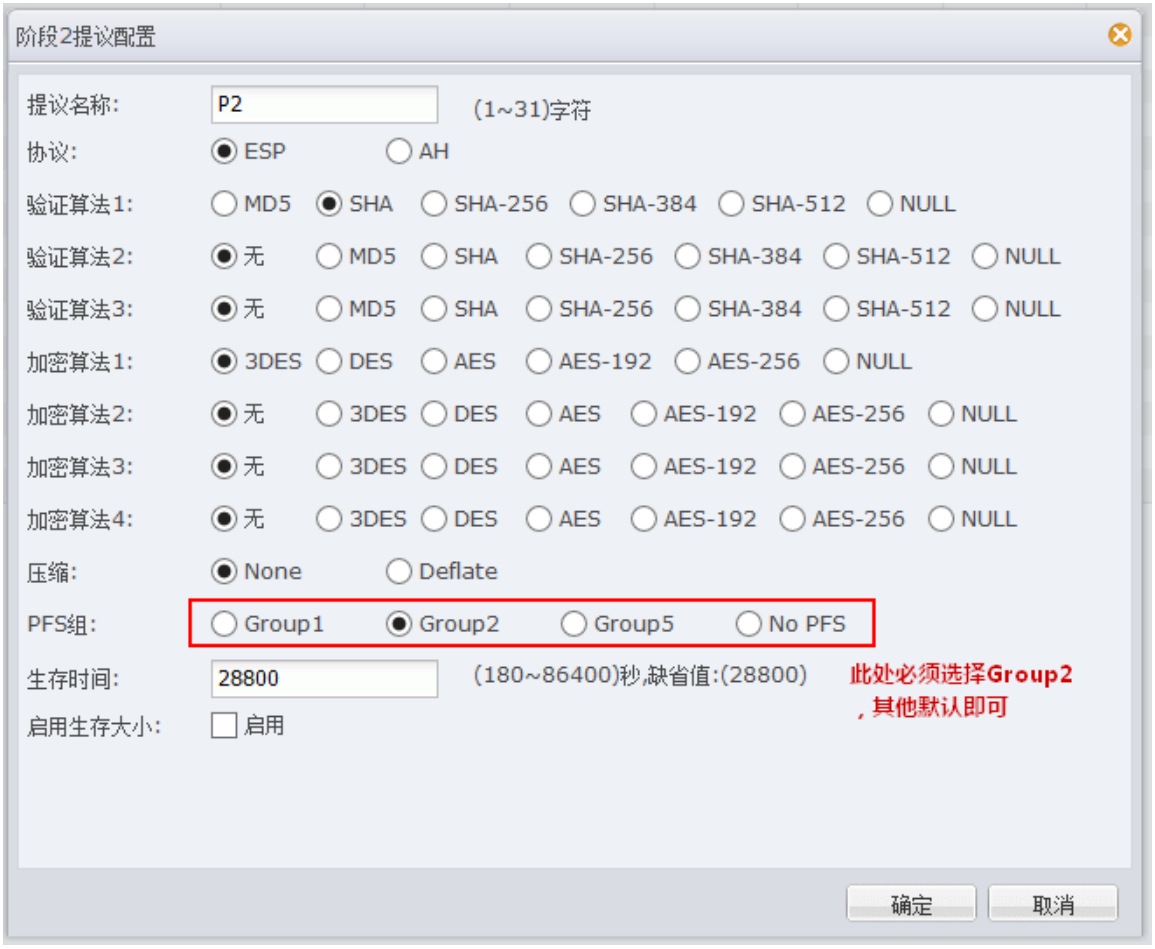
IKE VPN 配置包括 P1 提议配置、P2 提议配置、对端配置以及隧道配置。

按照以下步骤配置：

1. **配置 P1 提议。**从页面左侧导航树选择并点击“配置->网络->IPSec VPN”，进入 IPSec VPN 页面。点击『P1 提议』标签，进入 P1 提议标签页。
2. 点击 P1 提议列表左上方的『新建』按钮，弹出<阶段 1 提议配置>对话框。

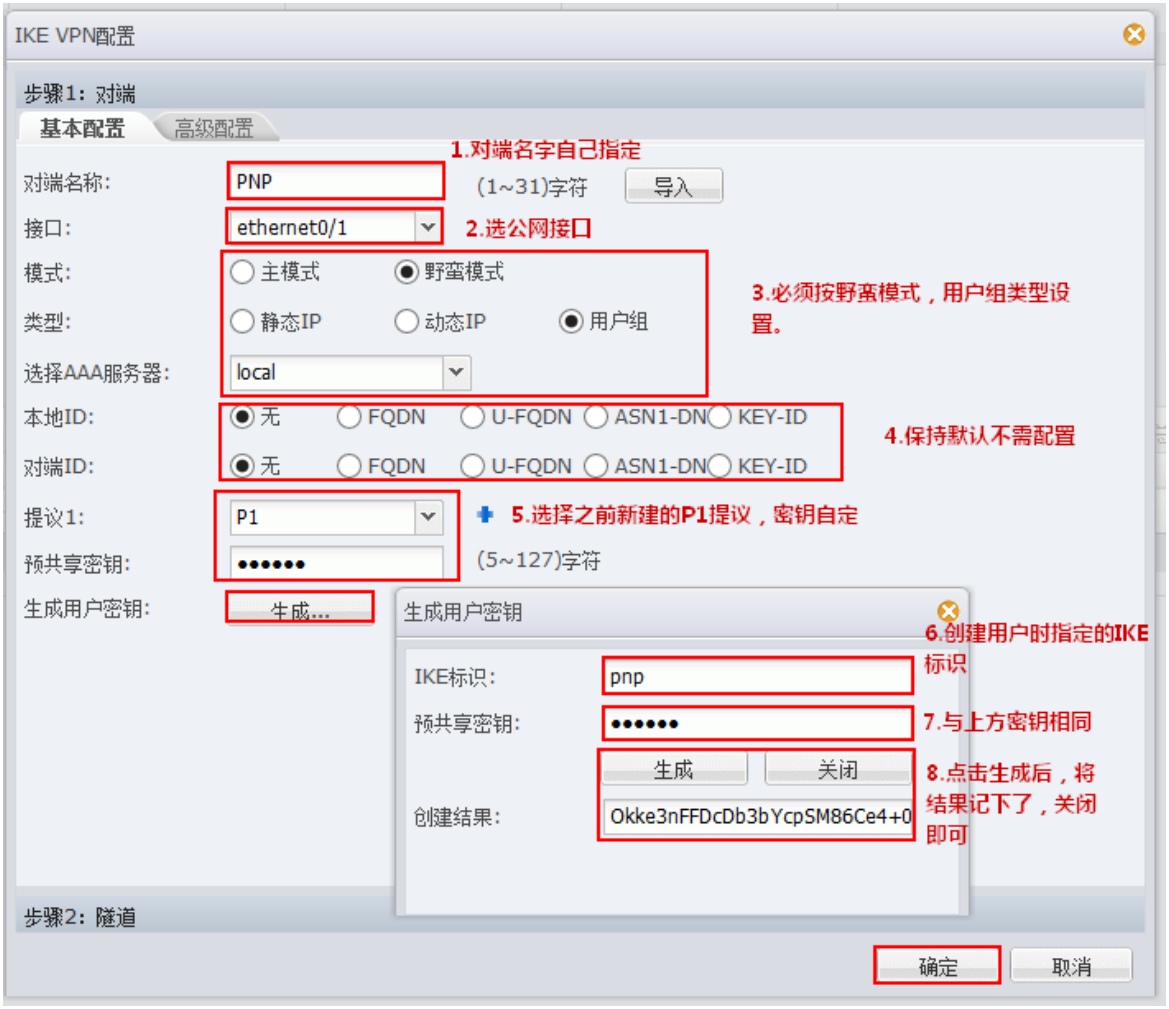
3. **配置 P2 提议。**从页面左侧导航树选择并点击“配置➤网络➤IPSec VPN”,进入 IPSec VPN 页面。点击『P2 提议』标签，进入 P2 提议标签页。

4. 点击 P2 提议列表左上方的『新建』按钮，弹出<阶段 2 提议配置>对话框。



5. **配置 VPN 对端。**从页面左侧导航树选择并点击“配置➤网络➤IPSec VPN”，进入 IPSec VPN 页面。点击『VPN 对端列表』标签，进入 VPN 对端列表标签页。

6. 点击列表左上方的『新建』按钮，弹出<VPN 对端配置>对话框。

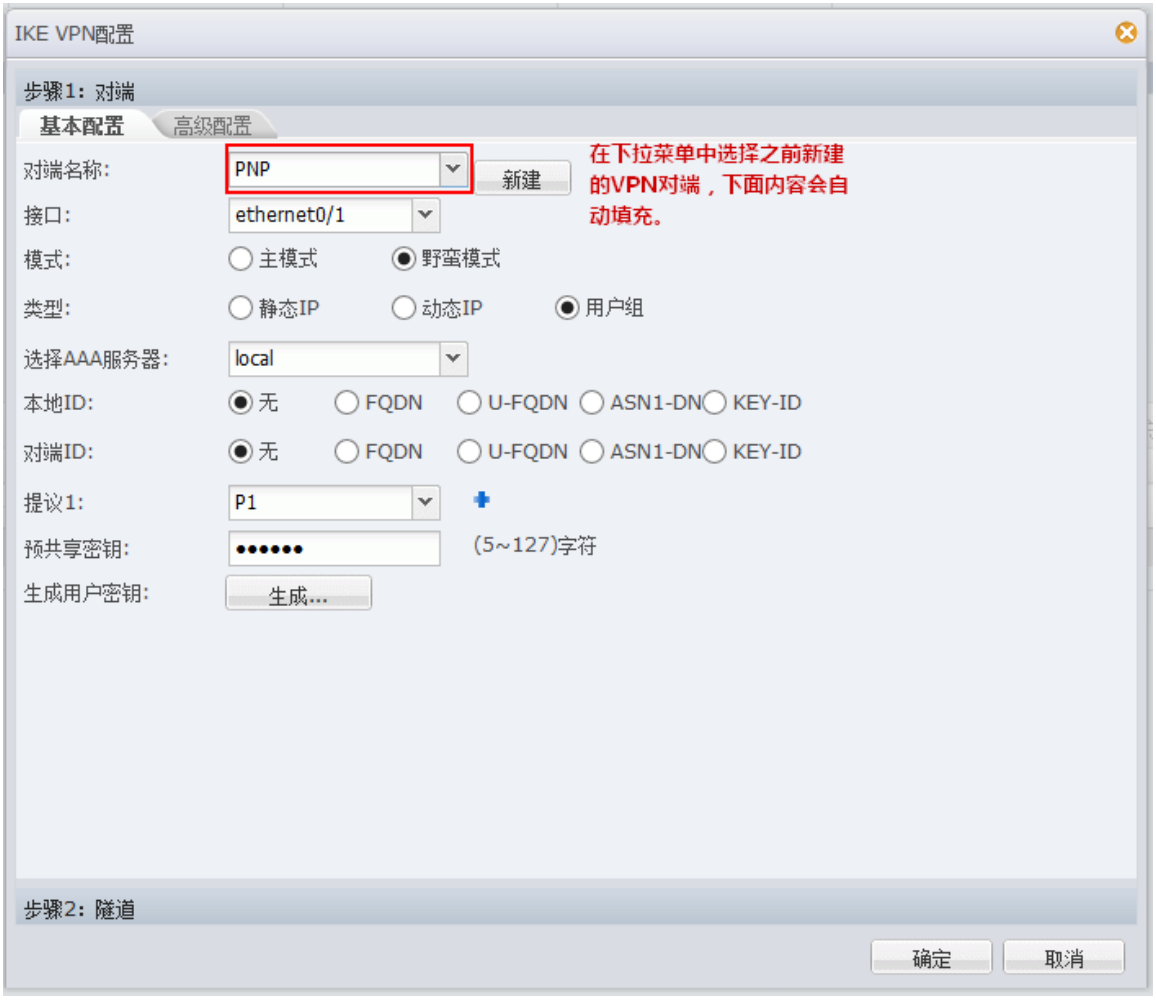


7. **配置隧道**。从页面左侧导航树选择并点击“配置➤网络➤IPSec VPN”，进入 IPSec VPN 页面。点击『IPSec VPN』标签，进入 IPSec VPN 标签页。

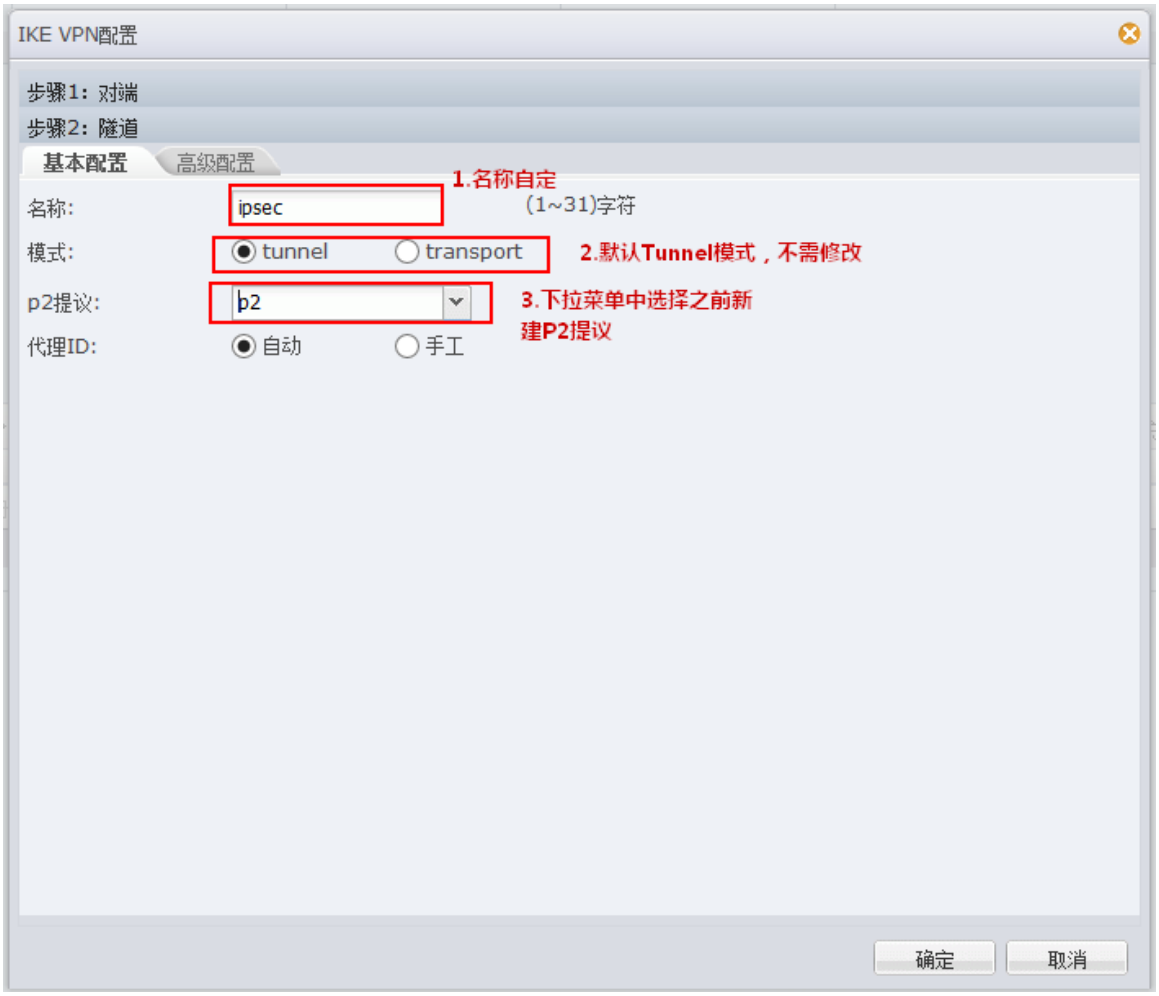
8. 点击 IKE VPN 列表左上方的『新建』按钮，弹出<IKE VPN 配置>对话框。

9. 在<步骤 1：对端>部分，点击<对端名称>的『导入』按钮，然后从下拉菜单中选择需要

的对端。用户也可以直接在该页面新建对端（ISAKMP 网关）。



10. 点击<步骤 2：隧道>，展开隧道具体配置选项。



隧道接口配置

请按照以下步骤进行隧道接口配置：

1. 点击“配置->网络->网络连接”，进入网络连接页面。点击接口列表左上方的『新建』下拉菜单，选择并点击<隧道接口>，弹出<接口配置>对话框。
2. 接口创建完成之后，进入该隧道接口，配置隧道绑定。

策略配置

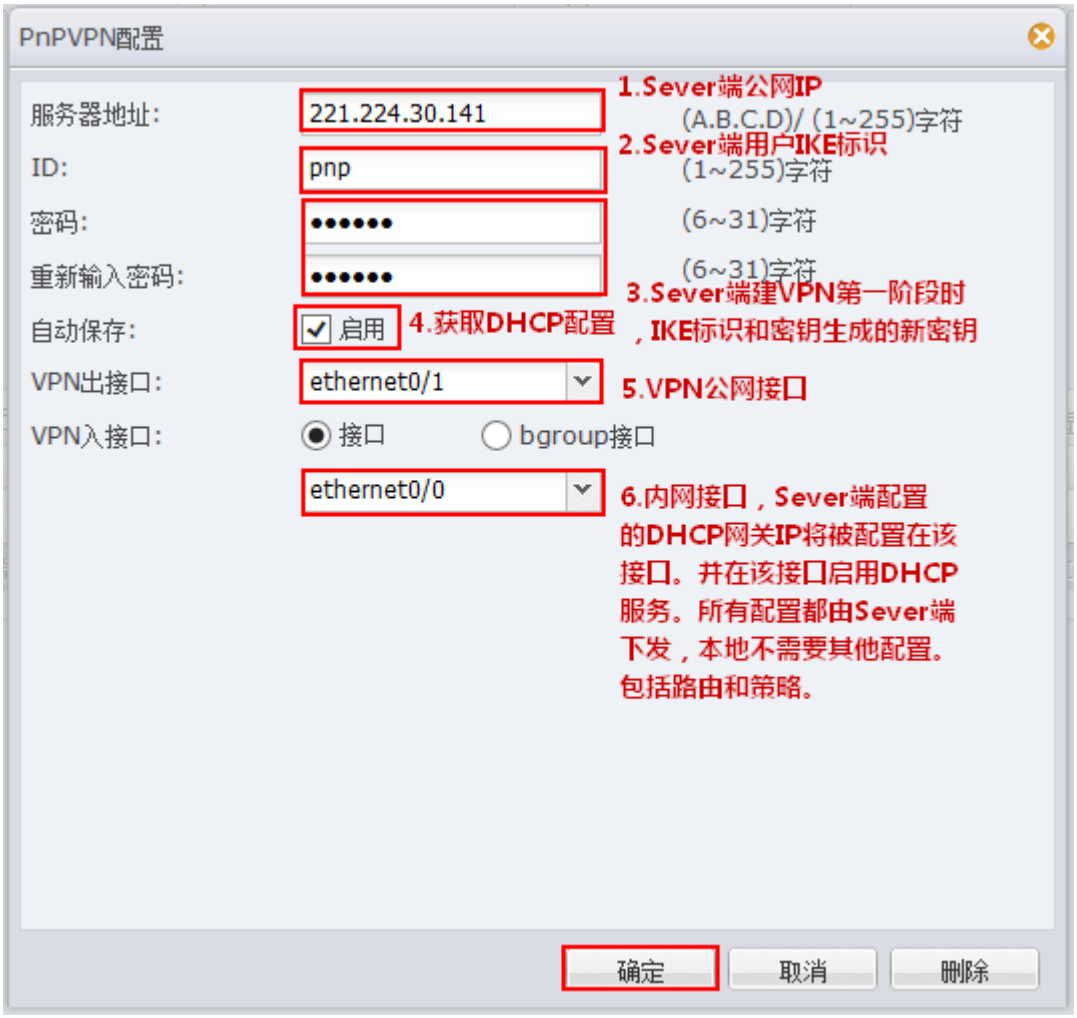
根据网络拓扑情况，配置相应的访问策略。

1. 从页面左侧导航树选择并点击"配置->安全->策略"，进入策略页面。
2. 点击列表左上角的『新建』按钮，弹出<策略配置>对话框，在该对话框对策略规则进行编辑。

PnPVPN 客户端配置

请按照以下步骤进行配置：

1. 将设备接入互联网，配置外网 IP 以及默认路由。
2. 从页面左侧导航树选择并点击“配置->网络->IPSec VPN”，进入 IPSec VPN 页面。
3. 从页面右侧辅助栏的<任务>区选择『PnPVPN 客户端』链接，弹出<PnPVPN 配置>对话框。依次填写或者选择各项。



4. 配置完成，点击『确定』按钮保存所做配置并返回 IPSec VPN 页面。

5. 大概需要 1 分钟协商，之后接入端 VPN 配置以及内网 IP 配置均自动完成。

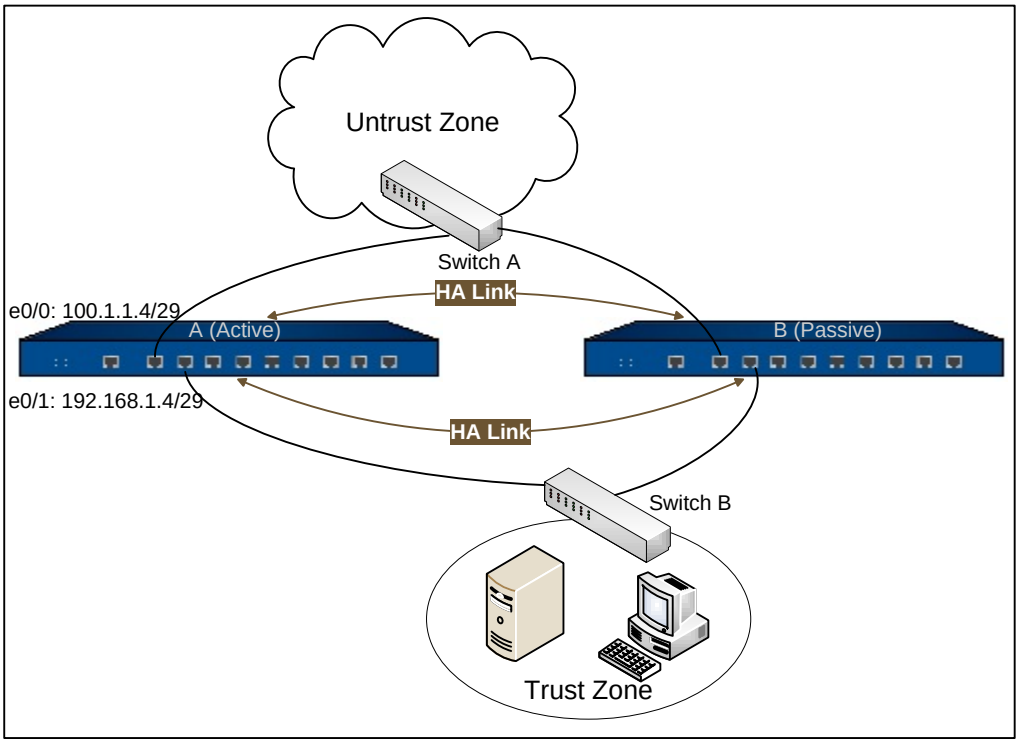
第 8 章 高可靠性

高可靠性介绍

高可靠性(High Availability),简称为 HA ,能够在通信线路或设备产生故障时提供备用方案，从而保证数据通信的畅通，有效增强网络的可靠性。实现 HA 功能，用户需要配置两台采用完全相同的硬件平台、固件版本，均安装相同的许可证、且所有接口对应关系一致的 Hillstone 设备组成 HA 簇。当一台设备不可用或者不能处理来自客户端的请求时，该请求会及时转到另外的可用设备来处理，这样就保证了网络通信的不间断进行，极大地提高了通信的可靠性。

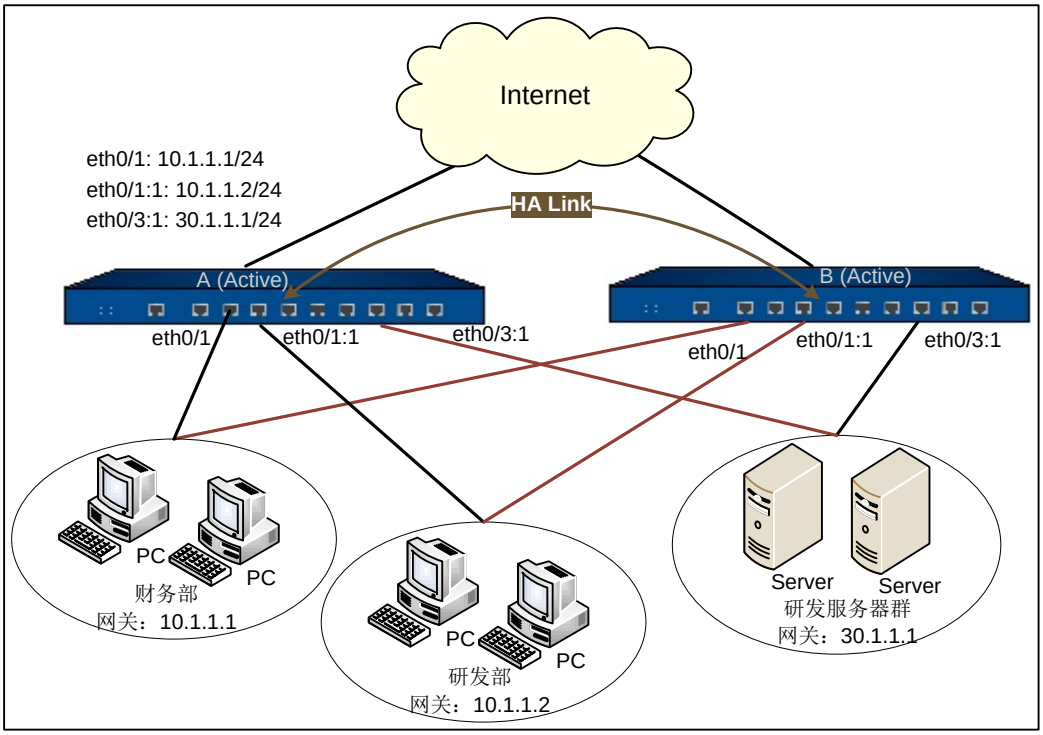
Hillstone 设备支持 HA 的 2 种工作模式 :Active-Passive(A/P)模式和 Active-Active(A/A) 模式：

- Active-Passive（A/P）模式：系统会将安全网关 A 选举为主设备，进行流量转发。安全网关 B 为备份设备，安全网关 A 会将其配置信息以及状态数据同步到安全网关 B。当安全网关 A 出现故障不能正常转发流量或安全网关 A 的 TRACK 生效时，安全网关 B 会在不影响用户通信的状态下切换为主设备，继续转发流量，拓扑如下：



- Active-Active（A/A）模式：两台设备均会开启 HA 功能。系统将安全网关 A 选举为 group0 的主设备。安全网关 A 向安全网关 B 进行同步配置。同步配置完成后，安全网关 B 抢占为 group1 的主设备。在正常情况下，两台设备独立运行各自的工作：安全网关 A 对财务部和研发部访问网络的流量进行转发；安全网关 B 对研发服务器群访问网络的流

量进行转发。如果其中一台设备发生故障或者 TRACK 生效时，另外一台设备可运行自身工作的同时接管故障设备的工作，保证工作不间断。例如：安全网关 B 故障无法工作，安全网关 A 在转发财务部和研发部访问网络流量的同时 将转发研发服务器群访问网络的流量，拓扑如下：



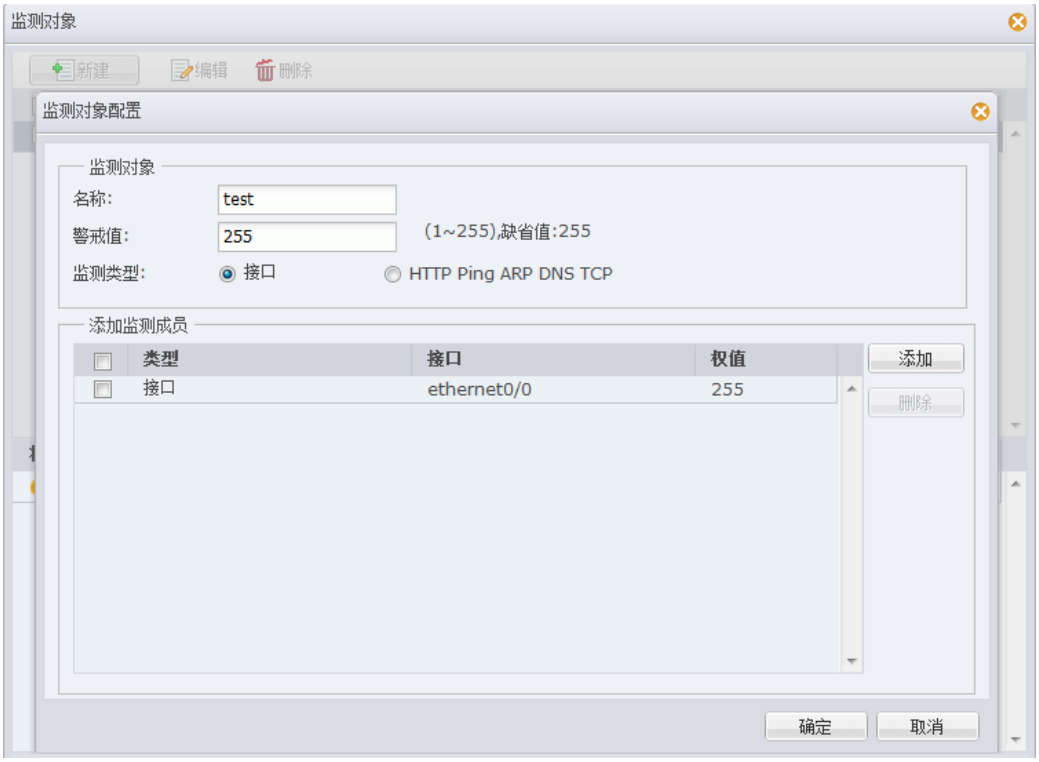
高可靠性配置

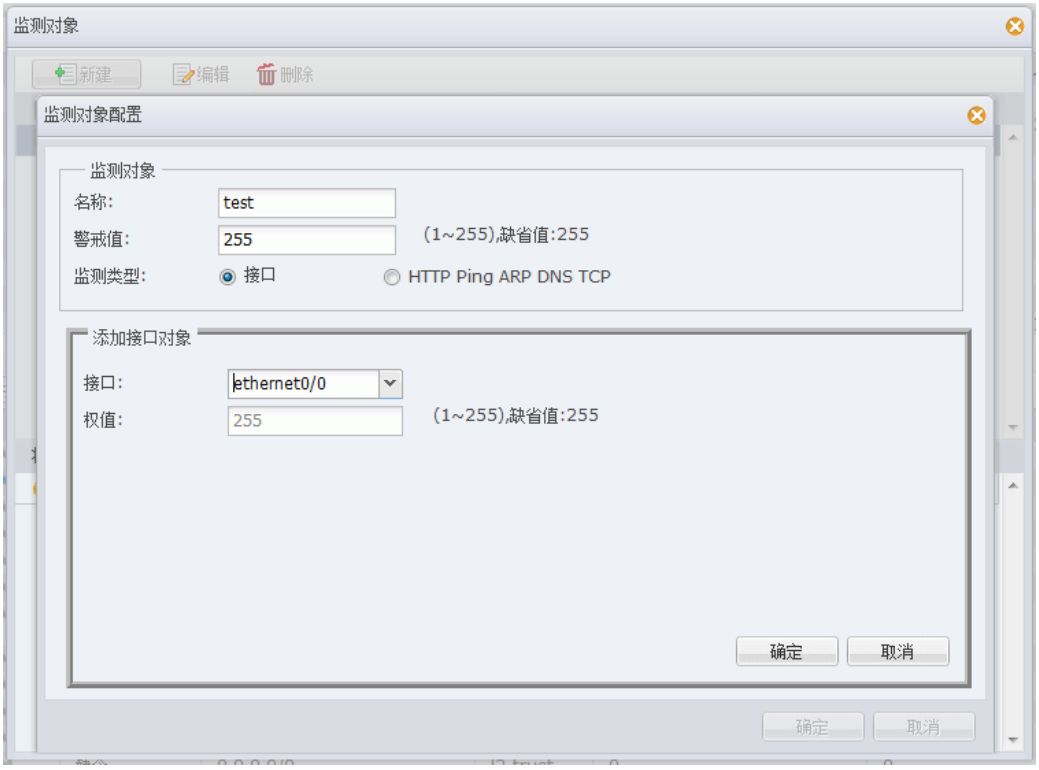
请按照以下步骤进行配置：

1. 从工具栏的<系统管理>下拉菜单选择『HA』，弹出<HA>对话框。按照下图配置：

2. **配置监测对象**。从工具栏的<对象用户>下拉菜单选择『监测对象』，弹出<监测对象>对话框。点击监测对象列表左上方的，弹出<监测对象配置>对话框。

3. 如果选择"接口"监测类型，点击『添加』按钮，然后在<添加接口对象>部分添加监测条目，用来监测接口的物理状态，可以添加多个接口，每个接口有一个权值，该数值表示该接口 DOWN 后将释放的数值，当所有释放的权值累计数值大于等于警戒值的时候，该检测对象就生效，权值和警戒值都可以自行调整。

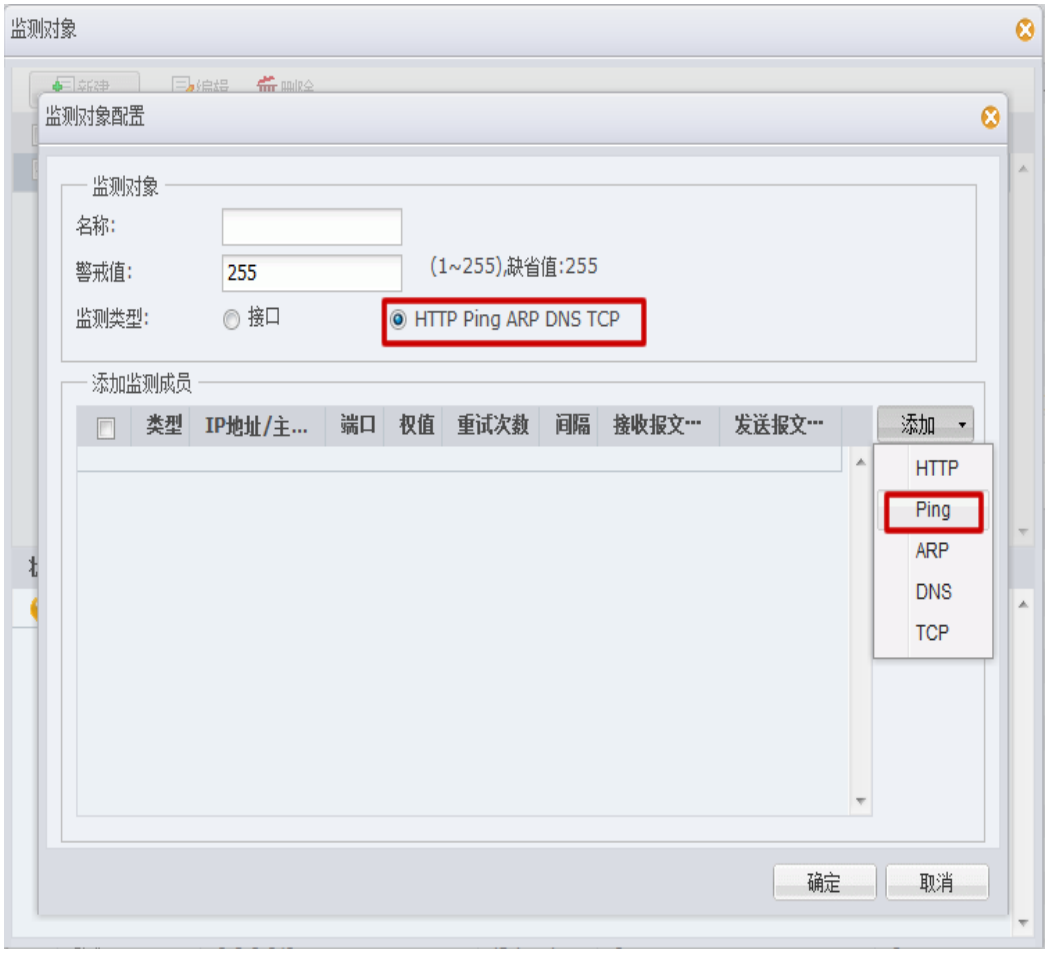


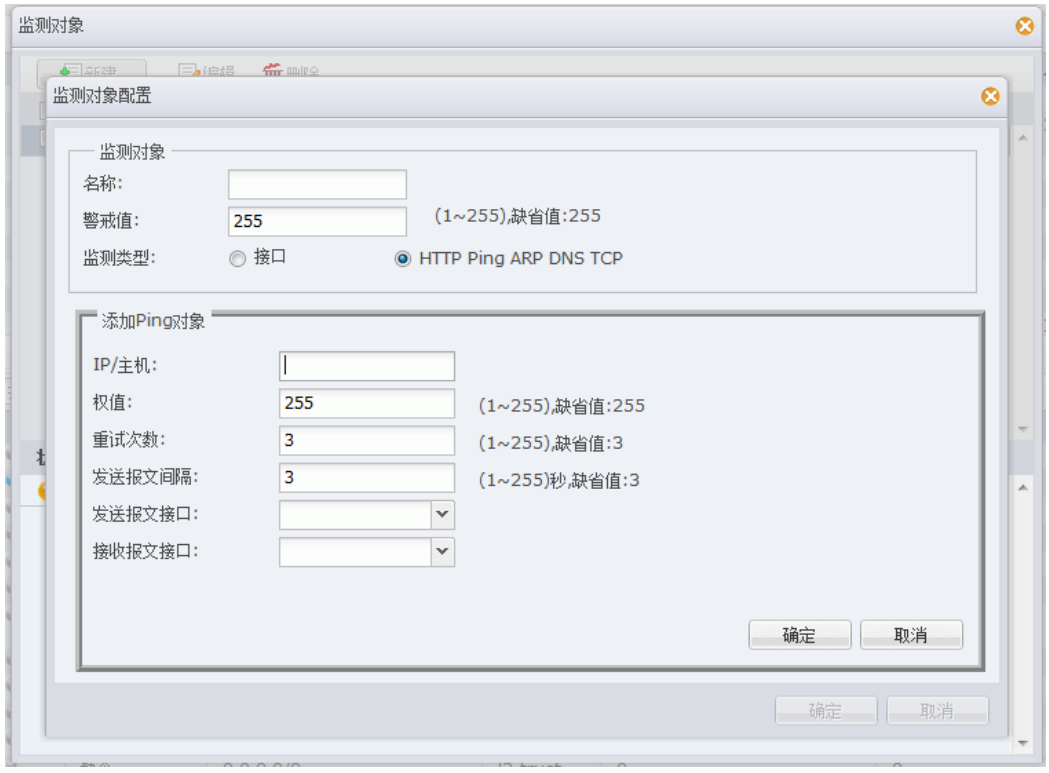


4. 如果选择"HTTP Ping ARP DNS TCP"监测类型，点击『添加』，从下拉菜单中选择需要的报文类型，然后在<添加/HTTP/Ping/ARP/DNS/TCP>部分添加监测条目。用来监测链路逻辑状态，可以配置多种形式的探测。

以 PING 为例，如下图配置中，设备没 3 秒发一个 PING 包，连续 3 个包不通，该条目即生效，设备会优先使用配置的收包接口的管理 IP 为源地址(如没有管理 IP 就用接口的 IP 为源地址)

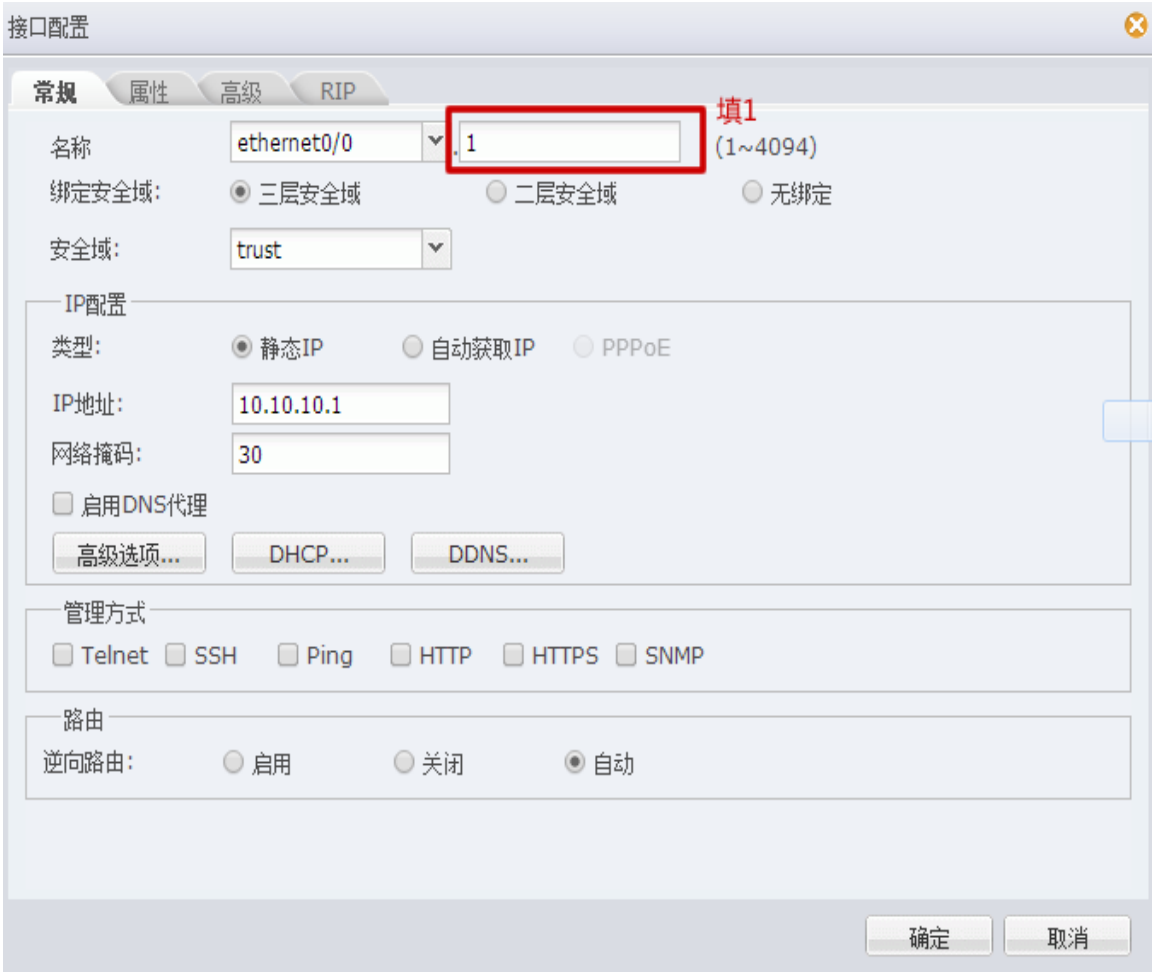
通过配置的发包接口把 PING 包发出。



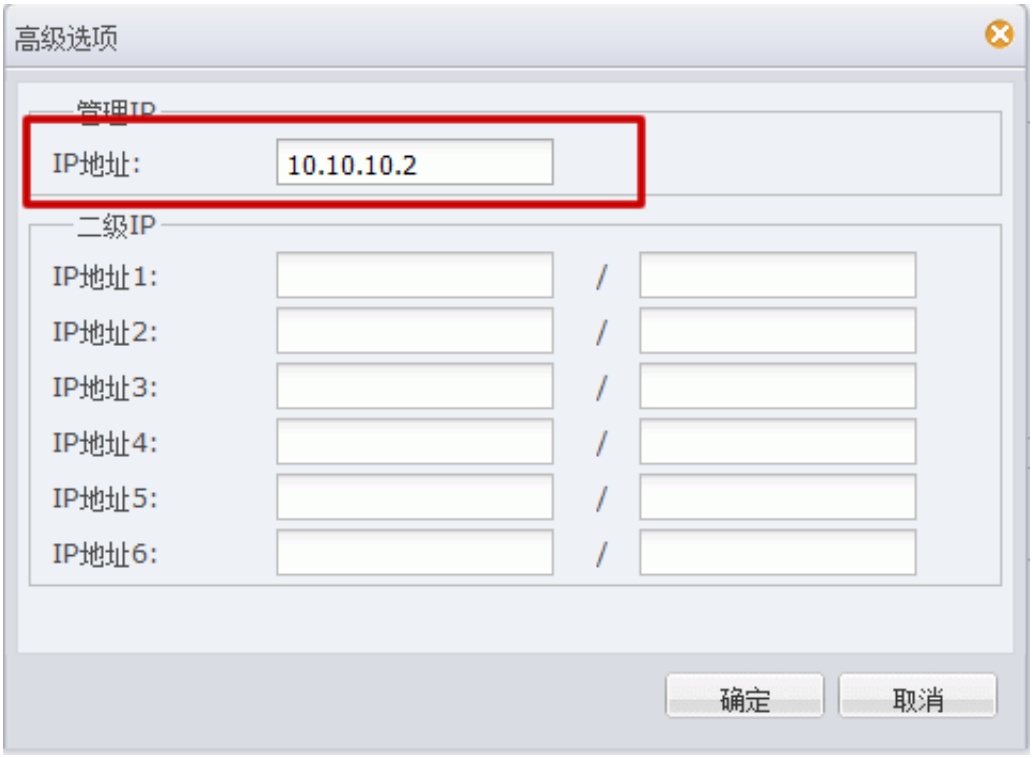


5. **配置接口**。在 AP 模式下,配置方式和普通配置一致,直接在接口上进行配置即可，请参阅接

口配置。在 AA 模式下,组 0 和普通配置一致,组 1 需要配置 Virtual Forward 接口。点击接口列表左上角的『新建』按钮 ,弹出接口类型下拉菜单。从下拉菜单中选择并点击<Virtual Forward 接口>，系统弹出<接口配置>对话框。如下图：

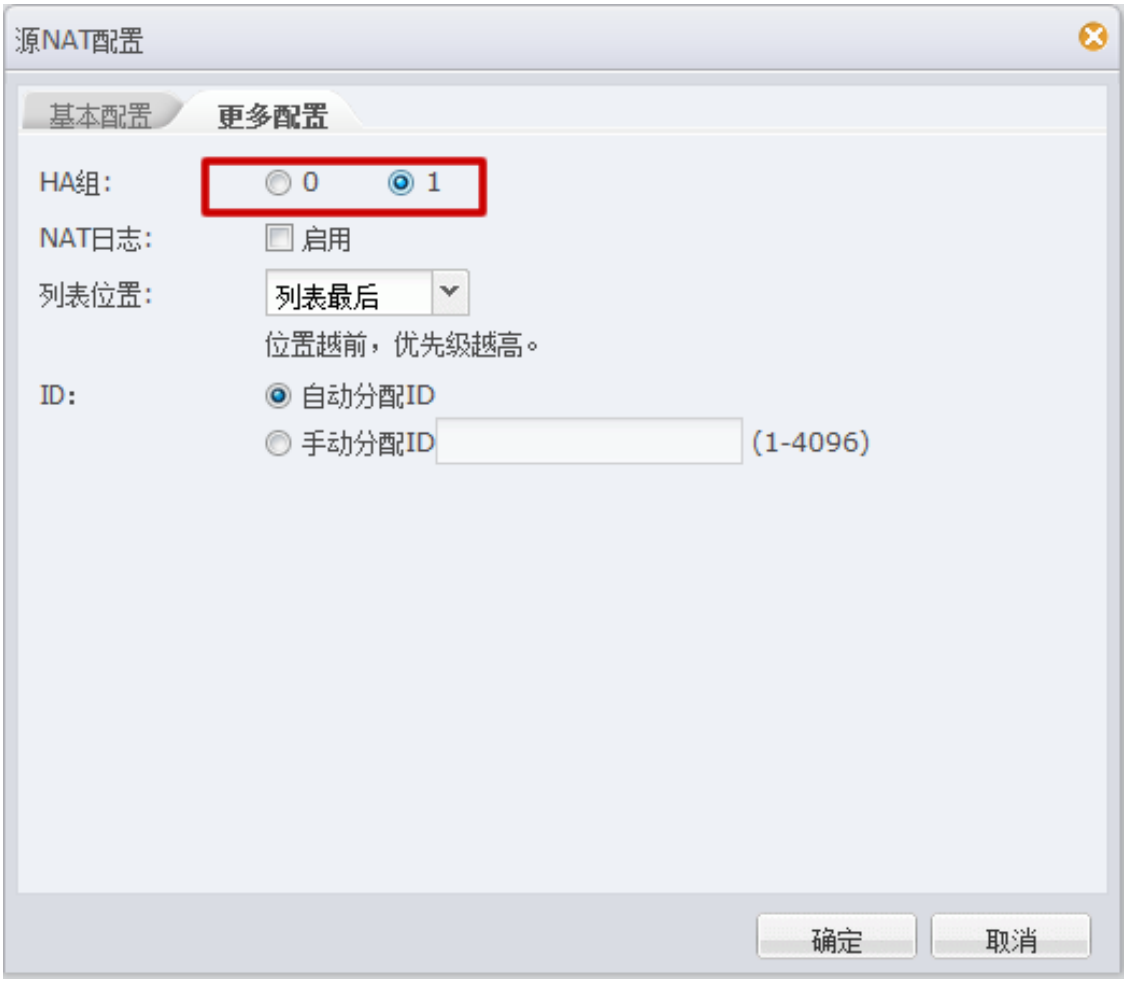


6. **配置管理 IP**。由于备机是不转发流量的,所以需要在组 0 的接口上配置管理 IP,用于设备的管理和进行 TRACK 监测。在<接口配置>对话框，点击『高级选项』按钮，在<管理 IP>文本框中输入 IP 地址，为接口指定管理 IP。

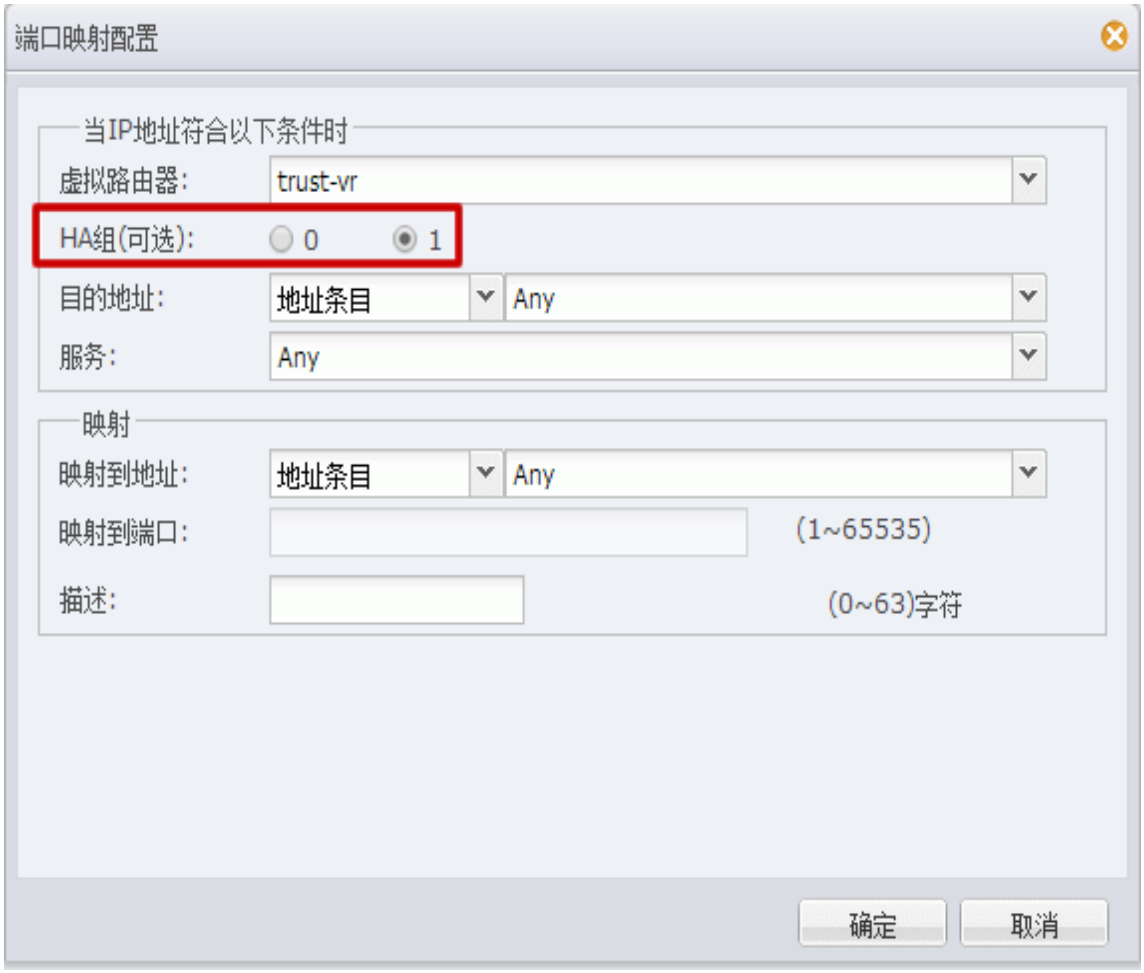


提示：管理 IP 可以和接口 IP 在同一网段,也可以是单独的 IP,只需路由可达即可。

7. **配置 NAT 规则。**在 AP 模式下,配置 NAT 规则的方法和普通配置一致,直接配置即可，请参阅源 NAT 配置。在 AA 模式下,组 0 配置 NAT 和普通配置一致,组 1 配置 NAT 需要选择组 1。
8. **源 NAT。**点击源 NAT 列表中的『新建』按钮，弹出<新建源 NAT>对话框。在『更多配置』标签页中，选择<HA 组>单选按钮，指定源 NAT 规则所属的 HA 组。



9. **目的 NAT**。从页面左侧导航树选择并点击“配置->网络->NAT”，进入源 NAT 页面。点击『目的 NAT』标签，进入目的 NAT 页面。选择<HA 组>单选按钮，指定目的 NAT 规则所属的 HA 组。



10. **配置路由以及策略**，确保网络的畅通。配置方法请参阅路由配置和策略配置。


HA
HA控制连接接口1:
ethernet0/5
接口2:
无
HA数据连接接口:
无
IP地址:
1.1.1.1
/
30
HA簇ID:
1
节点ID:
0
Peer-mode:
启用
组0
优先级:
50
(1-254)
抢占时间:
0
(0-600秒)
Hello报文间隔:
1000
(50-10000毫秒)
Hello报文警戒值:
3
(3-255)
免费ARP包个数:
15
(10-20)
监测对象:
无
描述:
(1-31字符)
确定
取消


HA
HA控制连接接口1:
ethernet0/5
接口2:
无
HA数据连接接口:
无
IP地址:
1.1.1.2
/
30
HA簇ID:
1
节点ID:
0
Peer-mode:
启用
组0
优先级:
50
(1-254)
抢占时间:
0
(0-600秒)
Hello报文间隔:
1000
(50-10000毫秒)
Hello报文警戒值:
3
(3-255)
免费ARP包个数:
15
(10-20)
监测对象:
无
描述:
(1-31字符)
确定
取消


监测对象配置
监测对象
名称:
HA-Track
(1~31)字符
警戒值:
255
(1~255),缺省值:255
监测类型:
接口
HTTP Ping ARP DNS TCP
添加监测成员
类型
接口
权值
添加
接口
ethernet0/0
255
接口
ethernet0/2
255
删除
确定
取消


HA
HA控制连接接口1:
ethernet0/5
接口2:
无
HA数据连接接口:
无
IP地址:
1.1.1.1
/
30
HA簇ID:
1
节点ID:
0
Peer-mode:
启用
组0
优先级:
50
(1-254)
抢占时间:
0
(0-600秒)
Hello报文间隔:
1000
(50-10000毫秒)
Hello报文警戒值:
3
(3-255)
免费ARP包个数:
15
(10-20)
监测对象:
HA-Track
描述:
(1-31字符)
确定
取消