服务热线：400 828 6655

Hillstone 山石网科
多核安全网关
高级功能配置手册

V 5.0 版本

一．链路负载均衡

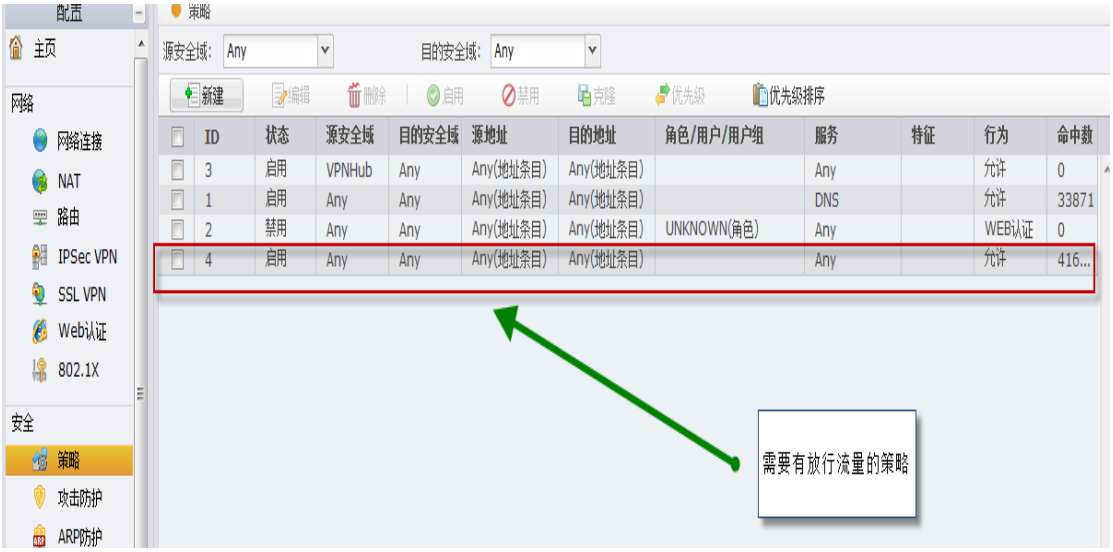
当防火墙有多条链路接入，同时需要对内网的流量根据源地址，目的地址或者服务进行流量的负载分摊时，需要进行负载均衡的配置，以便保证流量的负载分担；在配置源地址，目的地址的负载均衡时，可以实现冗余，当某一条路由失效时，可以保证正常的流量转发。

配置多链路负载均衡前，先保证接口，snat 和策略都配置正确。

1. 确认接口的地址和掩码都配置正确，其中**掩码的位数**一定和运行商确认：

2. 两条源地址转换，使内网的流量可以分别 nat 成对应公网出口地址池的地址，去访问互联网：

3. 确认流量穿越防火墙时，防火墙**策略允许**（源和目的地址以及服务可以根据具体情况作相应修改）：

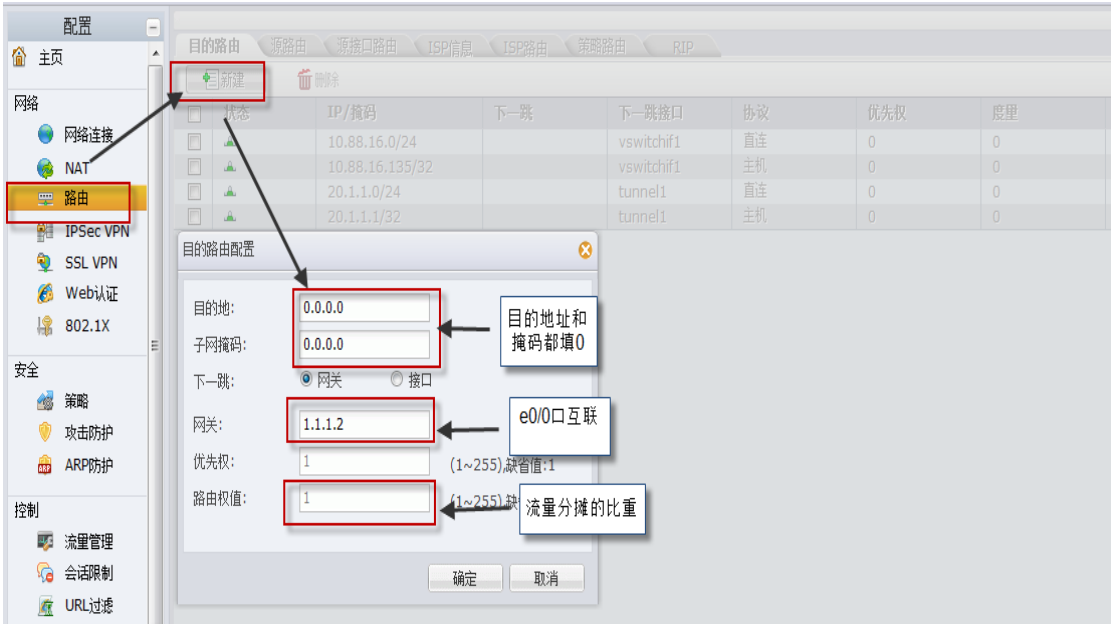


1.1 基于目的路由的流量负载

例：e0/1 口接入 10M 电信，e0/2 接入 20M 网通；实现所有访问公网的流量按 1：2 的比例分别从 e0/1 口和 e0/2 口转发出去。即当设备总共转发 3 数值的流量时，e0/1 转发 1 数值；e0/2 口转发 2 数值。

Web 页面配置如下：

1．网络-〉路由-〉新建 ：



2．创建一条默认路由权值为 2，即可得到配置如下：

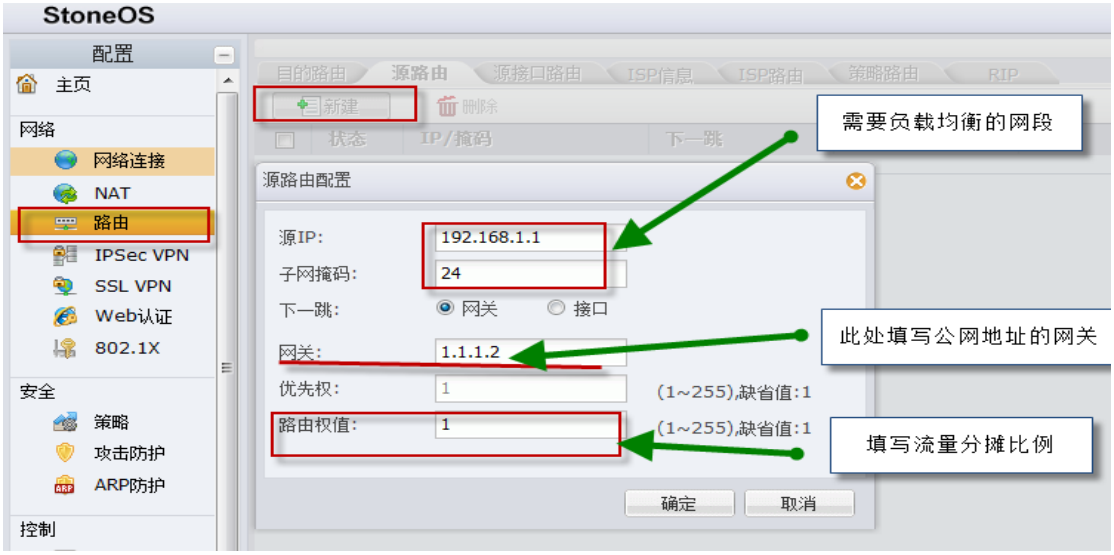
如此即可实现流量从 e0/1 转发和从 e0/2 转发的比是 10：20 即流量的 1：2 负载。具体比例可根据出口带宽的大小以及实际使用率确定。

1.2 基于源路由的流量负载

首先要确认流量需要负载的网段比如：192.168.1.1/24，

Web 页面新建源路由如下

1．网络->路由->源路由->新建：



2．重复上述操作并将网关改为 3.3.3.1；路由权值改为 2（根据需求）：

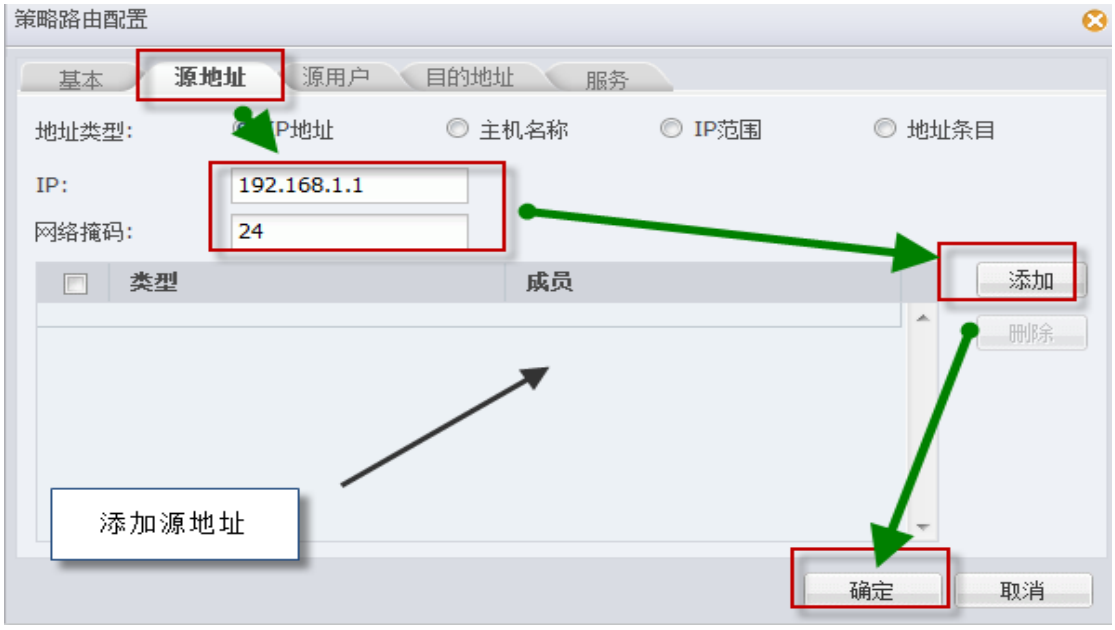
如此即可实现来自 192.168.1.1/24 网段的流量从 e0/1 转发和从 e0/2 转发的比是 1：2，具体比例可根据出口带宽的大小以及实际使用率确定。

1.3 基于策略路由的流量负载

例子：需要负载的网段是 192.168.1.1/24，此网段去往 8.8.8.8 的 HTTP 流量从 e0/1 口转发；去往 8.8.8.8 的 ICMP 流量从 e0/2 口转发。

Web 页面配置如下：

1．网络->路由->策略路由->新建：先配置源地址：



2．配置目的地址和服务：

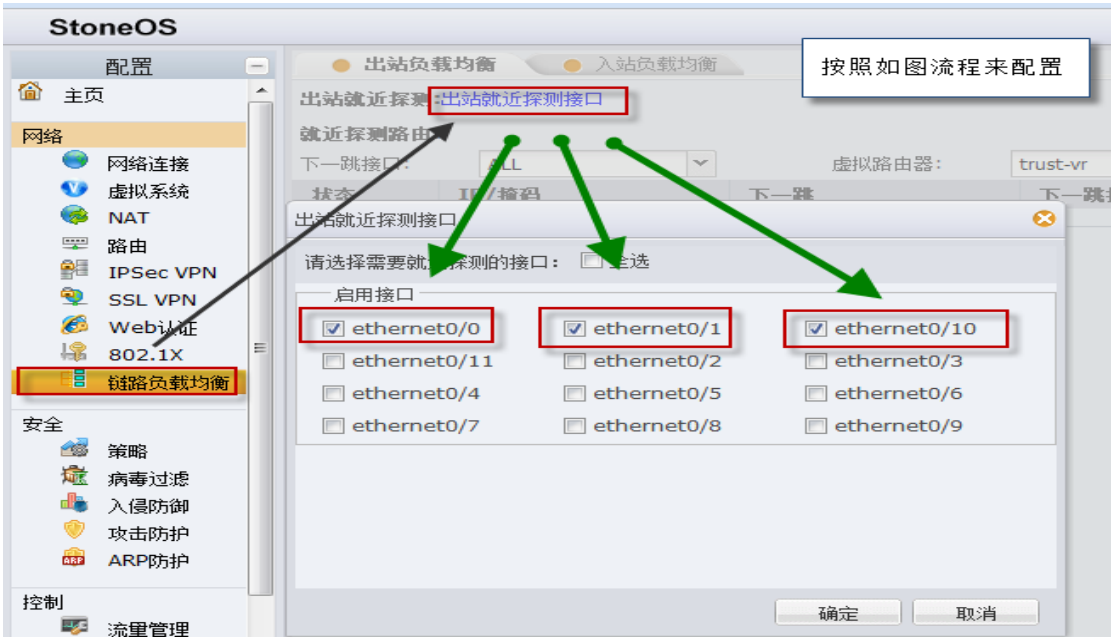
3．同样方法再新建一条策略路由，其中的服务选择 ICMP 得到配置如下 ：

按上述流程配置即可实现 192.168.1.1/24 网段对目的地址是 8.8.8.8 的 http 和 icmp 流量负载。

1.4 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，系统对只匹配到缺省路由的流量在符合条件的各条链路上进行探测，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。

配置如下图：

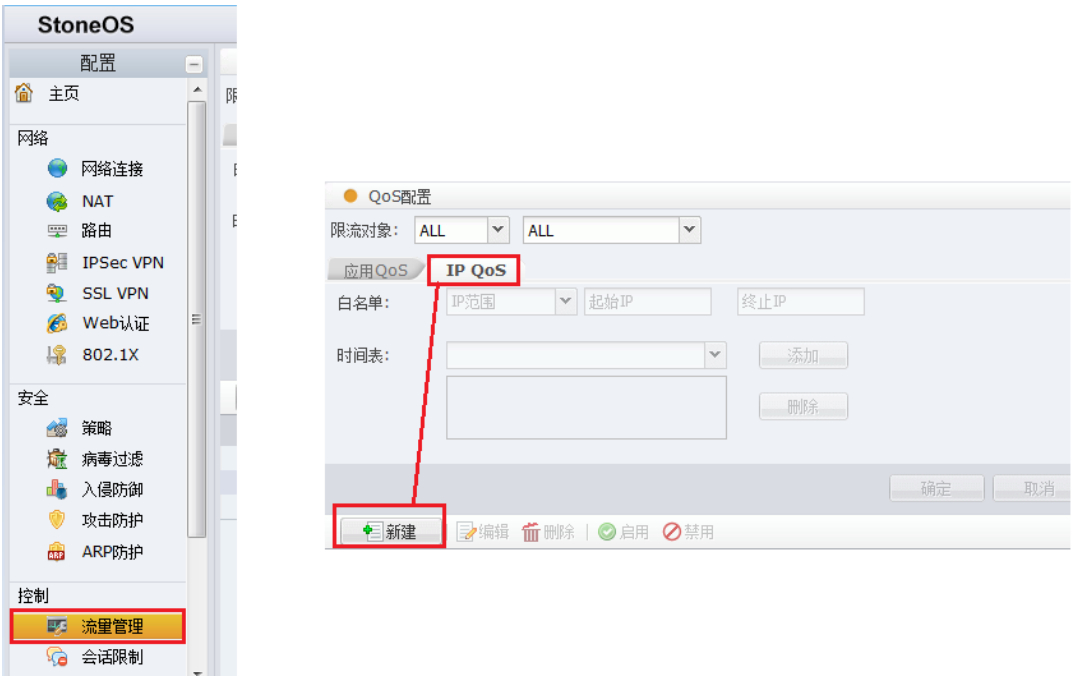


配置动态检测路由的老化时间和对应子网掩码：

二．流量控制 QOS 配置

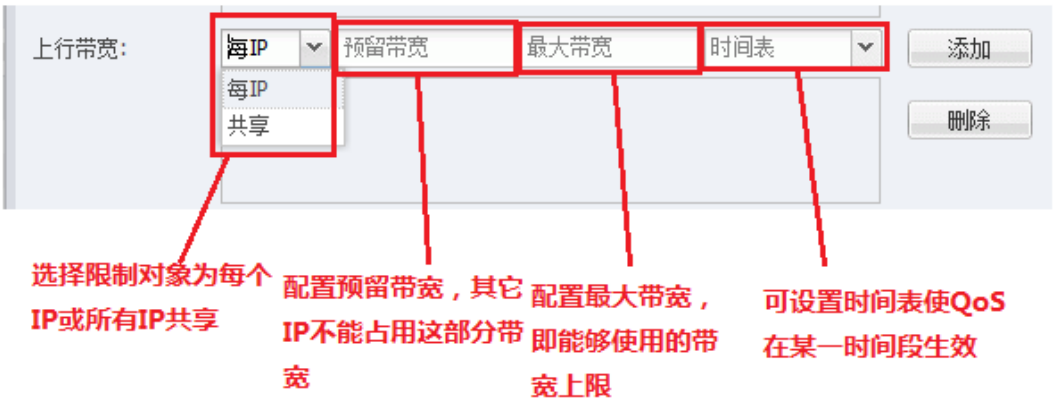
2.1 配置 IP QoS

1．进入配置界面，配置-控制-流量管理，点击 IP QoS-新建：



2．设置 IP QoS 的具体参数：

3．设置具体的限制带宽，以上行为例：

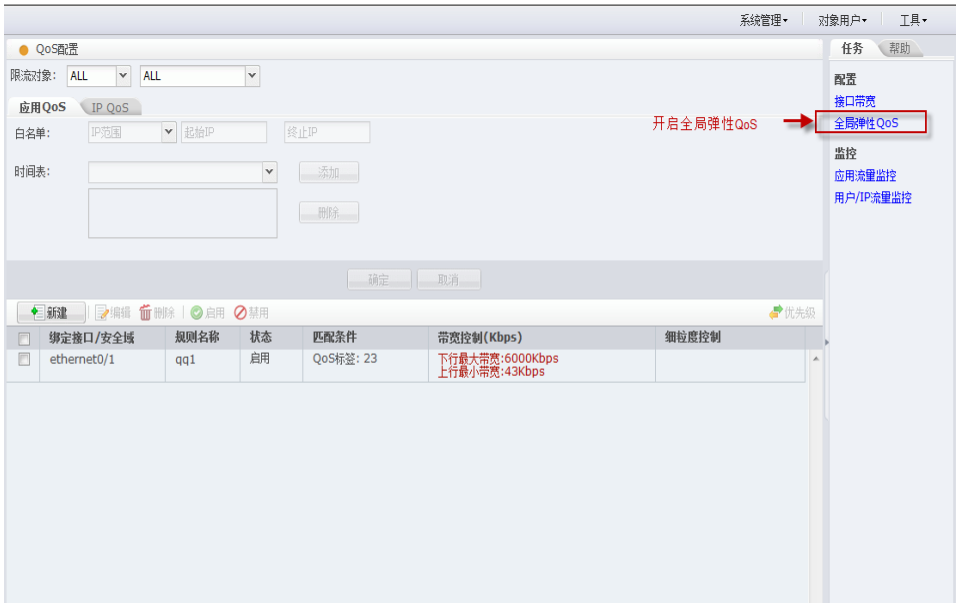


例：要配置 192.168.1.2 至 192.168.1.200 范围内 IP 在 e0/2 每 IP 上下行预留带宽 200K，最大带宽 1M，配置如下图所示：

IP QoS 的高级配置：

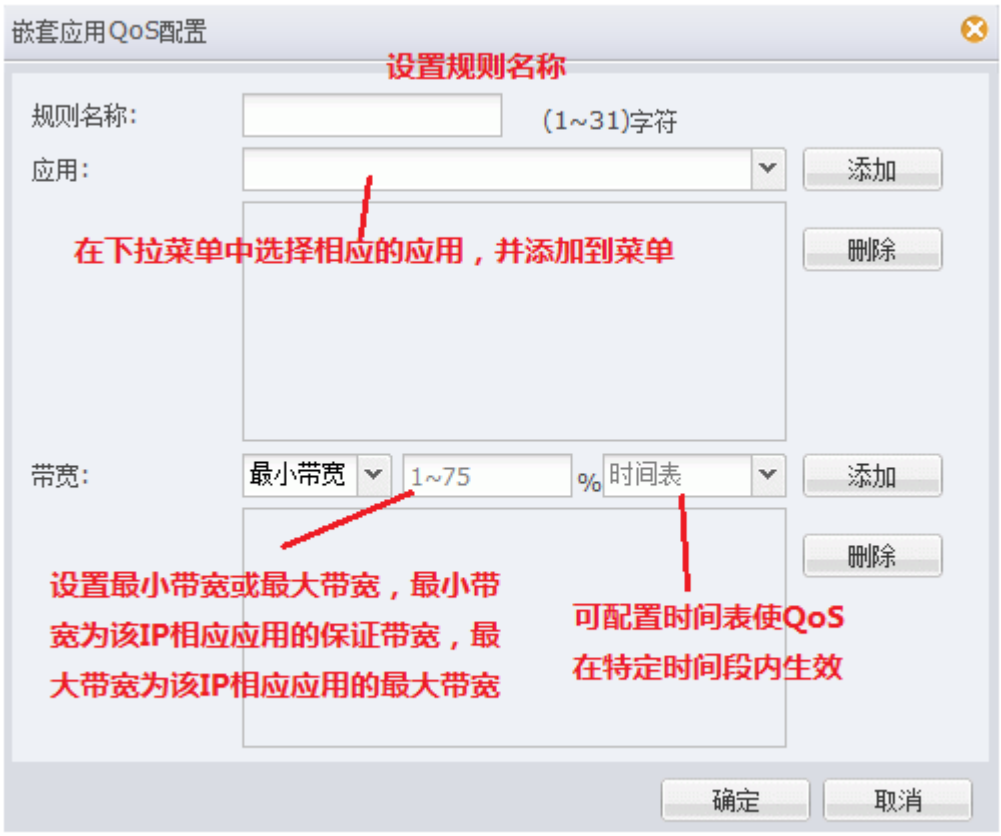
点击高级配置选项卡，进入高级配置页面：

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



细粒度控制：可在 IPQoS 的基础上，进行应用 QoS 的嵌套使用，进行更精确的 QoS 控制。

点击“添加嵌套应用 QoS 规则”，进入配置页面：



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。

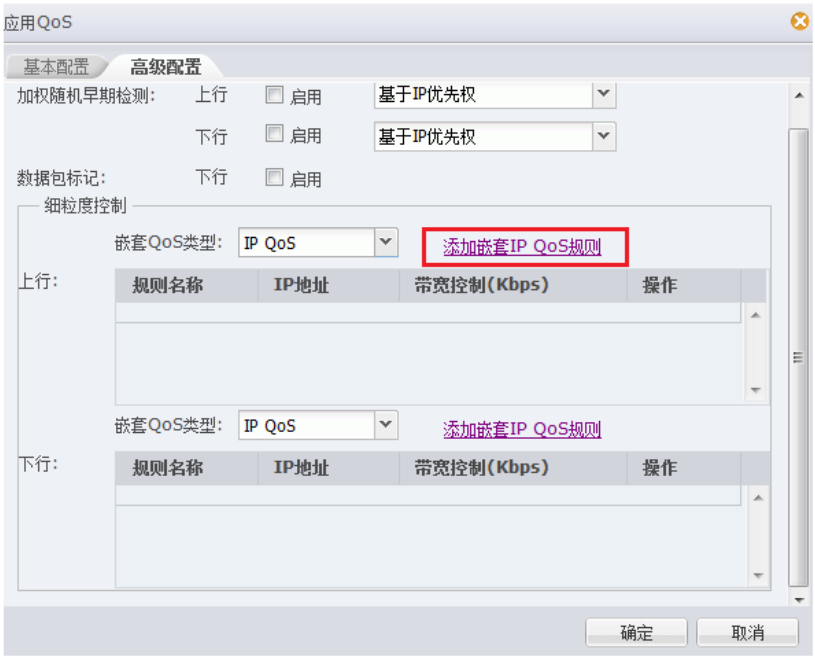
2.2 配置应用 QoS

1. 点击应用 QoS-新建，进入配置页面：

例：限制 P2P 软件及 P2P 流媒体在 e0/2 接口上行最大流量为 10M，如图所示：

应用 QoS 的细粒度控制：

点击“高级配置”选项卡，进入高级配置：

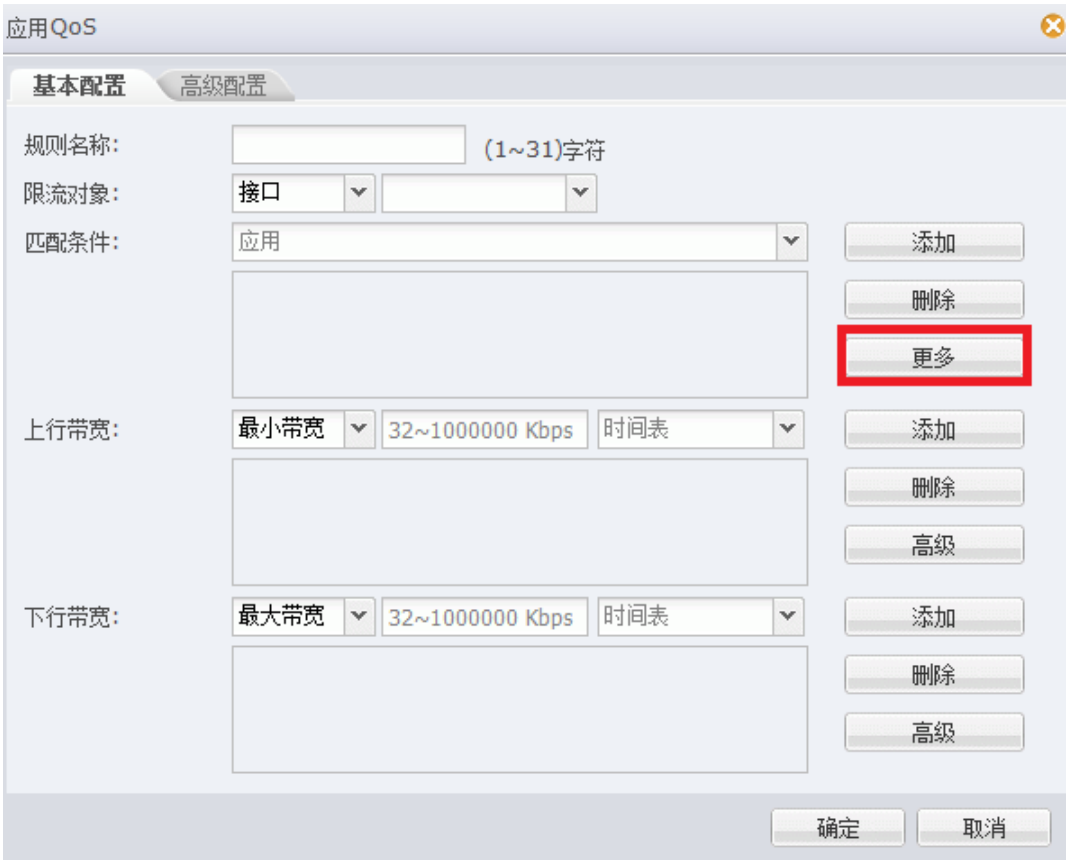


注意：使用应用 QoS 需要打开相应安全域的应用识别以及安装应用特征库许可证。

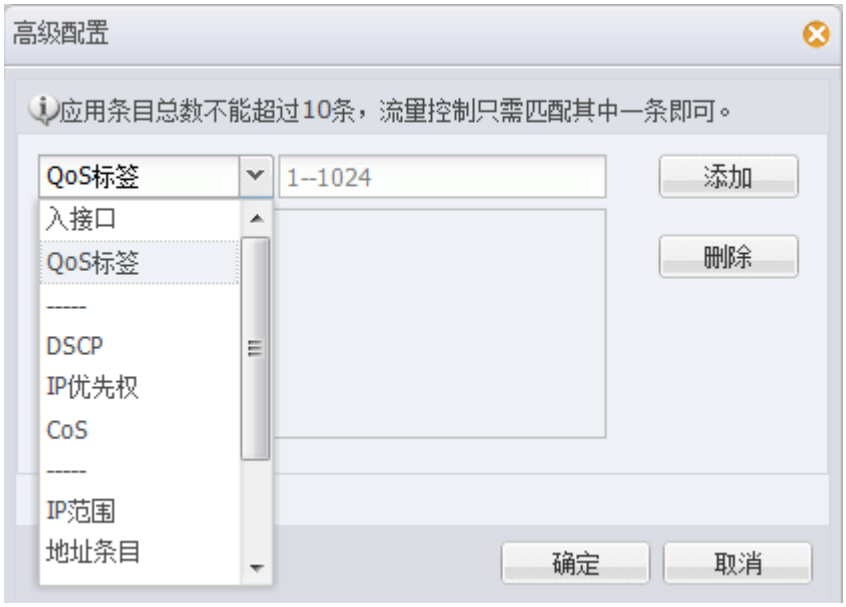
2.3 配置混合 QoS

HillStone 设备中的 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。

1. 点击应用 QoS-新建，进入配置页面，如下图，点击匹配条件右侧的“更多”：



2. 如下图所示，可针对策略标签，IP 优先权，IP 范围，地址条目等进行控制：



2.4 配置 QoS 白名单

以 IP QoS 的白名单为例，在流量管理界面上方，选择相应的限流对象，如下图所示，根据 IP 及时间表配置相应的白名单即可。

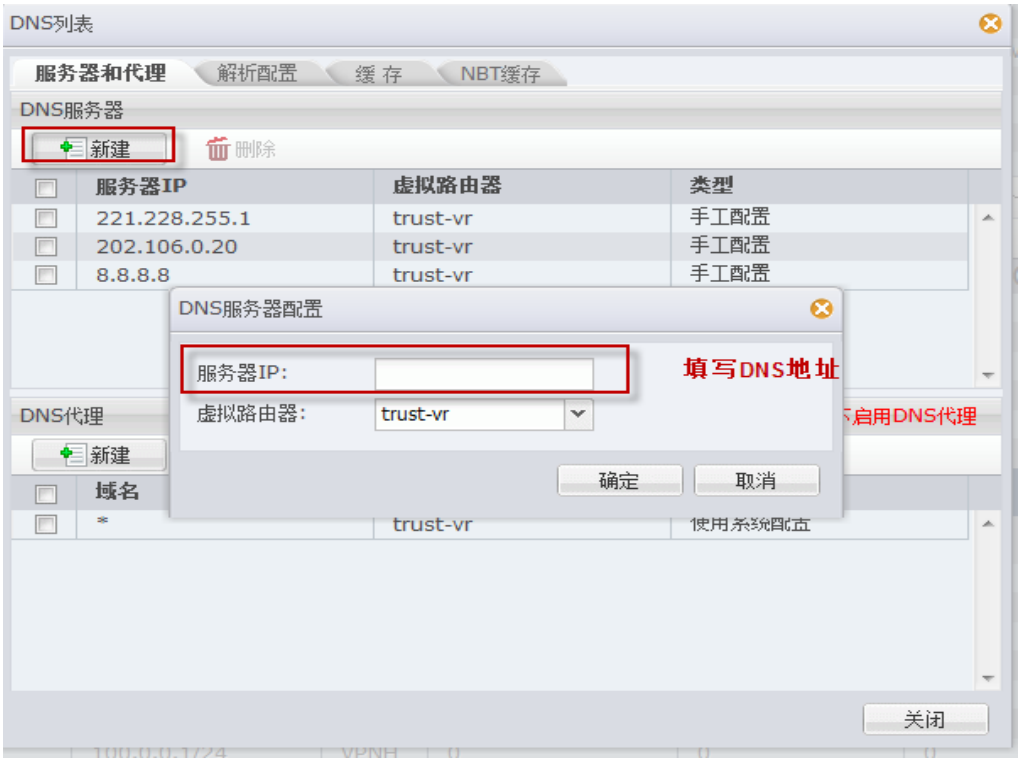
三．NBC 网络行为控制配置

在配置 NBC 功能中的 URL 过滤、bypass 域名以及应用行为控制等于网络域名有关的功能时，需要现在防火墙上进行防火墙 dns 的配置，并且尽量保证防火墙使用的 dns 与内部电脑的 dns 一致。

防火墙 DNS 配置方法：

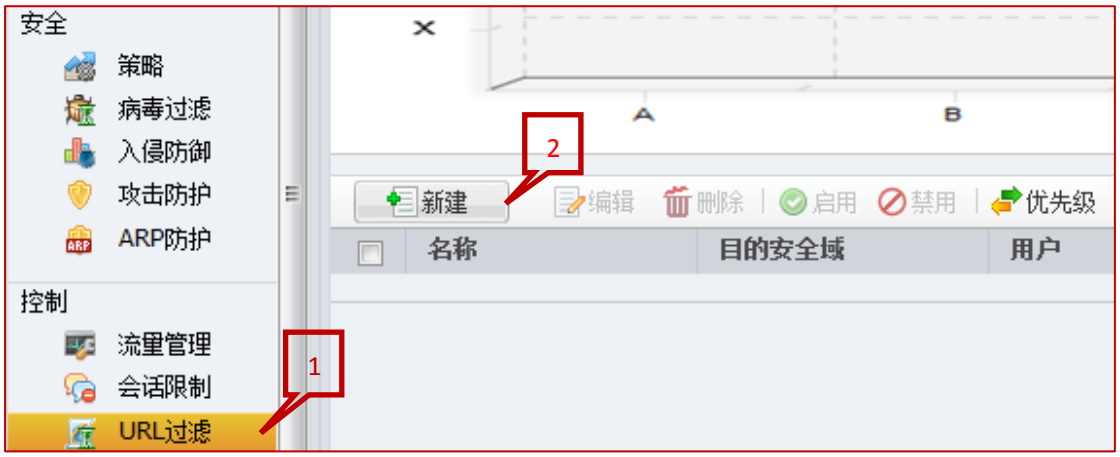
1．点击界面右侧“网络连接”，选择该界面右侧的“dns 列表”：

2．在弹出的 DNS 列表中点击新建，填入 dns 服务器 ip 地址；



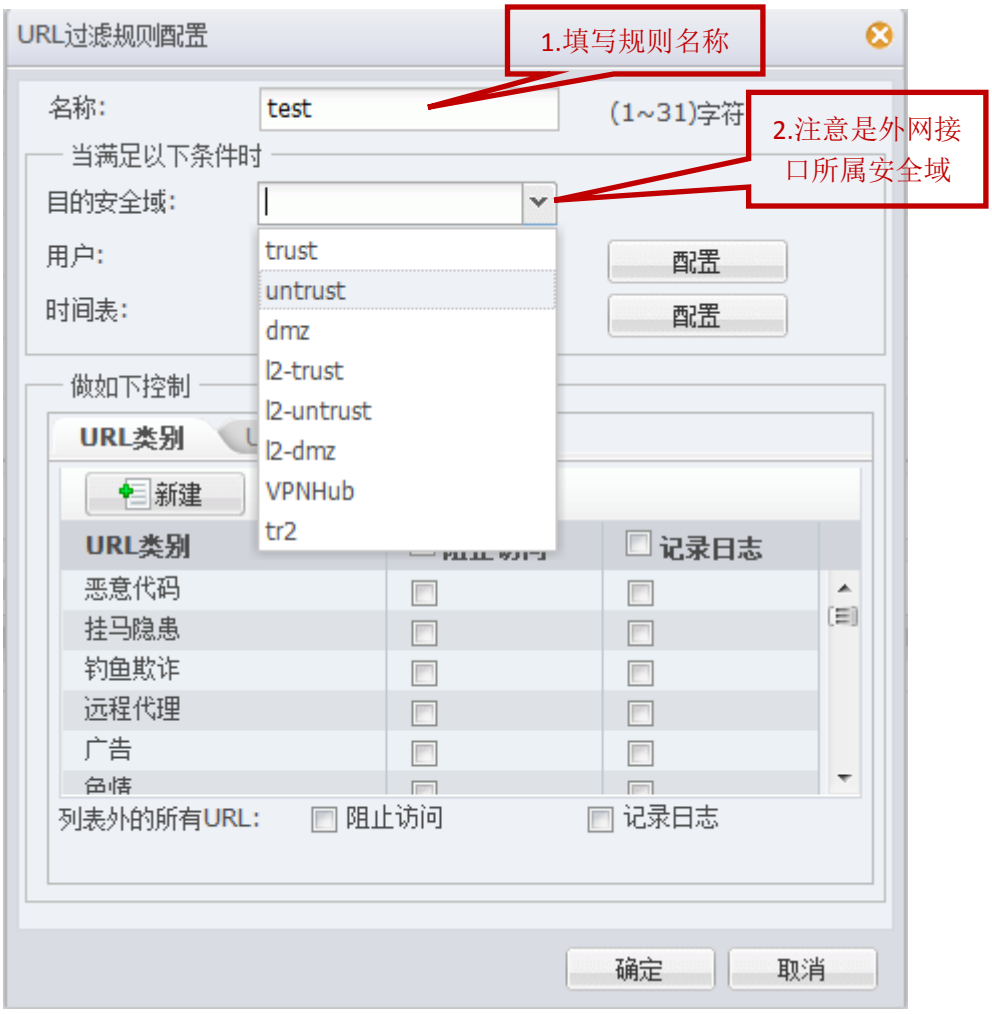
3.1 URL 过滤(有 URL 许可证)

1. 登陆设备主界面后，点 URL 过滤，再点新建：

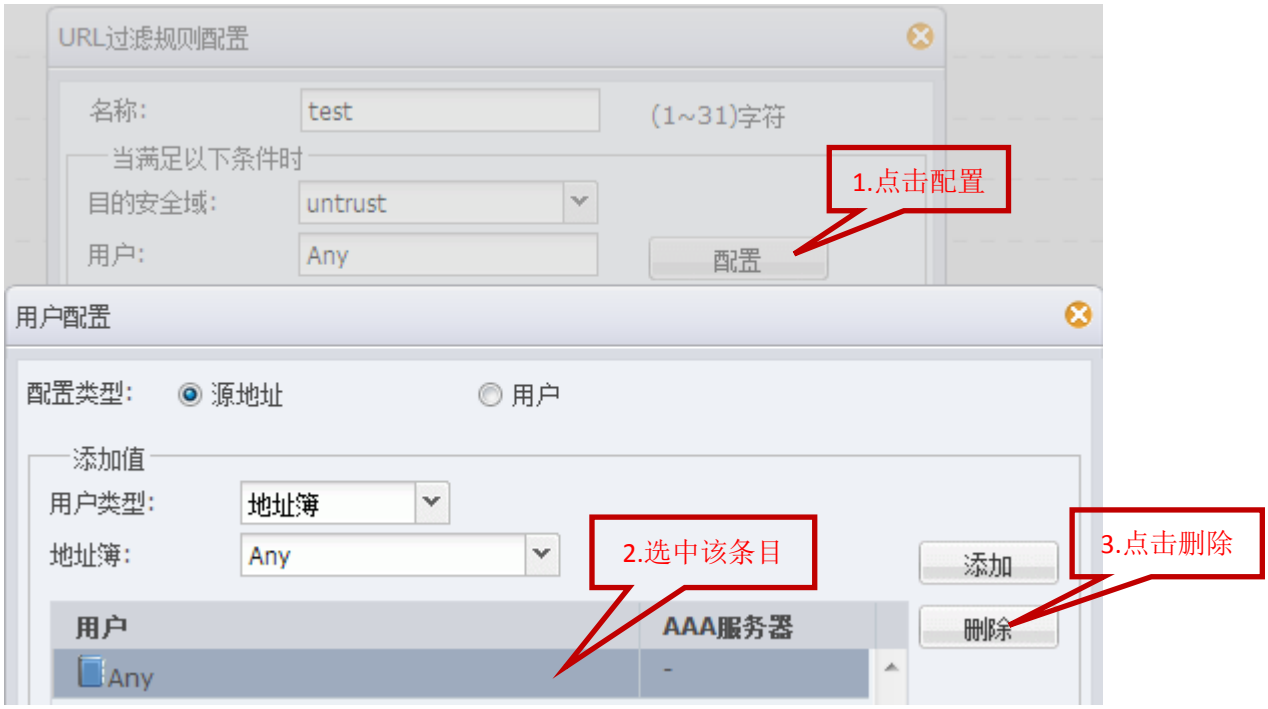


2. 进入 URL 过滤规则配置，名称中填写该规则的名字

点击目的安全域的下拉菜单选择目的安全域，需要注意的是应该选择外网接口所属安全域：

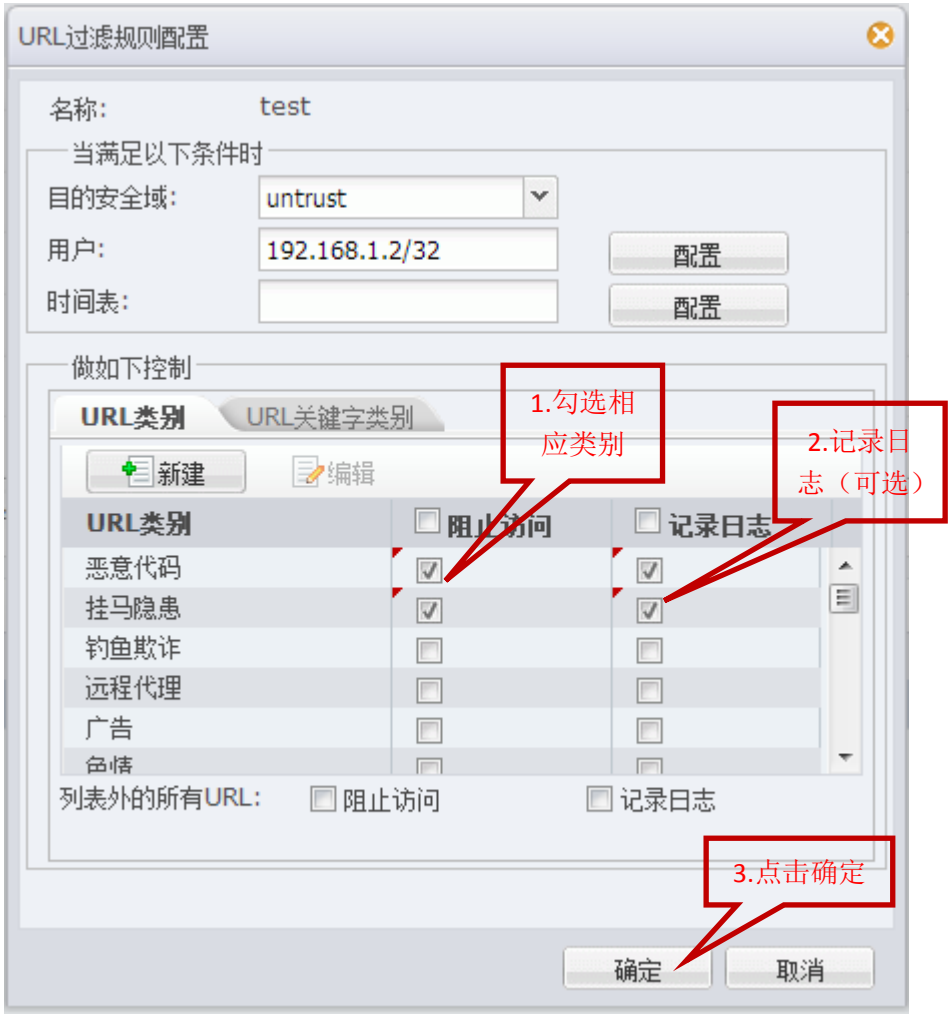


4．用户配置选择相应的用户，默认是 any，即全部内网用户，如果要修改，则先删除 any 用户：



5．然后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：

6.配置所要阻止的网站，也可以在用户访问该类网站的时候记录日志（可选）：

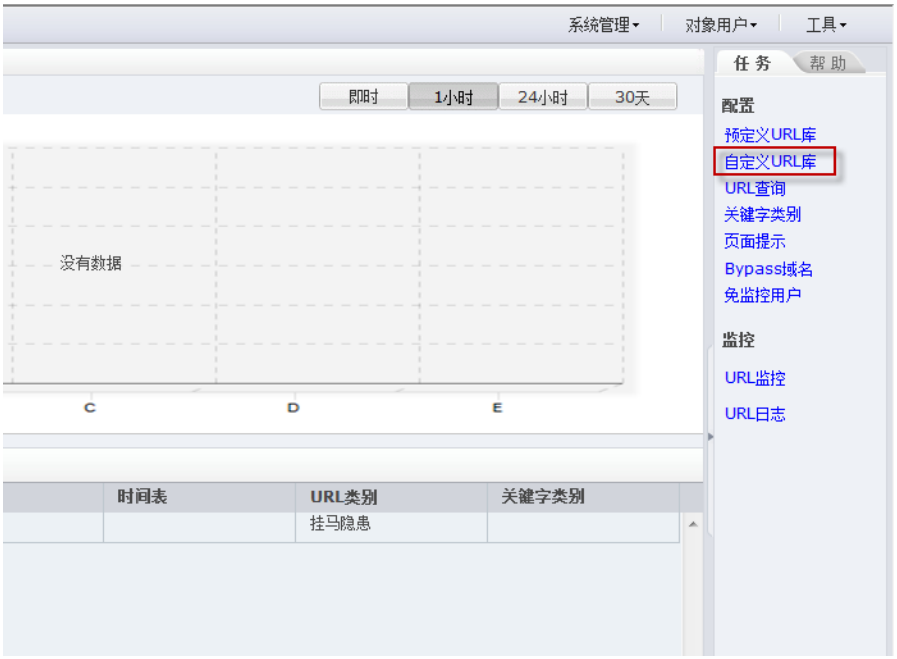


通过上述配置，即可实现阻止内网 192.168.1.2 这个 ip 访问“恶意代码”和“挂马隐患”这两类网站。

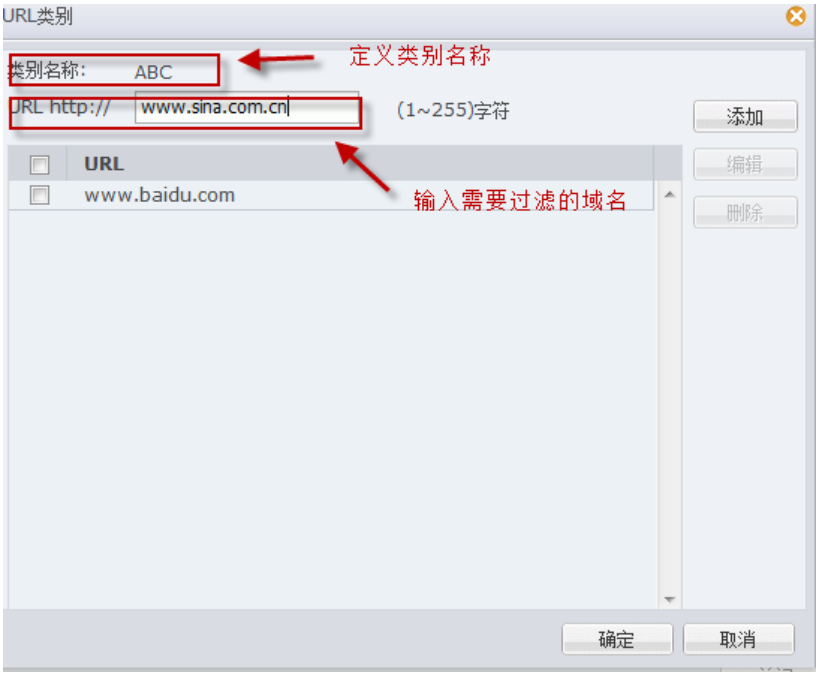
自定义 URL 分类：

配置界面右侧的“URL 查询”功能可以用来查询网站属于哪个预定义的 URL 类别，如果需要控制的网站不在预定义的 URL 类别中，可通过自定义 URL 库进行控制，方法如下：

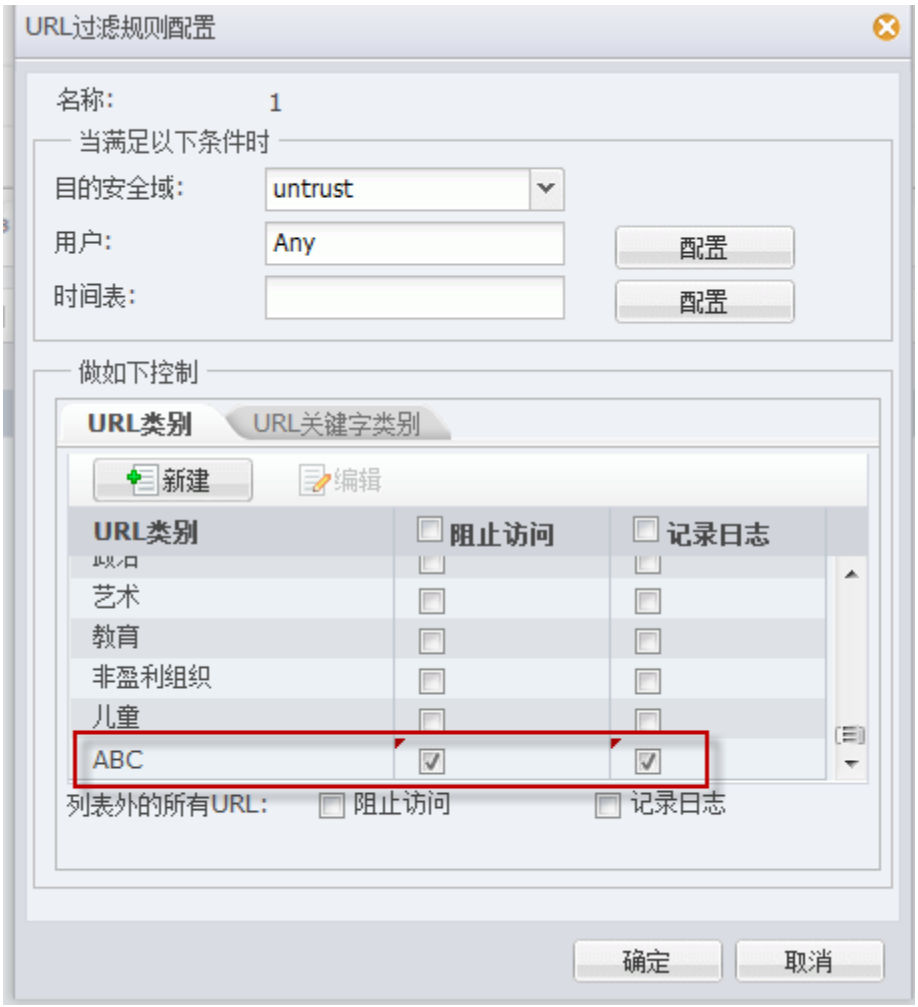
1．点击页面右侧的“自定义 URL 库”：



2．在弹出的自定义页面中点击“新建”，输入自定义的 URL 类别名称和需要过滤的域名，点击添加后确定：



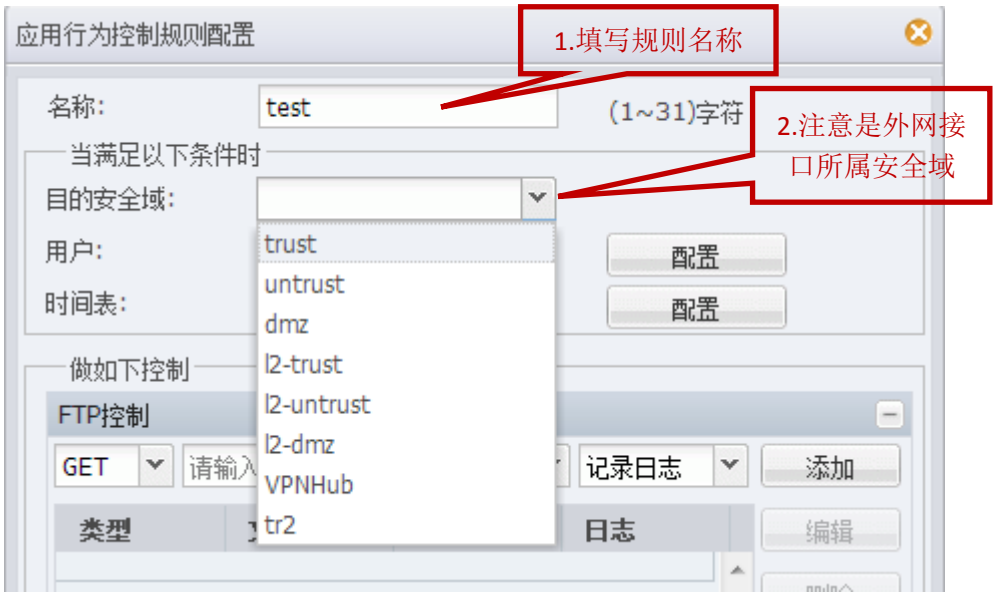
3．在配置 URL 过滤时找到自定义的类别，选择控制动作：



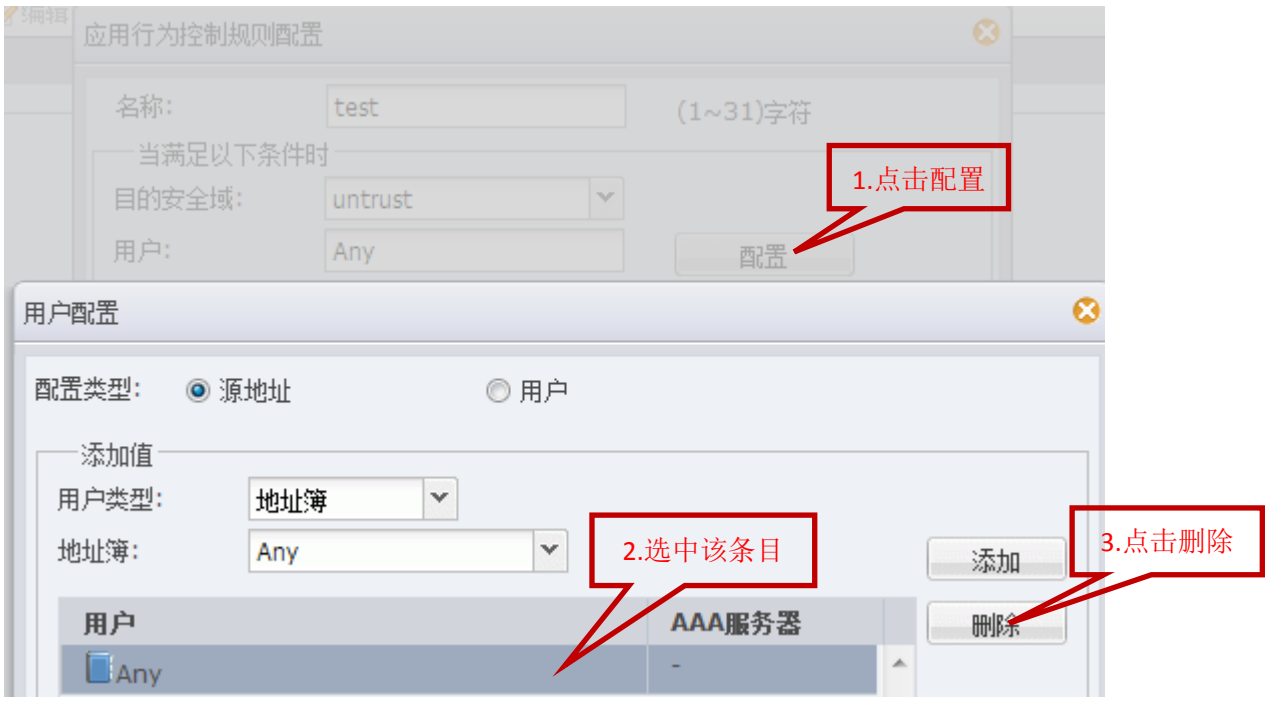
3.2 URL 过滤（无 URL 库许可证）

1．选择应用行为控制，点击新建：

2．进入应用行为控制规则配置，名称中填写该规则的名字，点击目的安全域的下拉菜单选择目的安全域，需要注意的是应该选择外网接口所属安全域：



3．用户配置选择相应的用户，默认是 any，即全部内网用户，如果要修改，则先删除 any 用户：



4．然后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：

5. 点击 HTTP 控制：

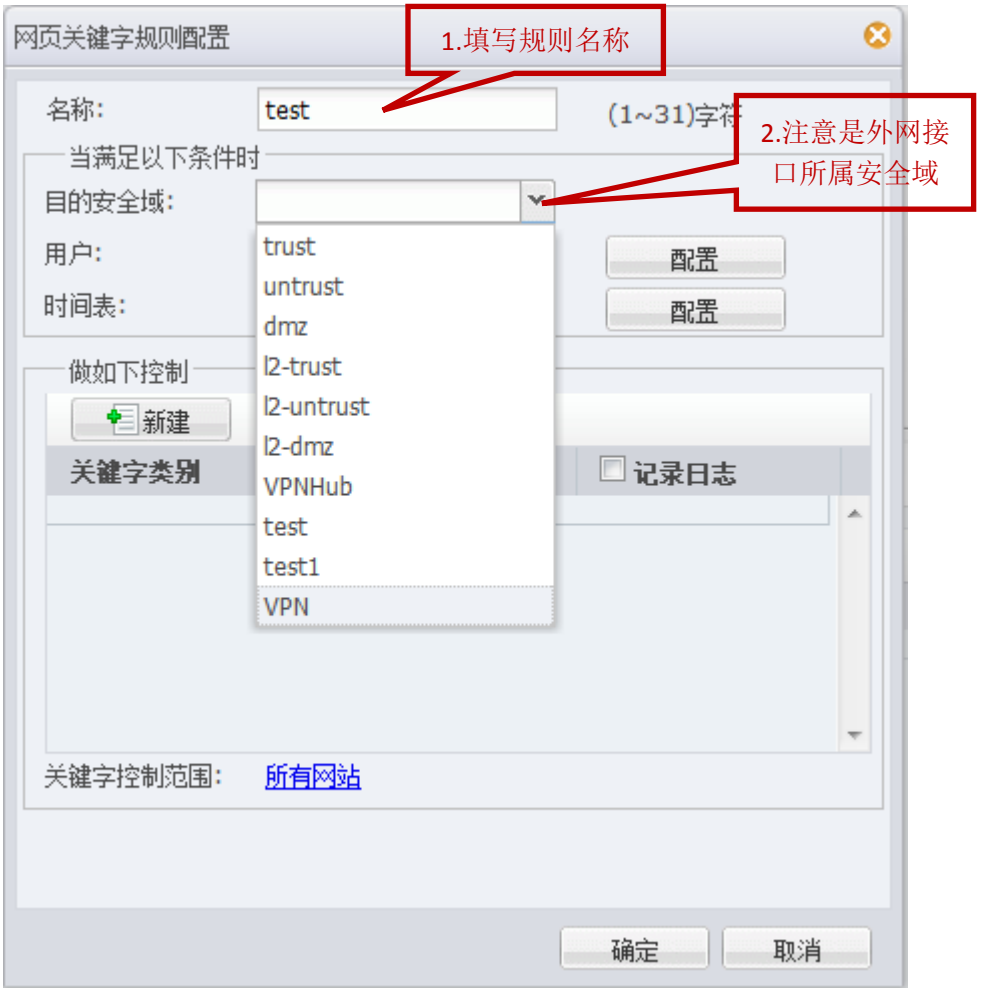
6. 添加要阻止的网站，*号表示通配符，这样该网站的子域名也会一起禁止，如果是仅需阻止单个域名，则填写该域名全称，也可以在用户访问该网站的时候记录日志（可选）：

通过上述配置，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。

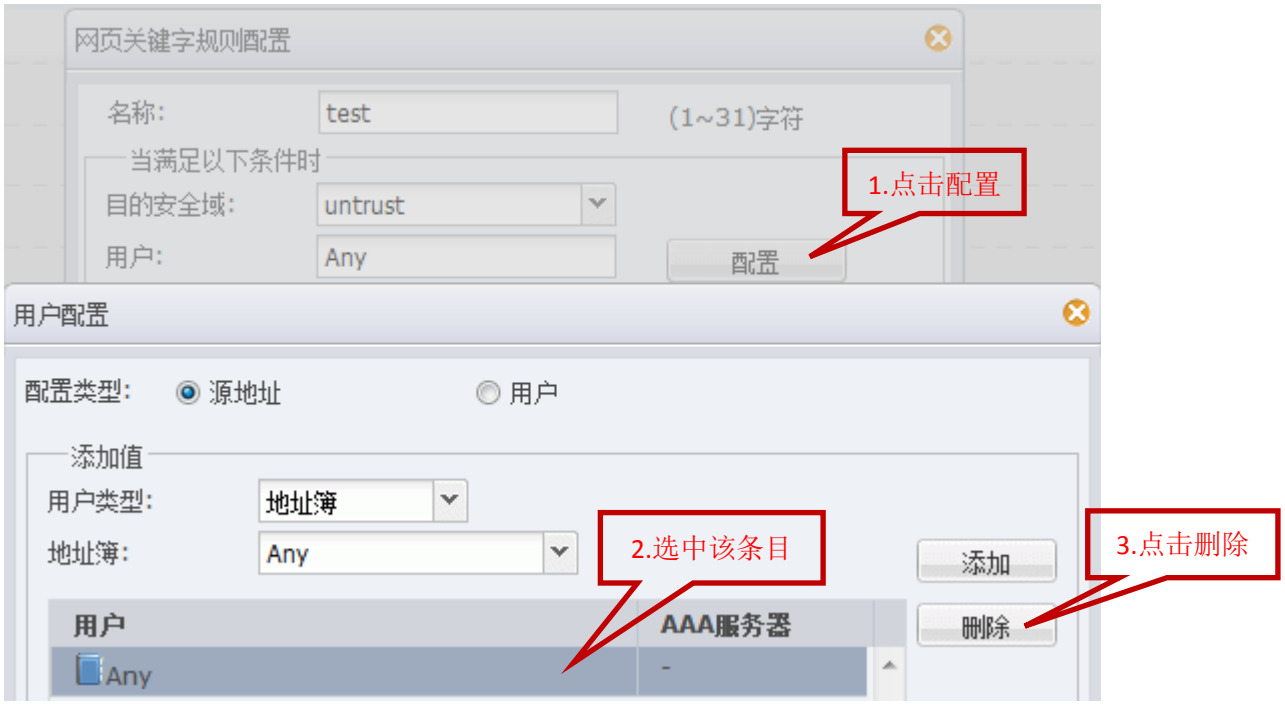
3.3 网页关键字过滤

1．登陆设备主界面后，选择网页关键字，点击新建：

2．进入网页关键字规则配置，名称中填写该规则的名字，点击目的安全域的下拉菜单选择目的安全域，需要注意的是应该选择外网接口所属安全域：



3．用户配置选择相应的用户，默认是 any，即全部内网用户，如果要修改，则先删除 any 用户：



4．然后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：

5．点击新建：

6．填写关键字类别名称，然后点击新建：

新建关键字列表，点击添加

7. 点击确定，选择相应的控制动作：

通过上述配置，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。

Baypass 域名

如果在设备上需要剔除某些不进行控制的网站，即配置白名单功能，可以在bypass域名中进行设置，设置 Bypass 域名后，系统将无条件允许用户对Bypass域名的访问，不受网络行为控制功能的控制。

注意：

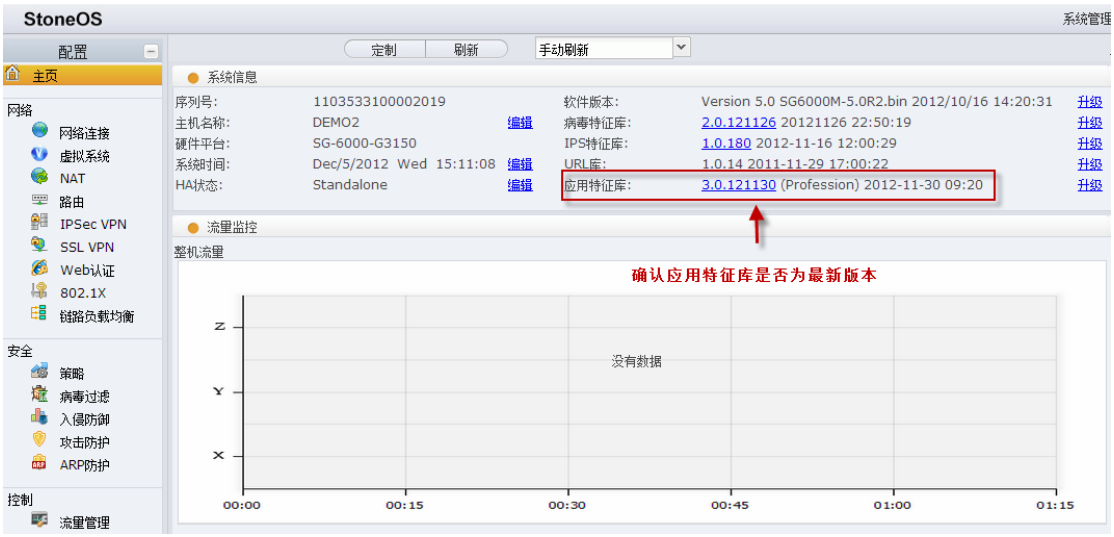
1. 系统对 Bypass 域名采用精确匹配。
2. Bypass 域名对整个系统生效。

3.4 网络聊天控制

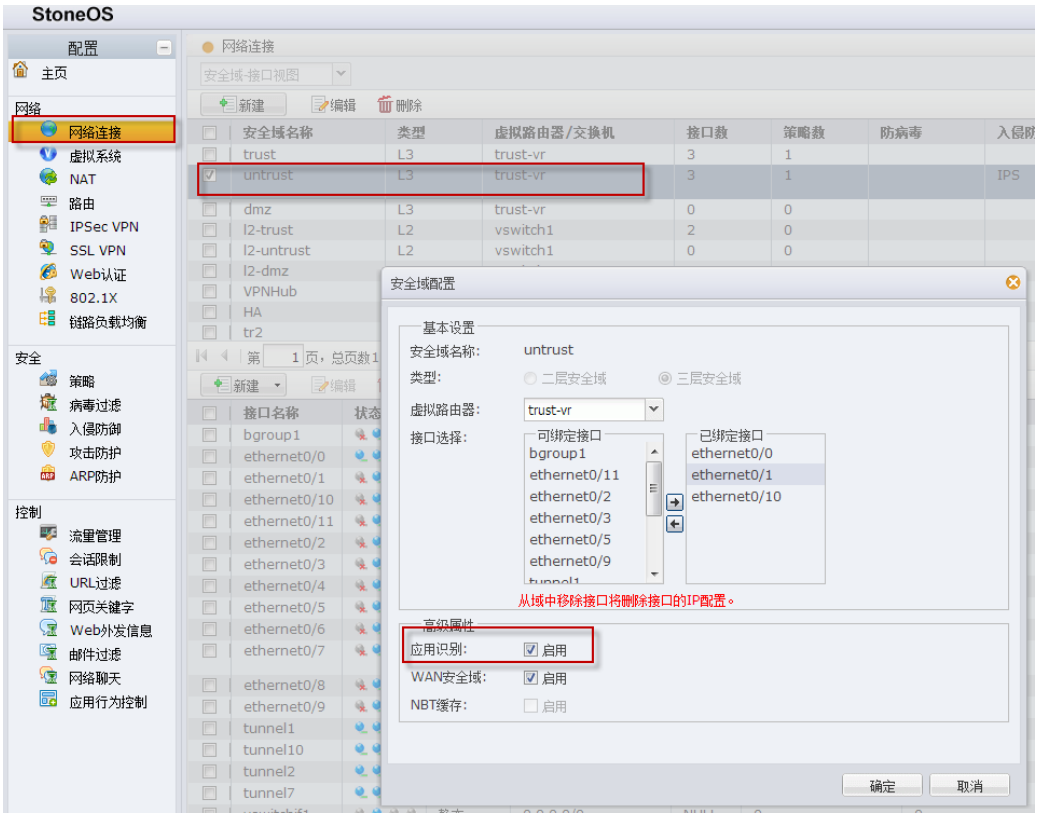
网络聊天功能可以通过聊天软件的账号控制用户使用 MSN、QQ 和雅虎通聊天的行为，并记录上下线日志。

以最常见的 QQ 控制为例，配置方法如下：

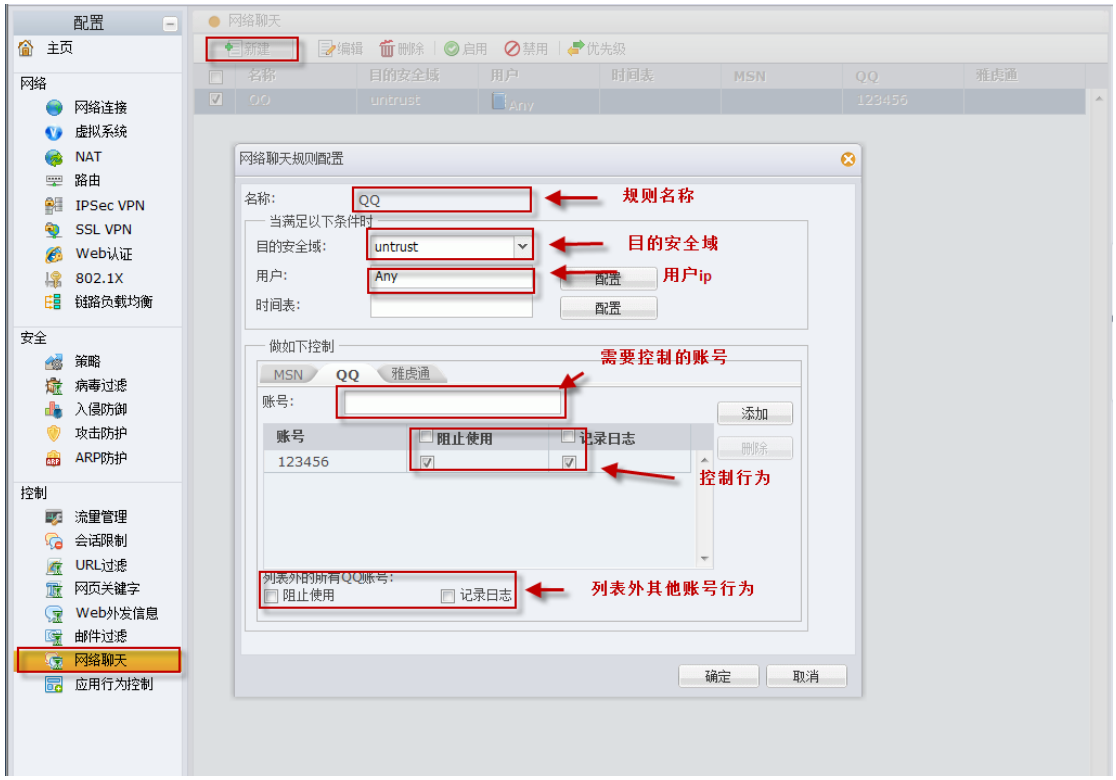
1. 确认设备已经安装了最新的应用特征库：



2. 打开内外安全域的应用识别功能，点击“网络连接”，双击相应的安全域，打开“高级属性”中的“应用识别”：



3. 点击左侧“控制”“网络聊天”，新建规则：



4. 如果想要阻止所有的 qq 账号都无法登录，则可以直接配置“列表外的所有 qq 账号阻止使用”或者直接通过防火墙的策略进行 qq 应用的阻止。

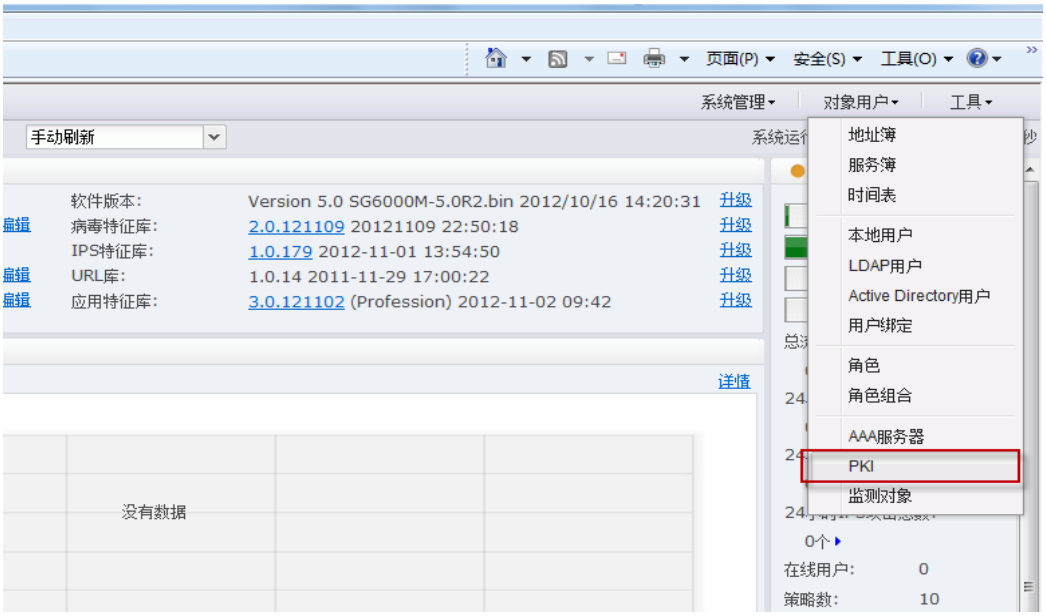
四．VPN 高级配置

4.1 基于 USB-KEY 的 SCVPN 配置

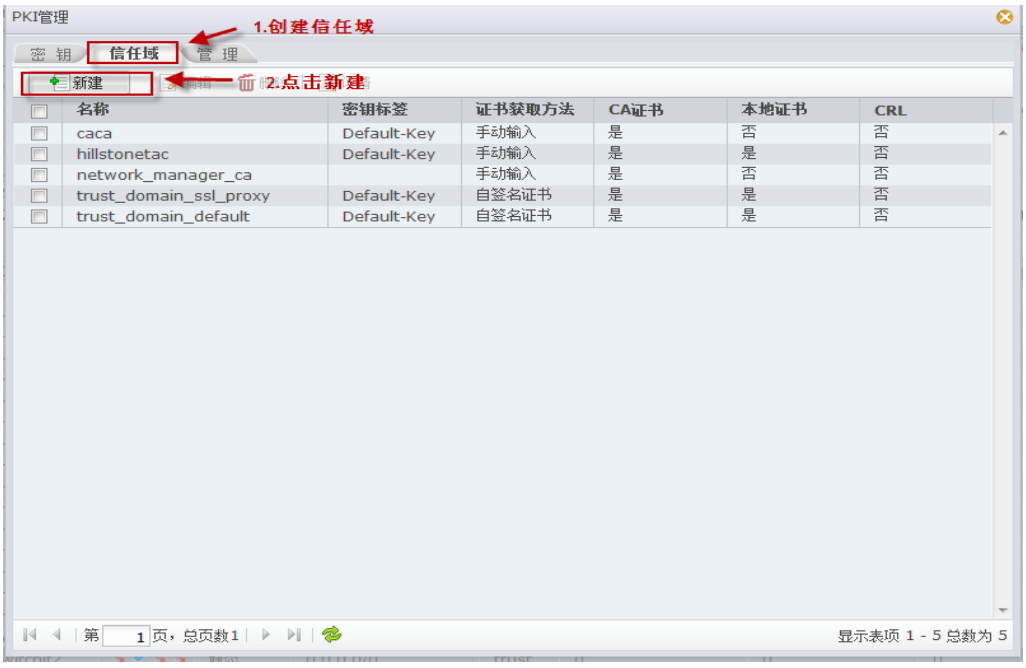
此处介绍的是基于 USB-KEY 的 SSL VPN 配置，普通 SSL VPN 配置请参考“Hillstone 基础配置手册”或者直接按照配置向导配置。

一． 创建 SSL VPN 信任域

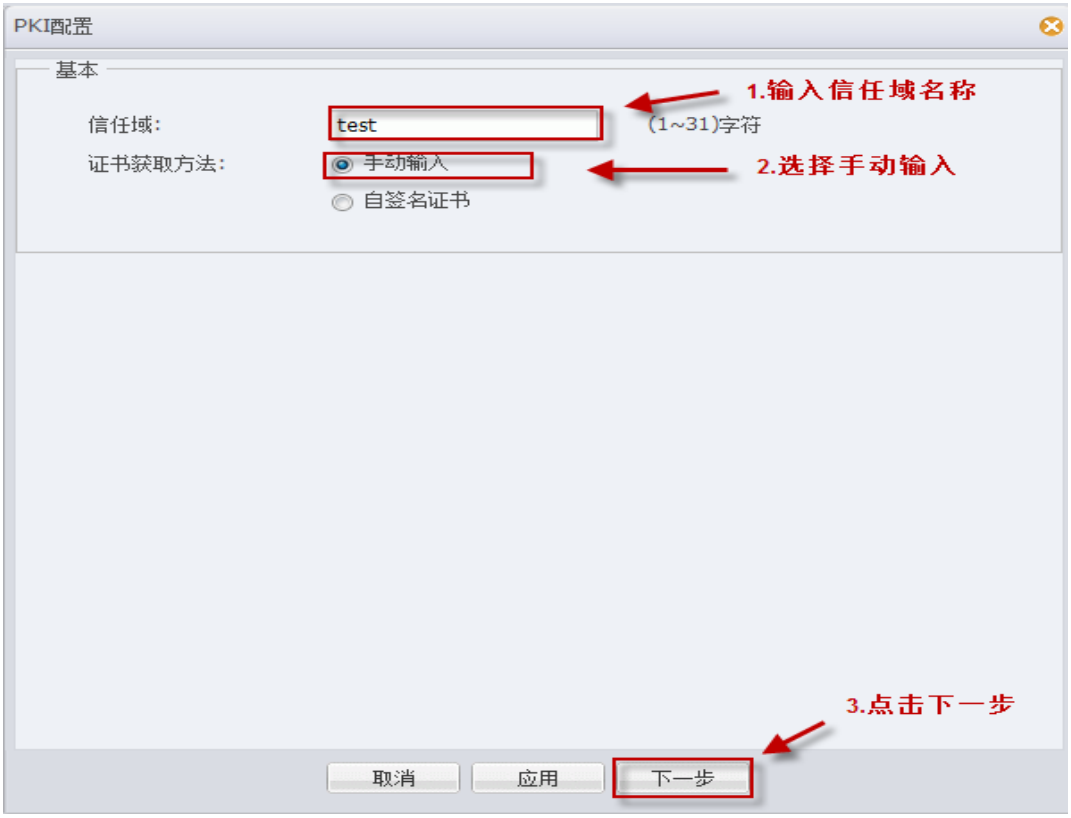
1．点击界面右上角“对象用户”—“PKI”：



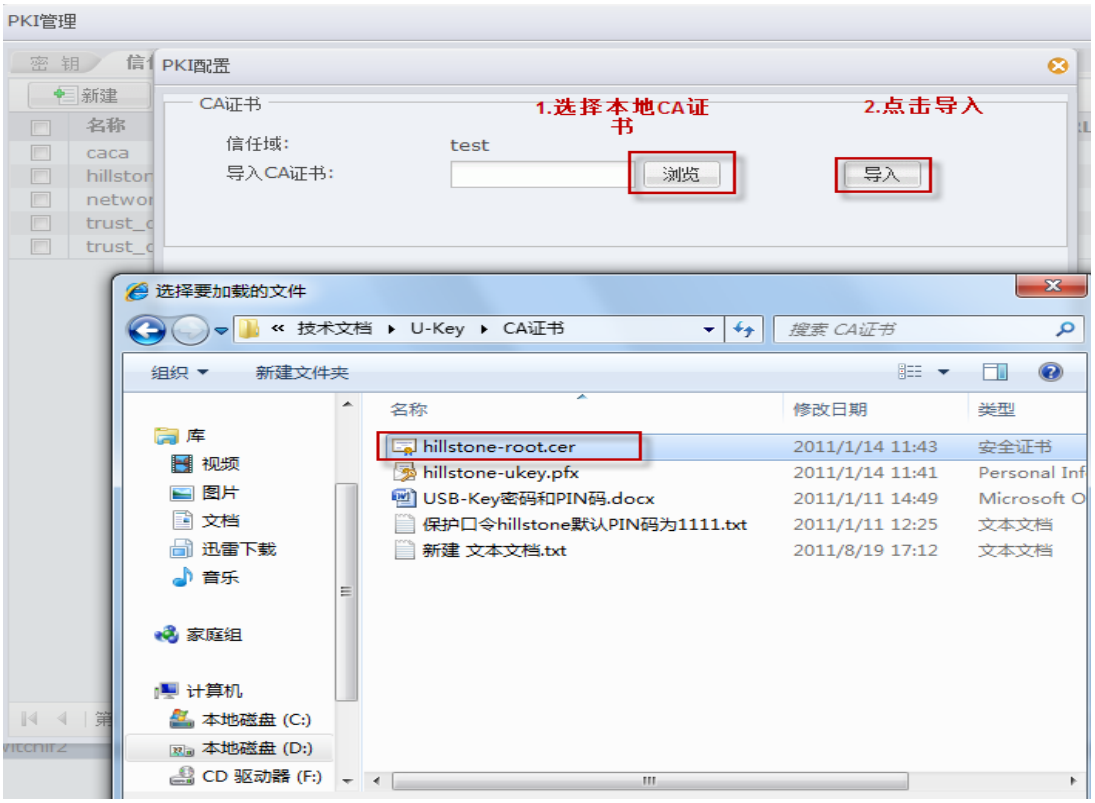
2．选择“信任域”，点击“新建”：



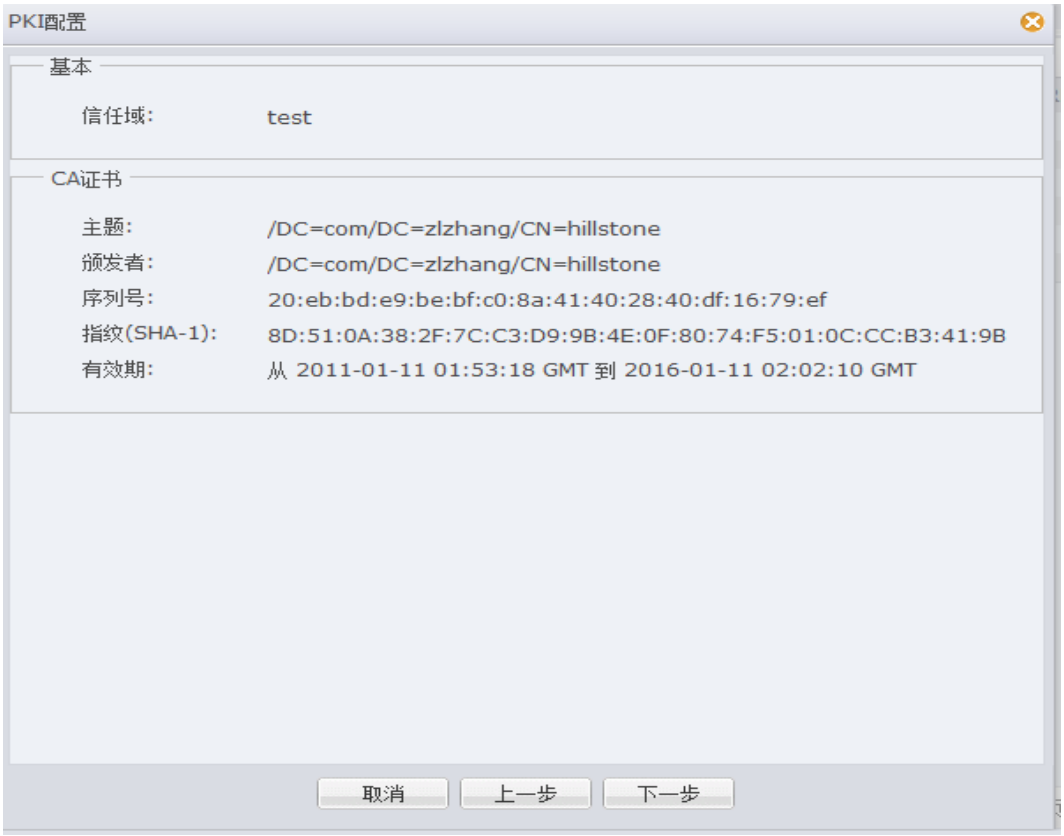
3．输入信任域名称，选择“手动输入”：



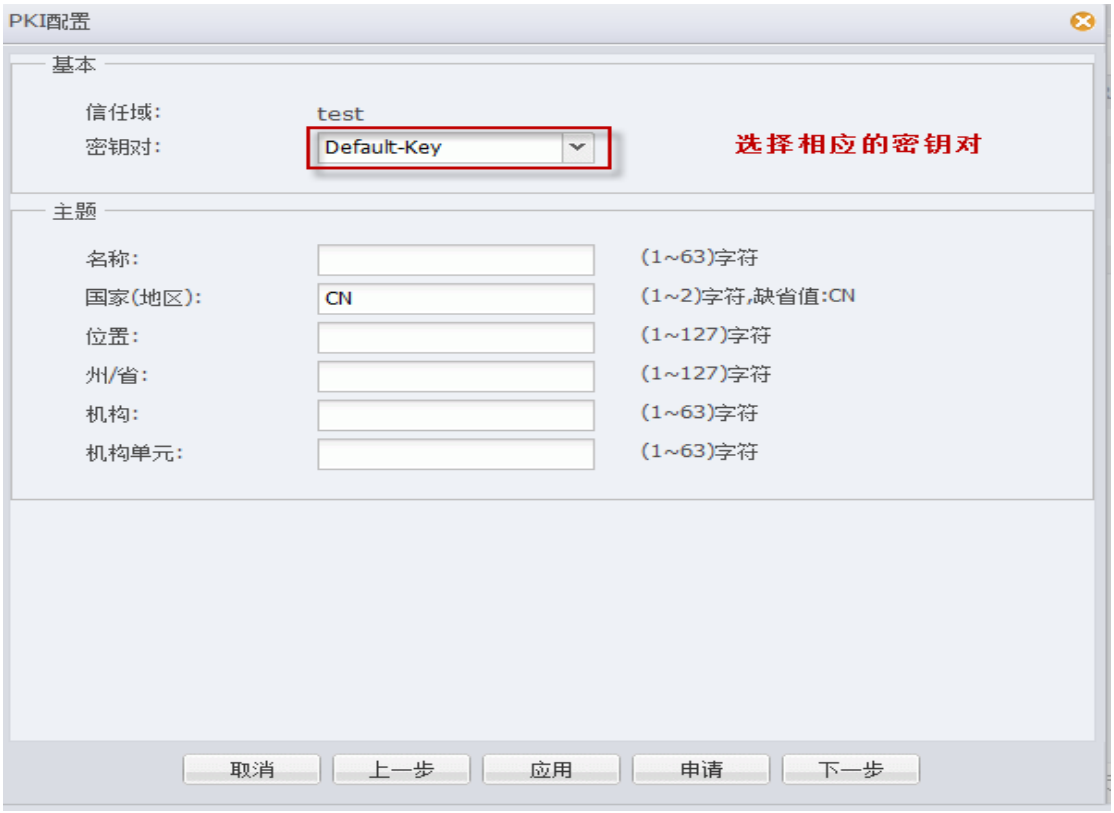
4．导入需要使用的 CA 证书：



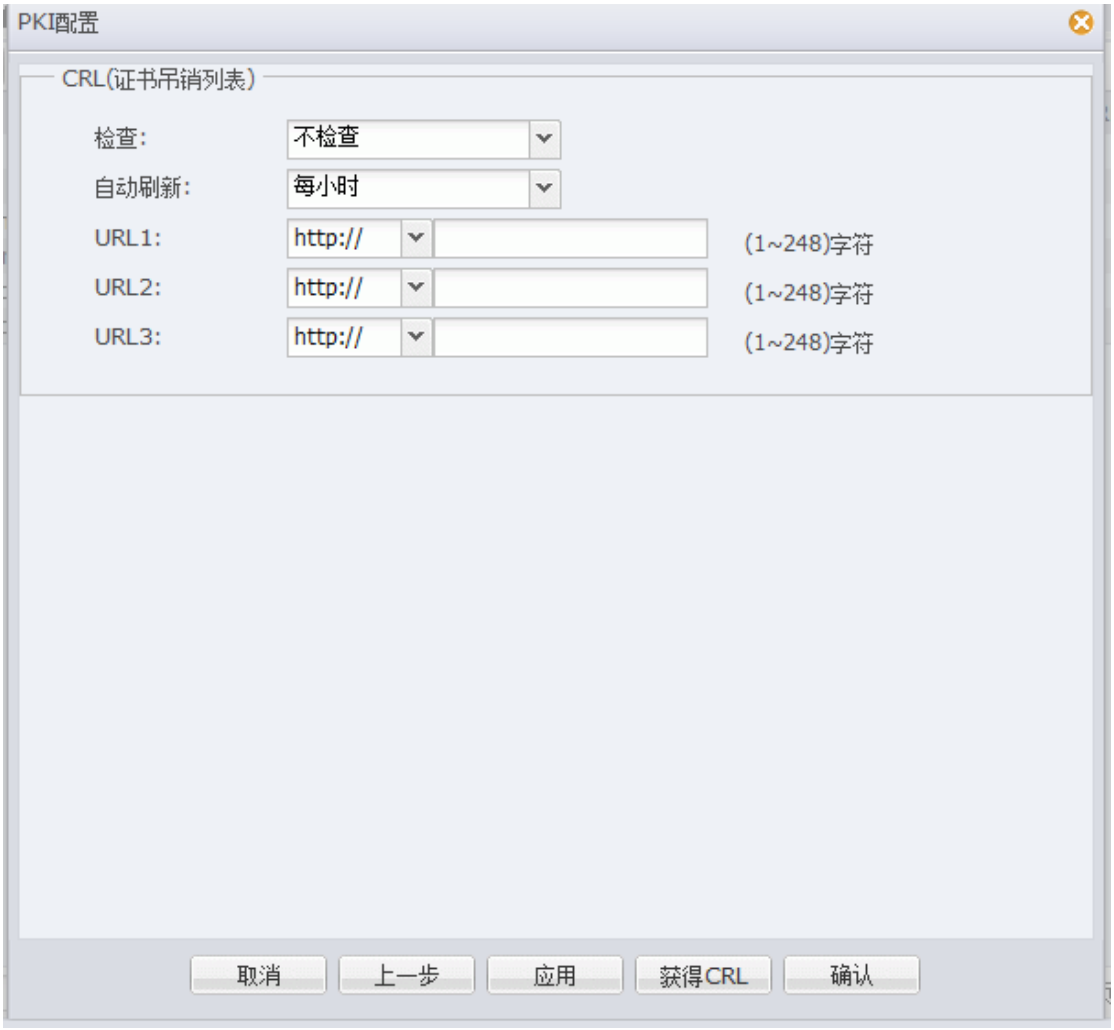
5．导入成功后可看到 CA 证书相关信息：



6．选择相应的“密钥对”，其他信息可选填：

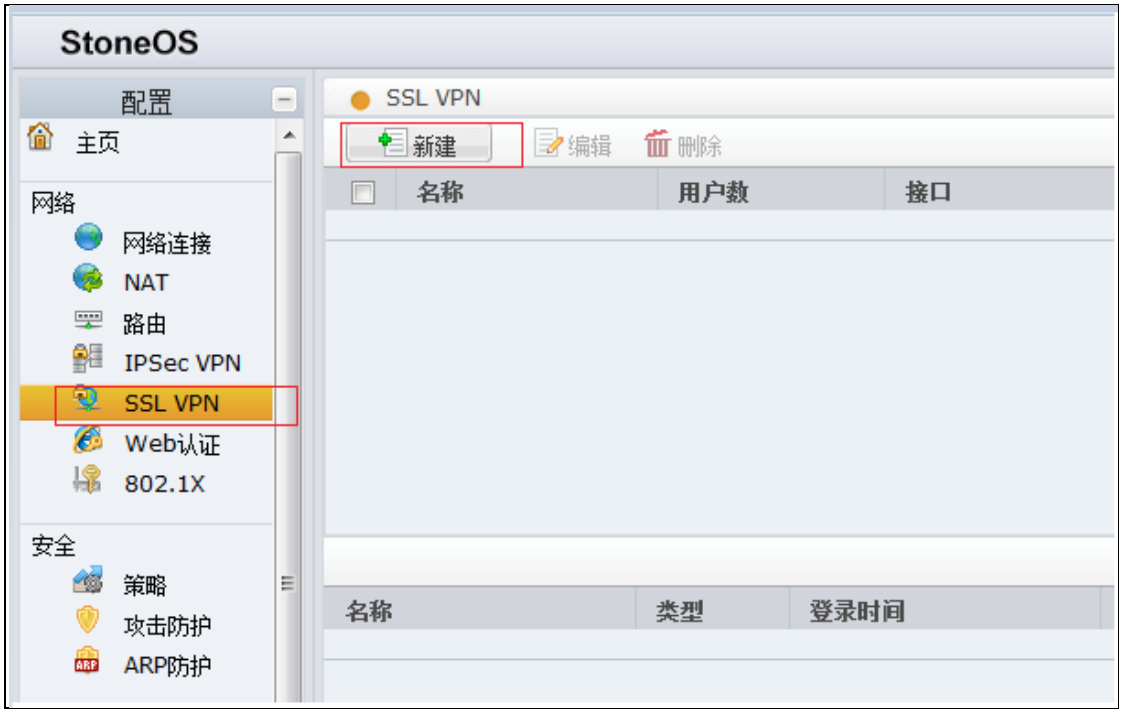


7．根据需求填写 CRL；如无，则直接“确认”：



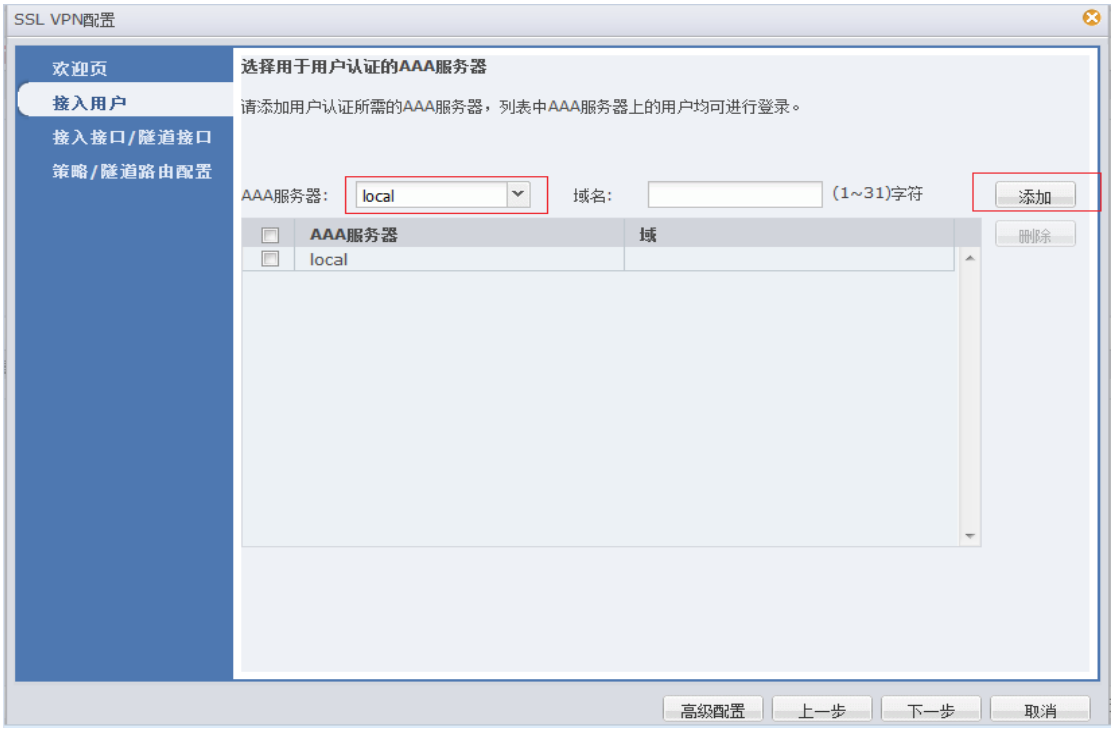
二． 配置 SSL VPN

1．WEB 界面登陆防火墙后，点击“配置”，“网络”，“SSL VPN”：

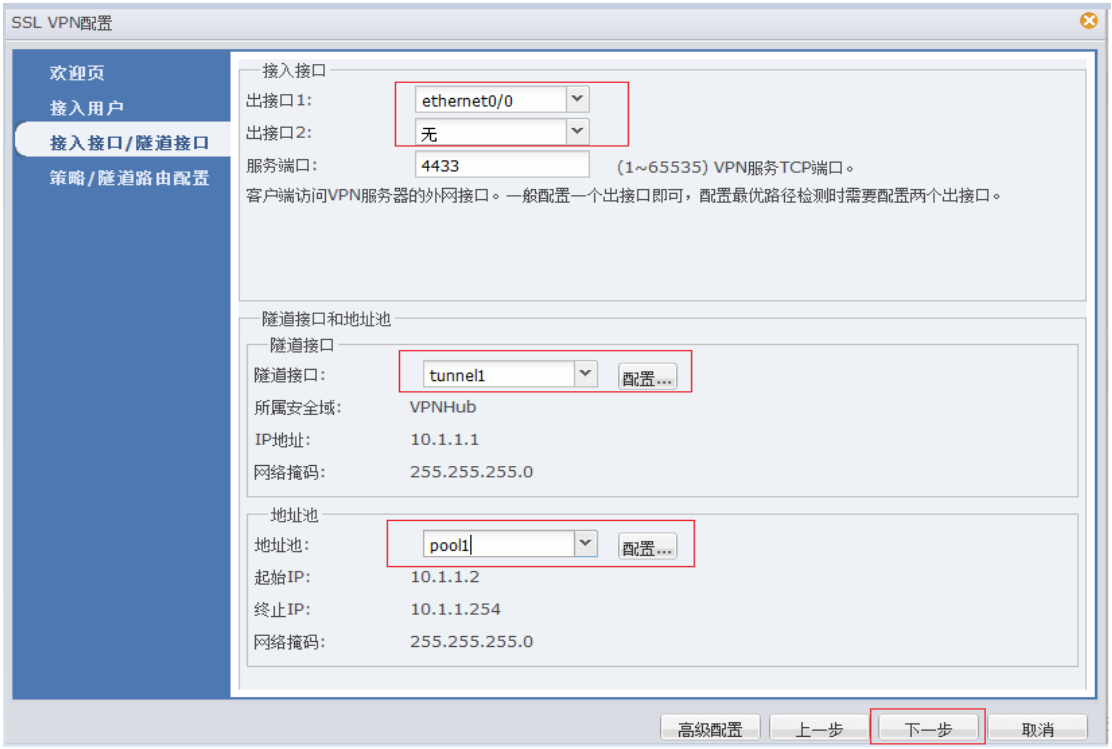


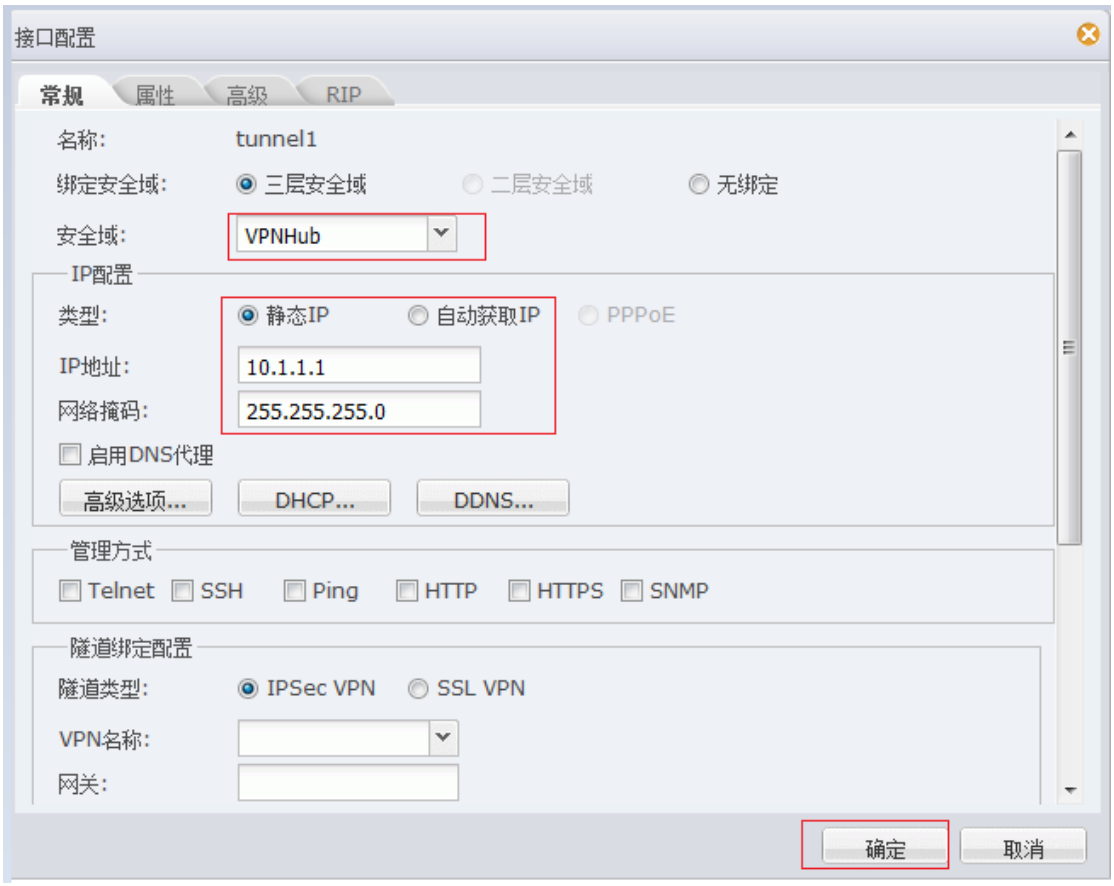
2．新建 SSL VPN 名称，点击下一步：

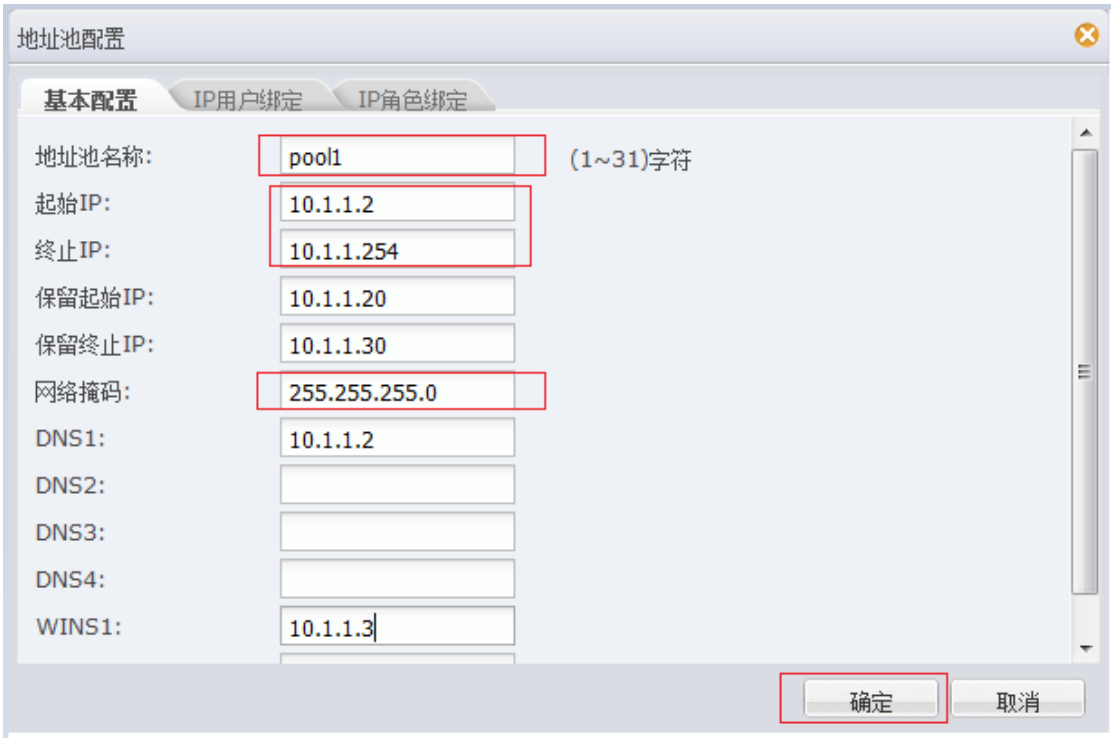
3．新建拨入用户，添加 AAA 服务器，AAA 服务器中需要创建登陆 SSL VPN 的用户名和密码：



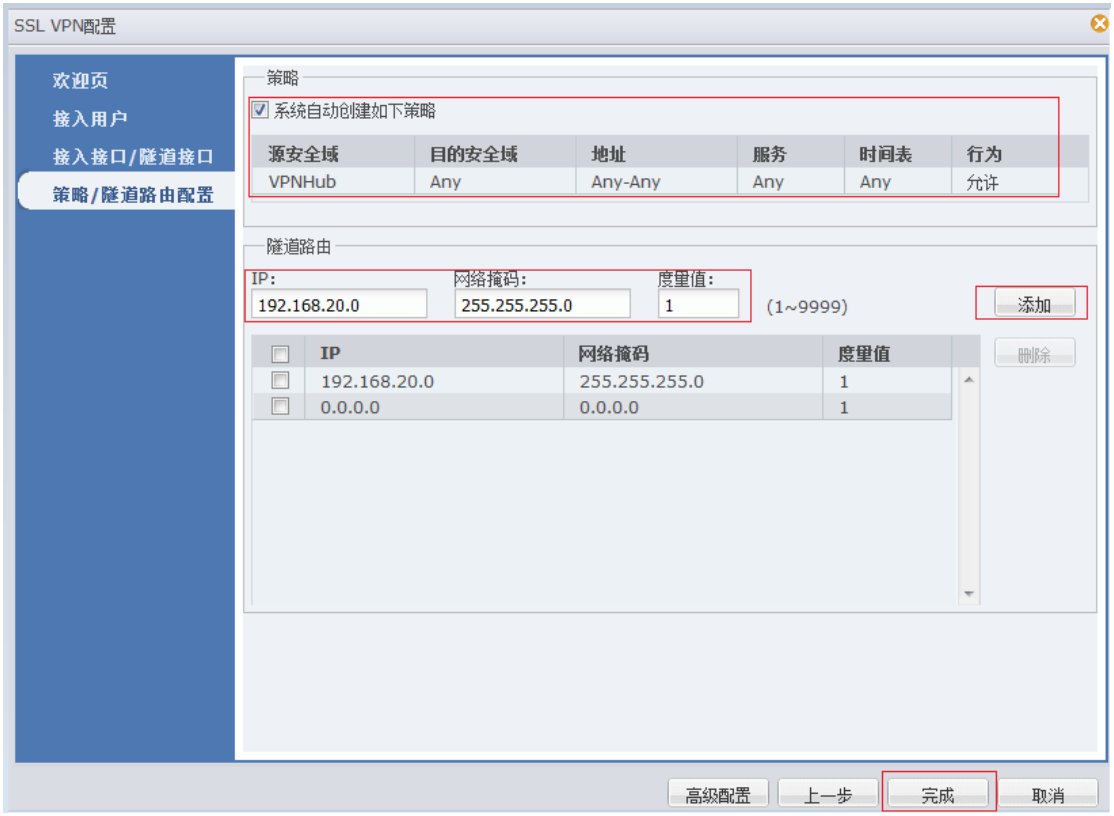
4．接入接口选择，配置隧道接口和地址池，隧道接口地址和地址池须在同一网段，且地址池地址段中不能包含隧道接口地址：




接口配置
常规
属性
高级
RIP
名称:
tunnel1
绑定安全域:
三层安全域
二层安全域
无绑定
安全域:
VPNHub
IP配置
类型:
静态IP
自动获取IP
PPPoE
IP地址:
10.1.1.1
网络掩码:
255.255.255.0
启用DNS代理
高级选项...
DHCP...
DDNS...
管理方式
Telnet
SSH
Ping
HTTP
HTTPS
SNMP
隧道绑定配置
隧道类型:
IPSec VPN
SSL VPN
VPN名称:
网关:
确定
取消


地址池配置
基本配置
IP用户绑定
IP角色绑定
地址池名称:
pool1
(1~31)字符
起始IP:
10.1.1.2
终止IP:
10.1.1.254
保留起始IP:
10.1.1.20
保留终止IP:
10.1.1.30
网络掩码:
255.255.255.0
DNS1:
10.1.1.2
DNS2:
DNS3:
DNS4:
WINS1:
10.1.1.3
确定
取消

5．配置策略和隧道路由，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：

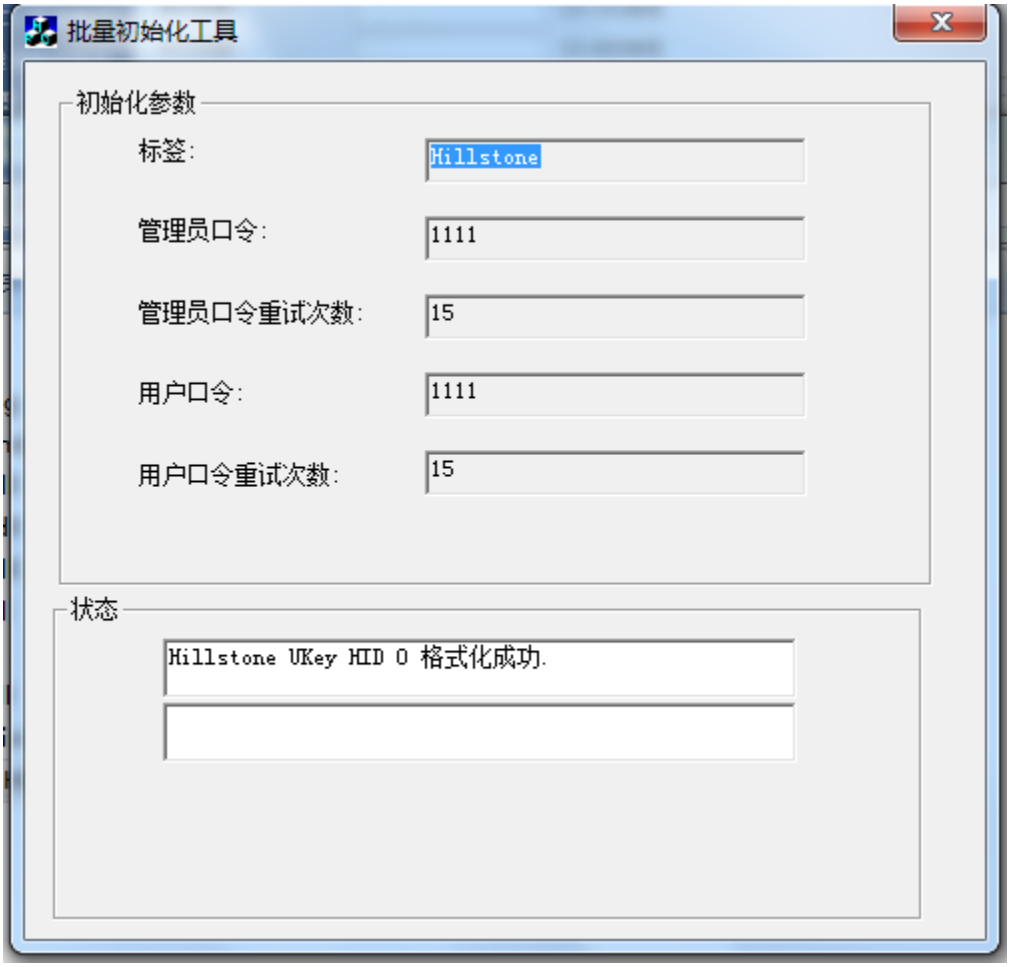


6．高级配置（可选），参数配置保持默认即可：

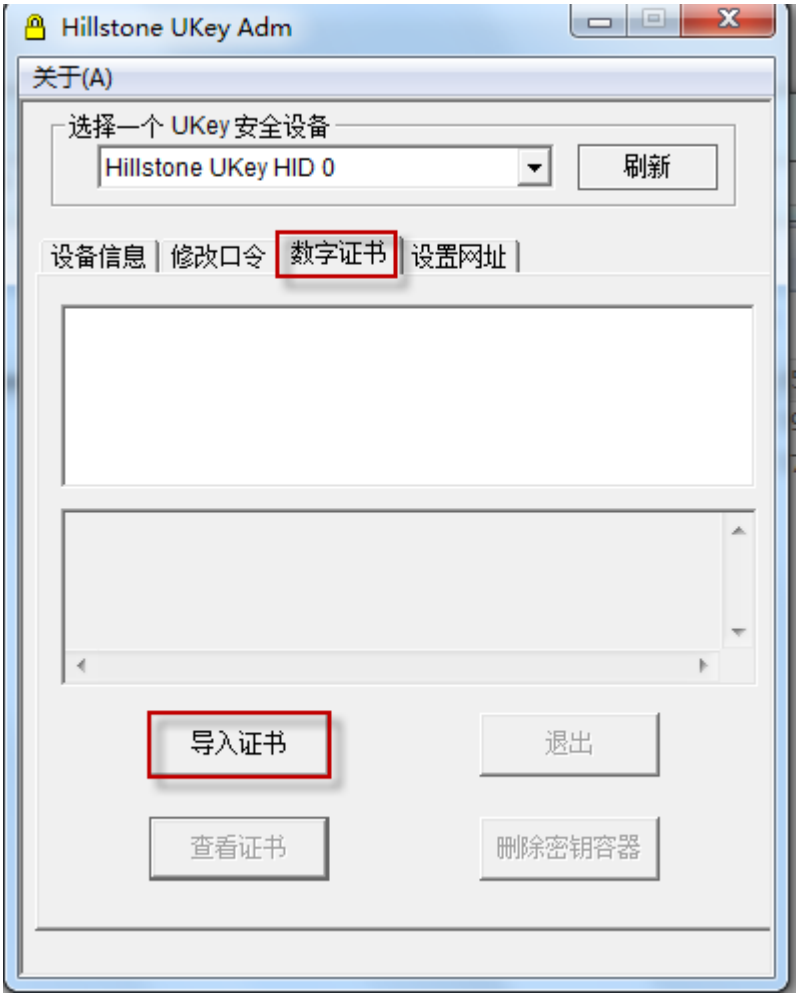
7．启用 USB Key 证书认证，选择客户端证书认证的方法，包括“用户名/密码+USB Key”和“只用 USB Key”两种，添加之前新建的信任域：

三． 制作 USB-KEY

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”，选择“数字证书”，“导入证书”，输入“保护口令（默认为 hillstone）”：


Hillstone UKey Adm
关于(A)
选择一个 UKey 安全设备
Hillstone UKey HID 0
刷新
设备信息
修改口令
数字证书
设置网址
导入证书
退出
查看证书
删除密钥容器

四. 使用 USB-KEY 认证方式登陆

1. 将 USB Key 插入 PC 的 USB 接口；

2. 在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。并在弹出的“请输入用户口令”中输入 UKey 的用户口令（默认为“1111”）：

4. 浏览器转到登录页面，输入用户名和密码，并点击“登录”。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. 使用 web 界面方式登陆成功后下载并安装 SSL VPN 客户端，选择登陆方式：

7. 输入服务器 ip，端口号，用户名，密码以及 pin 码：

4.2 PnP-VPN

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。

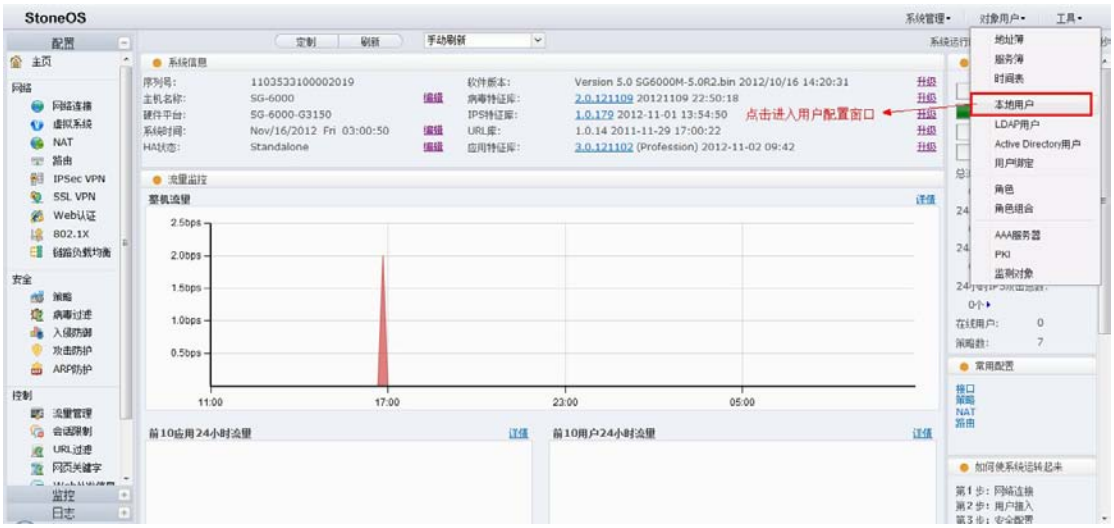
PnPVPN Client：通常放置于企业分支机构（如办事处），可由总部工程师远程维护，只需要做简单配置（如客户端ID、密码和服务器端IP 地址），和Server 端协商成功后即可从Server 端获取配置信息（如DNS、WINS、DHCP 地址池等）。

配置 pnp vpn 主要分为 3 个步骤：

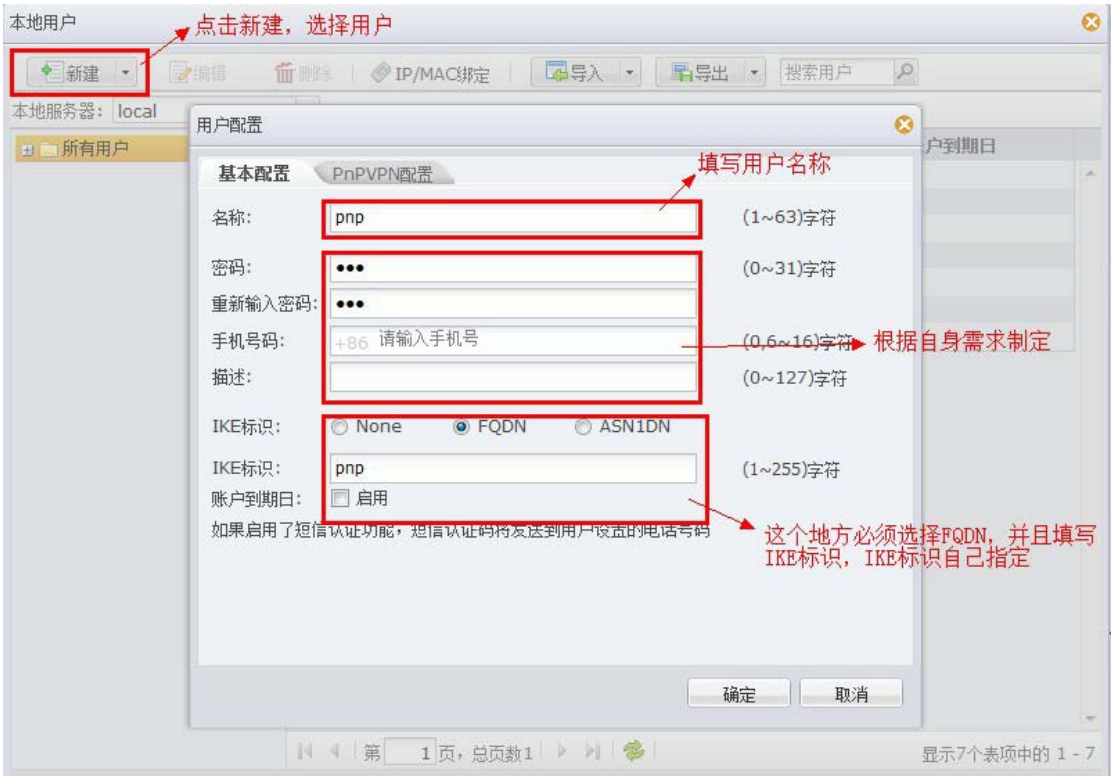
1. 配置用户
2. Server 端配置 IPSec VPN 实例
3. 客户端配置

一．配置用户

1．WEB 管理页面>>点击右上角的“对象用户”>>本地用户：



2．点击“本地用户”进入用户配置窗口：



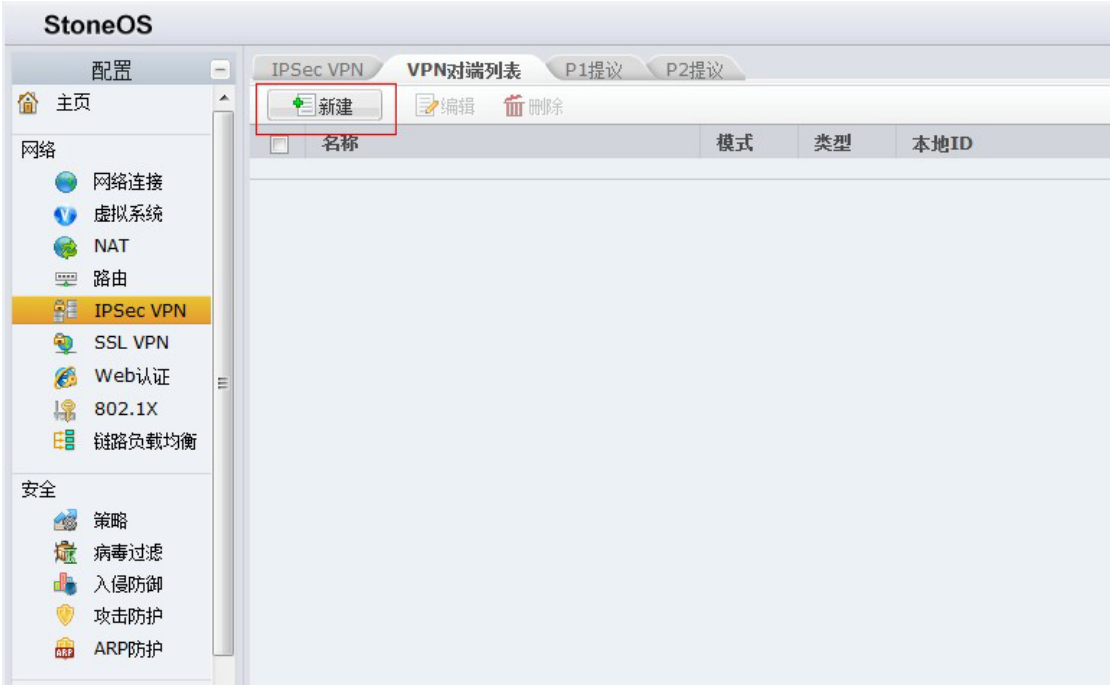
3．按照上图配置完基础配置之后，先不要点确定关闭窗口，选择“PnPVPN 配置”标签：

此时，用于给客户端登陆的用户信息已经设定完成。如果有多个分支客户端可重复上述步骤。

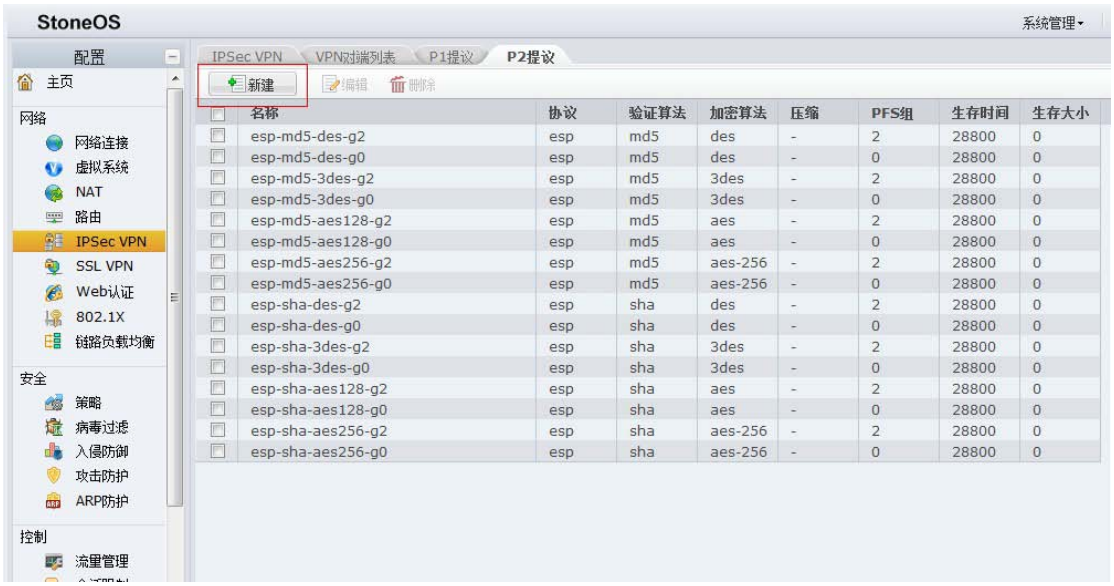
二．配置 IPSec VPN 实例（本配置只需在服务器端配置）

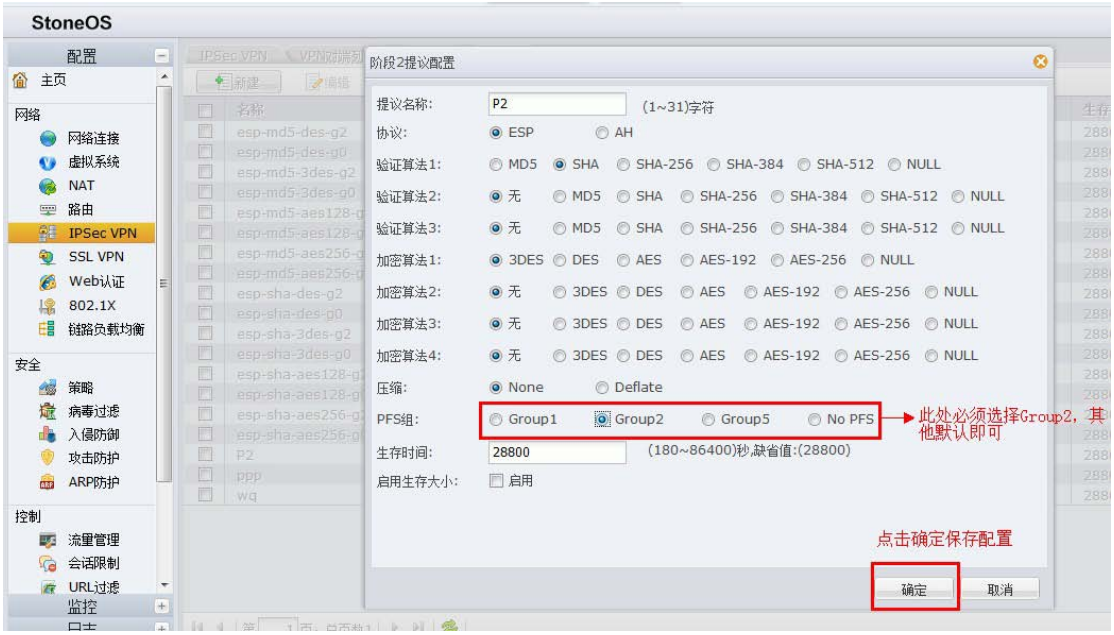
1．配置>>网络>>IPSec VPN>>P1 提议>>新建：

2. 配置>>网络>>IPSec VPN>>VPN 对端列表>>新建：

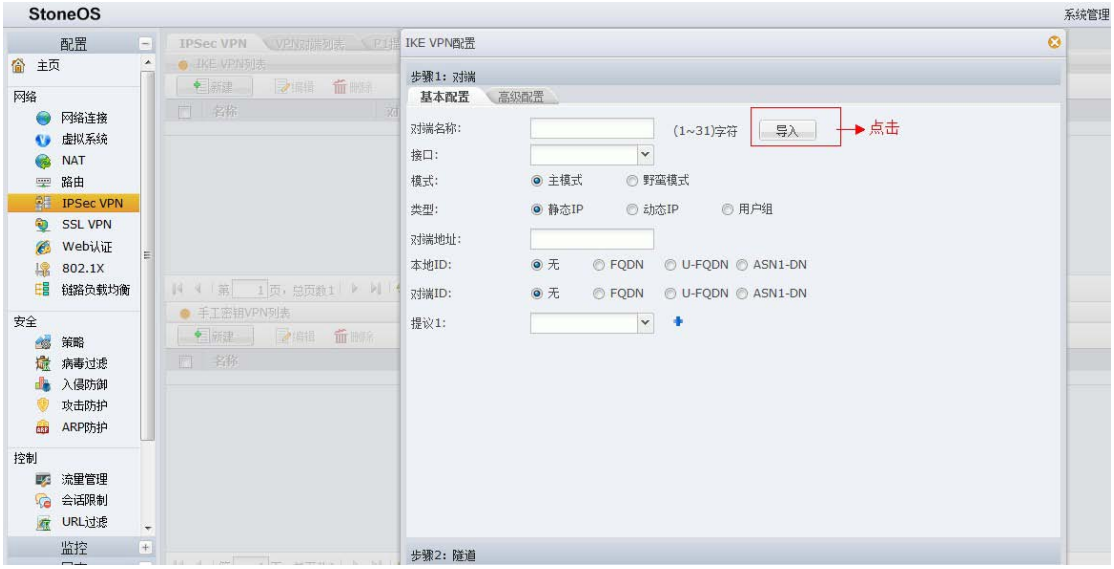


3. 配置>>网络>>IPSec VPN>>P2 提议>>新建：

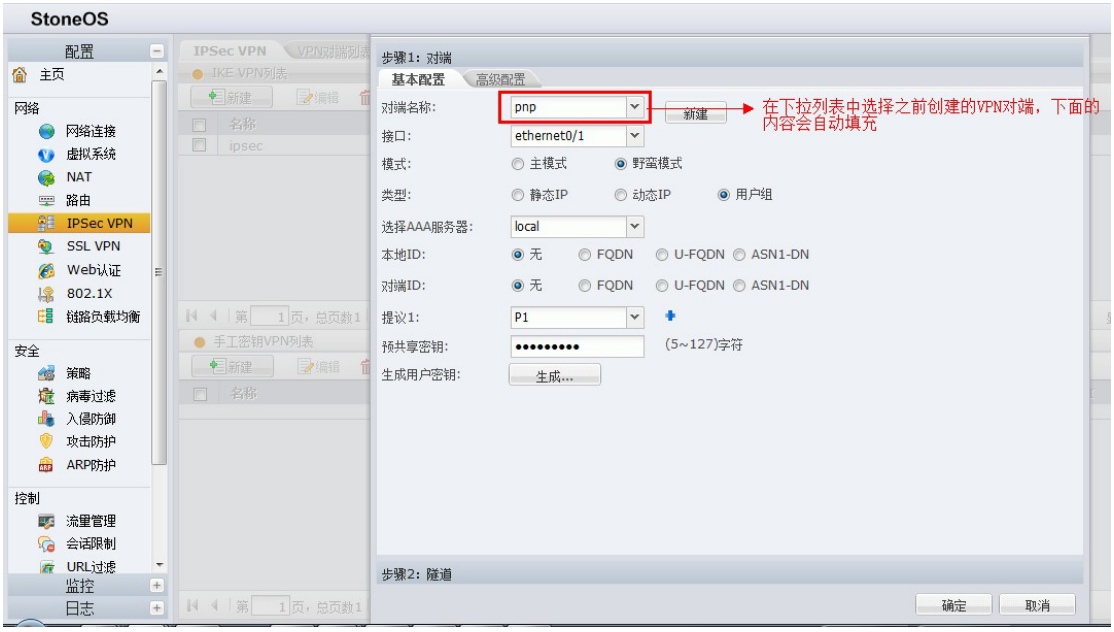




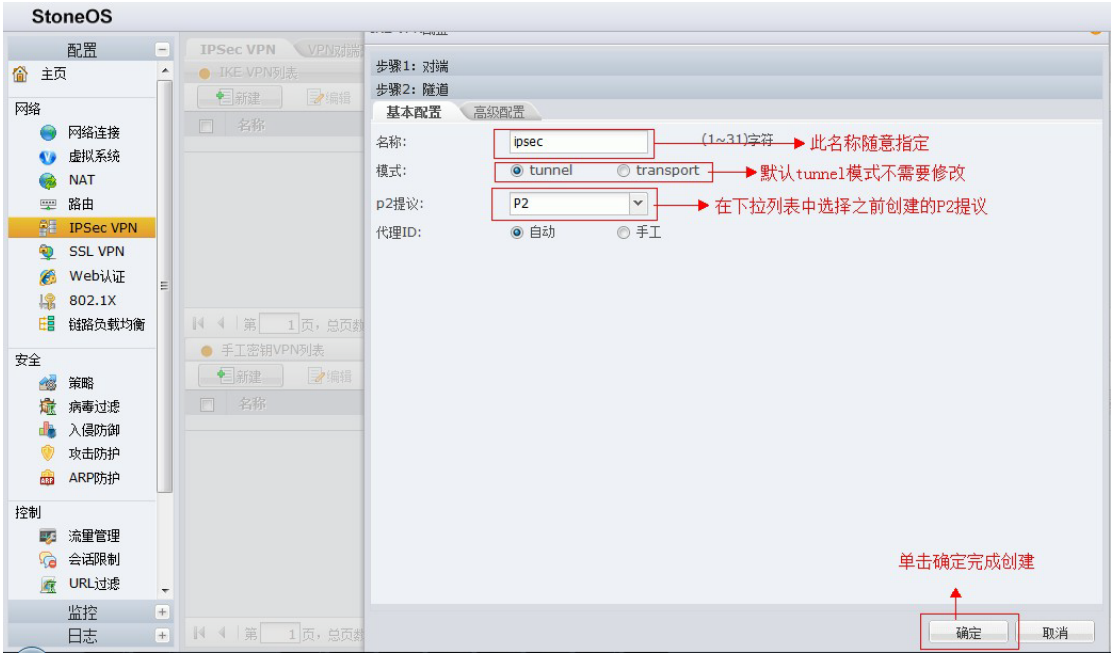
4. 配置>>网络>>IPSec VPN>>IPSec VPN>>新建：



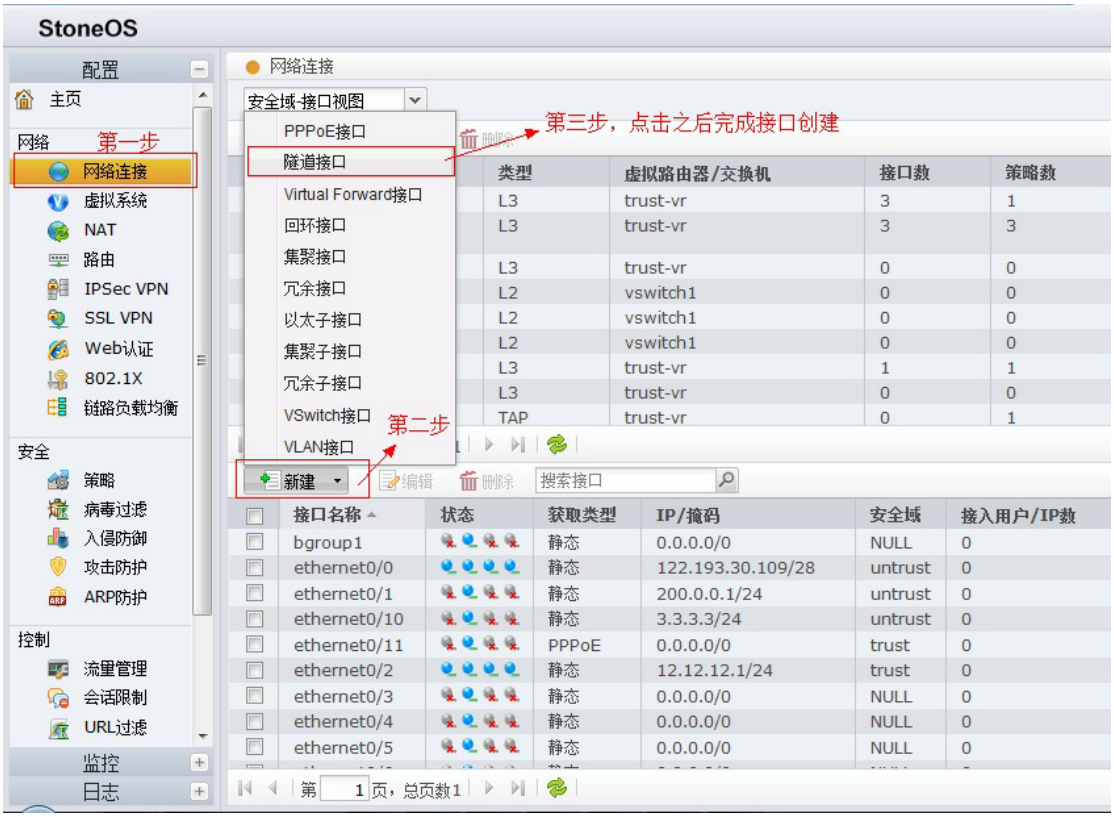
5．点击导入后，在对端名称的下拉列表中选择之前创建的“VPN 对端列表”后，下面的内容会自动填充，如图所示：



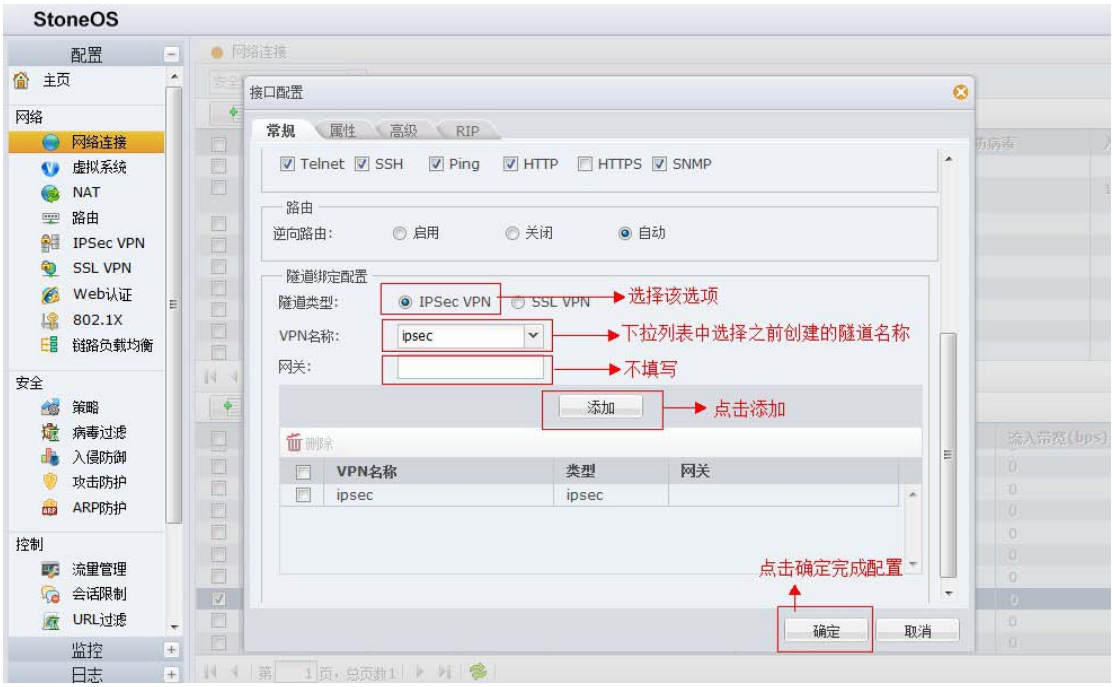
6．点击“步骤二：隧道”：



7．点击确定完成后，IPSEC VPN 实例已经创建完成，下面需要将实例绑定到 tunnel 接口，点击配置>>网络>>网络连接，在下面的接口列表中点击“新建”，选择“隧道接口”：

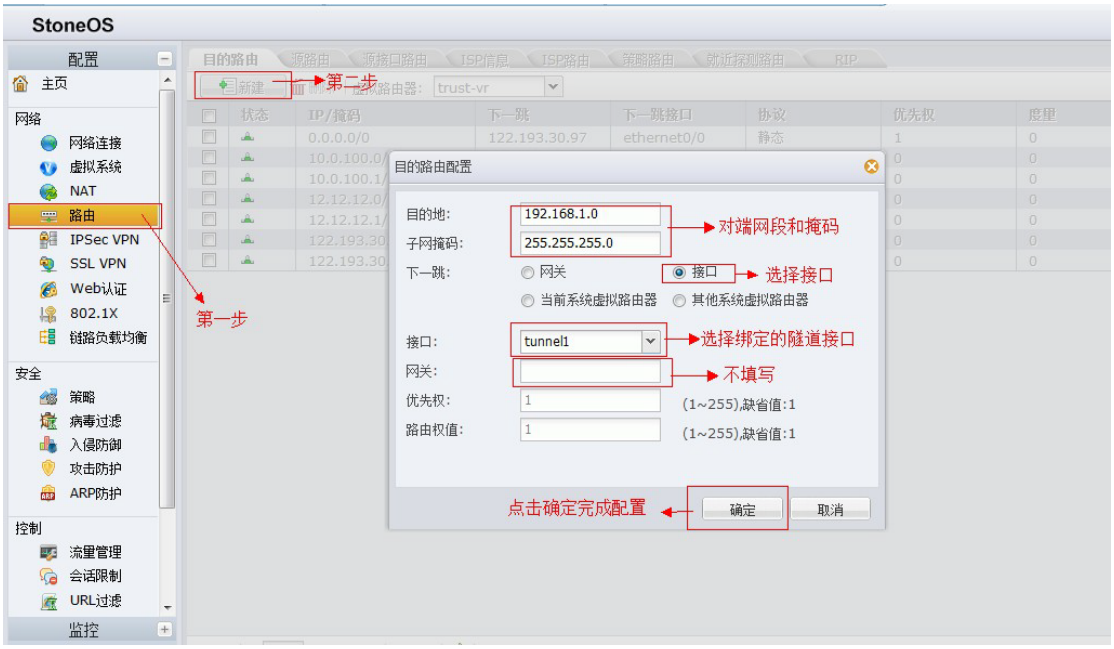


8. 接口创建完成之后，进入该 tunnel 接口，配置隧道绑定，如图所示在 tunnel 接口配置框中：

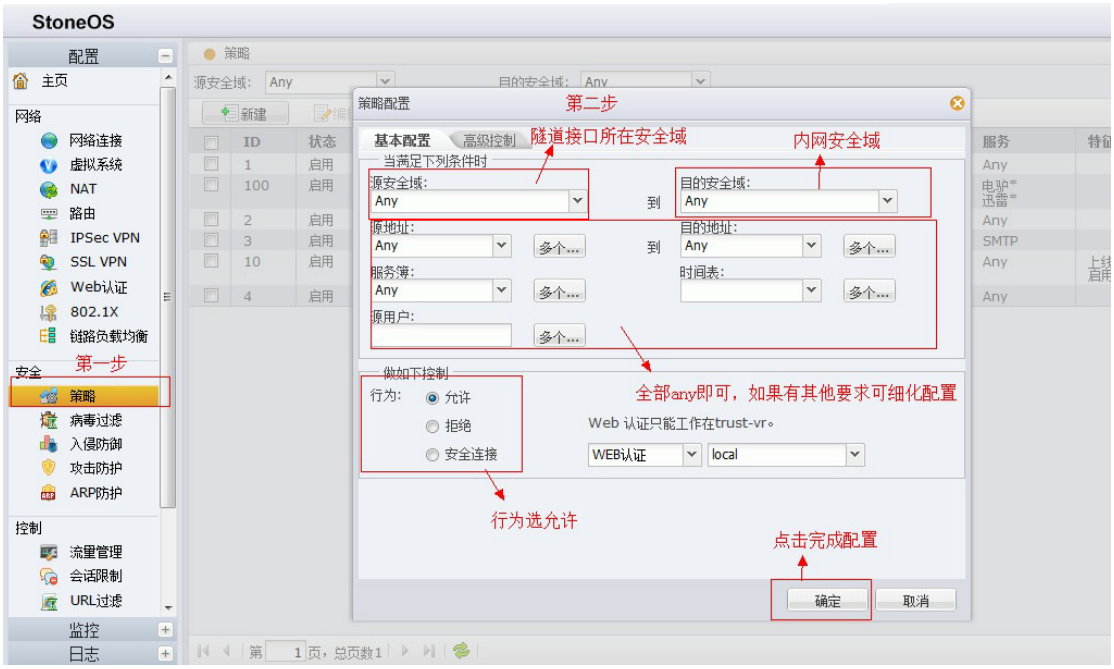


9. 接下来需要配置 server 端的路由和策略：

路由配置：



策略配置：



至此，server 端已经配置完成，只需要在 cliect 端设备上填写几个简单参数即可与 server 端建立 IPSec vpn。

三．PnP 客户端配置：

1．将客户端防火墙接入互联网，配置外网 ip 以及默认路由；

2．配置>>网络>>IPSec VPN>>任务>>PnPVPN 客户端：

点击确定后，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。

五．高可靠性 HA 配置

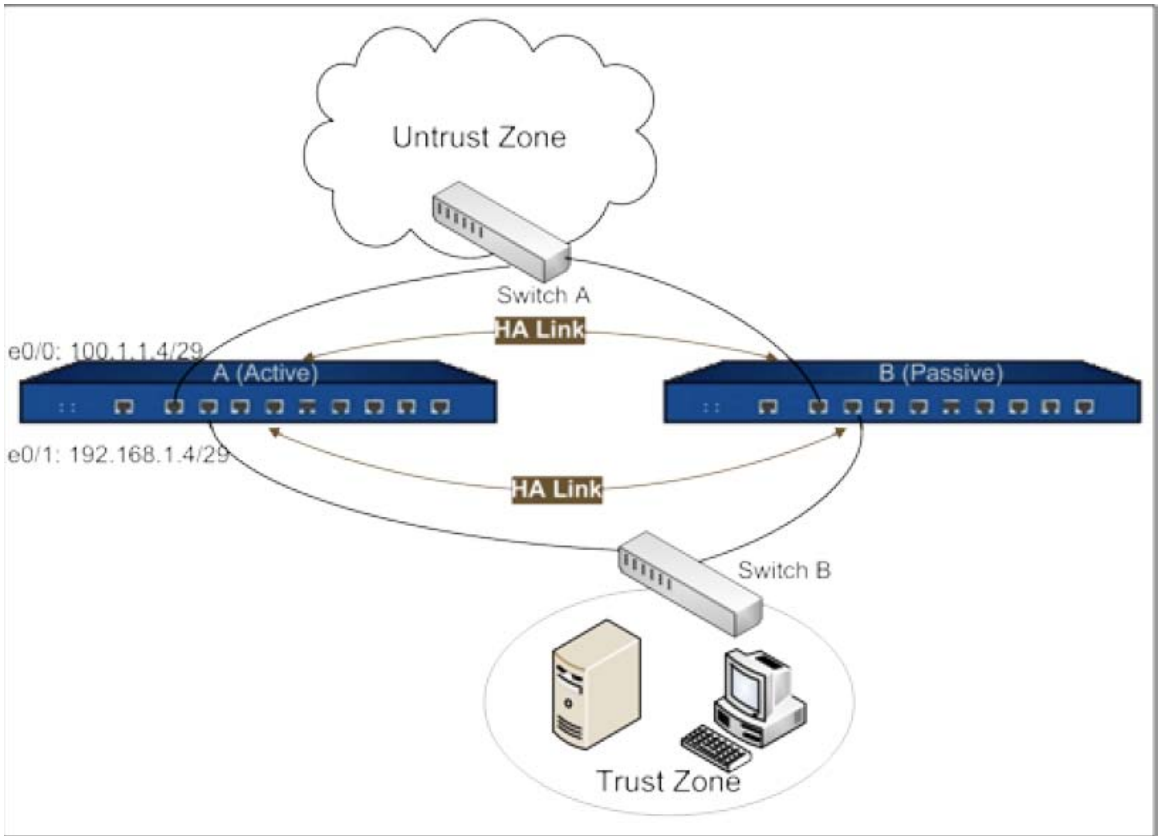
1．配置 HA 所需要具备的条件：

本节介绍如何将两台设备配置为HA A/A 冗余模式。在配置之前，确认搭建成HA 典型组网模式的两台安全网关采用完全相同的硬件平台、固件版本，均启用VR及防病毒、IPS功能，安装防病毒、IPS许可证，并且两台设备使用同样的接口连接到网络。

2．HA 的两种模式介绍

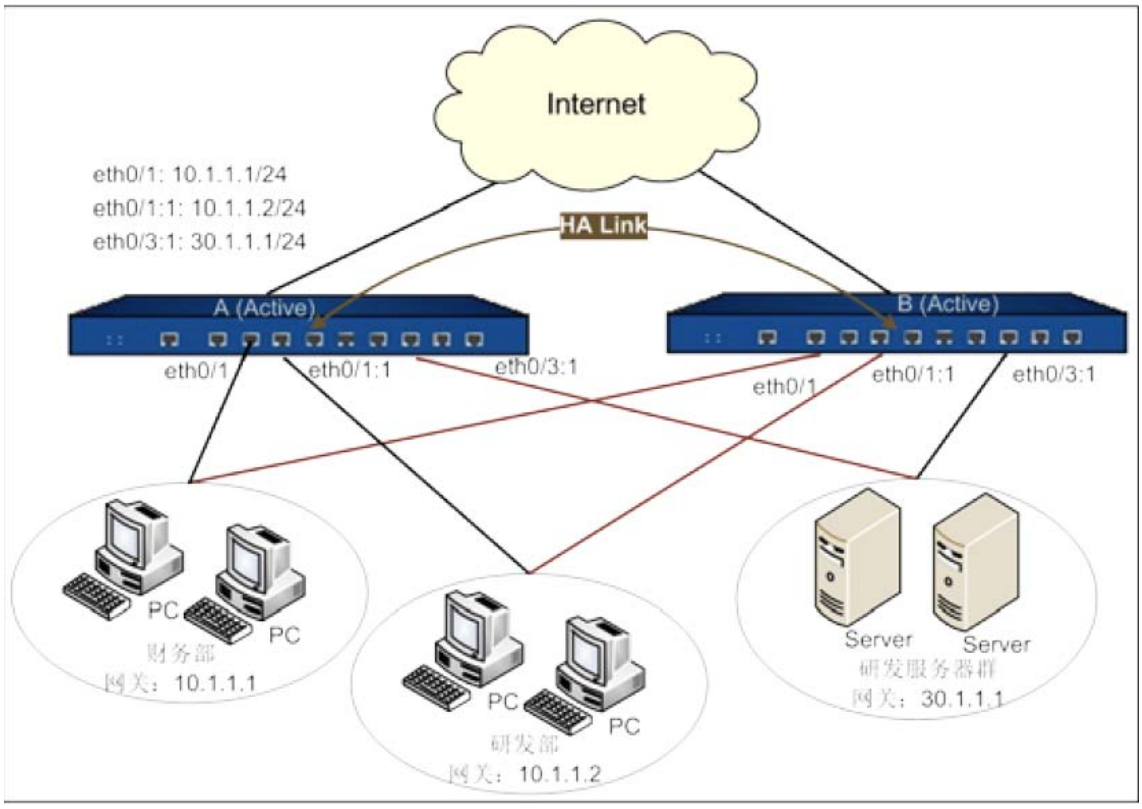
AP 模式：

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：



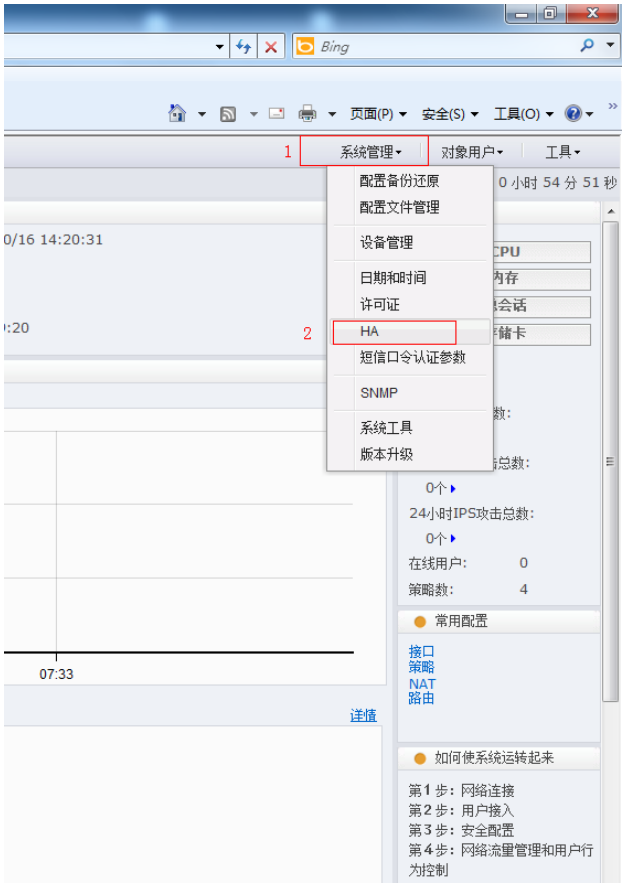
AA模式：

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：

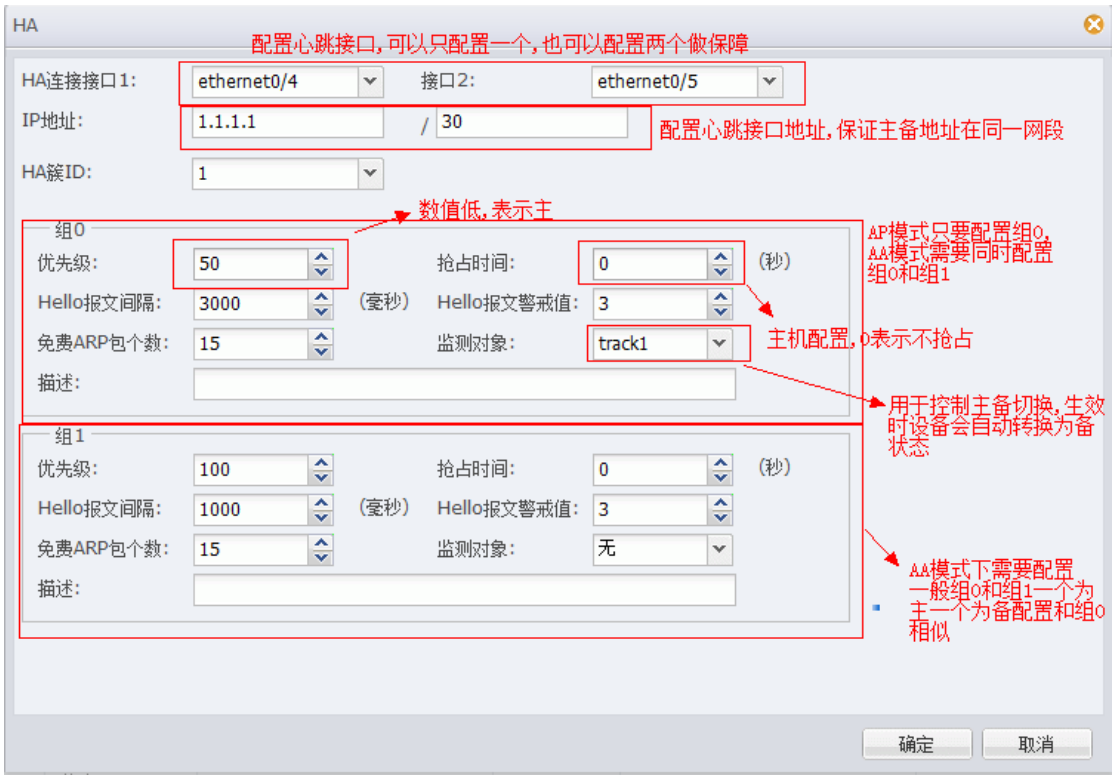


3. HA 的配置方式：

1. 点击系统管理中的 HA 按钮，进入 HA 配置界面：



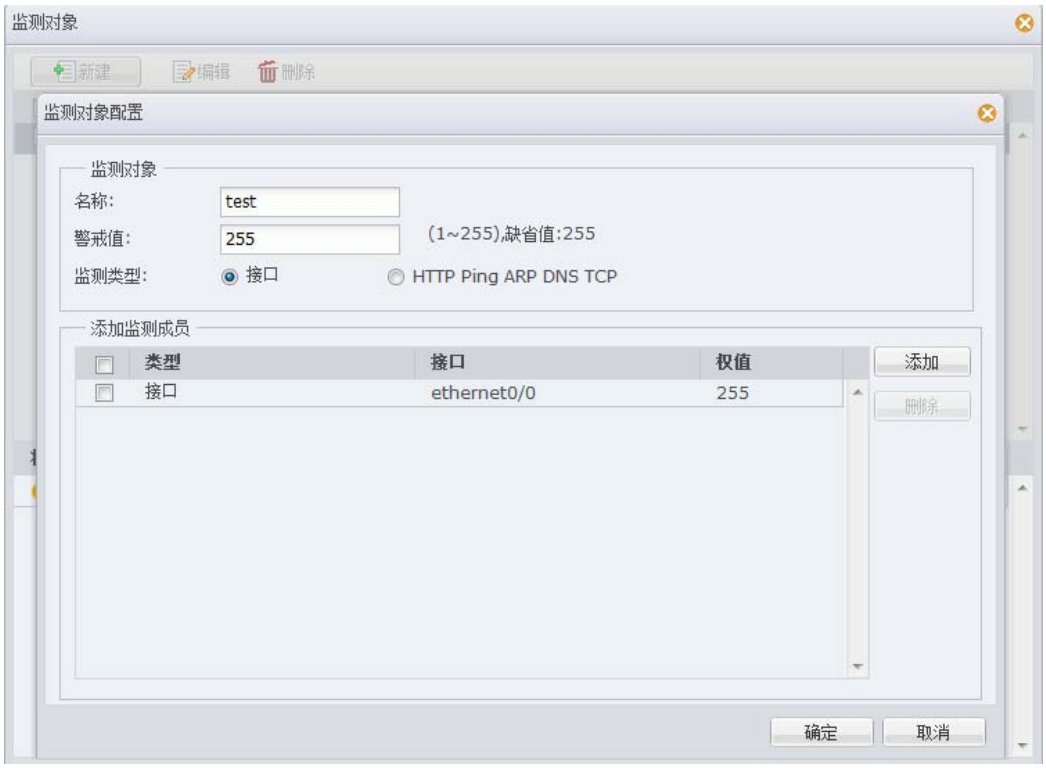
2. 配置心跳接口，和心跳接口地址，HA 簇 ID 选 1，优先级数值小表示主机，数值大表示备机，抢占时间只有主机需要配置（0 表示不抢占），配置检测对象来控制主备的切换，当监测对象生效时，设备自动变成备机：

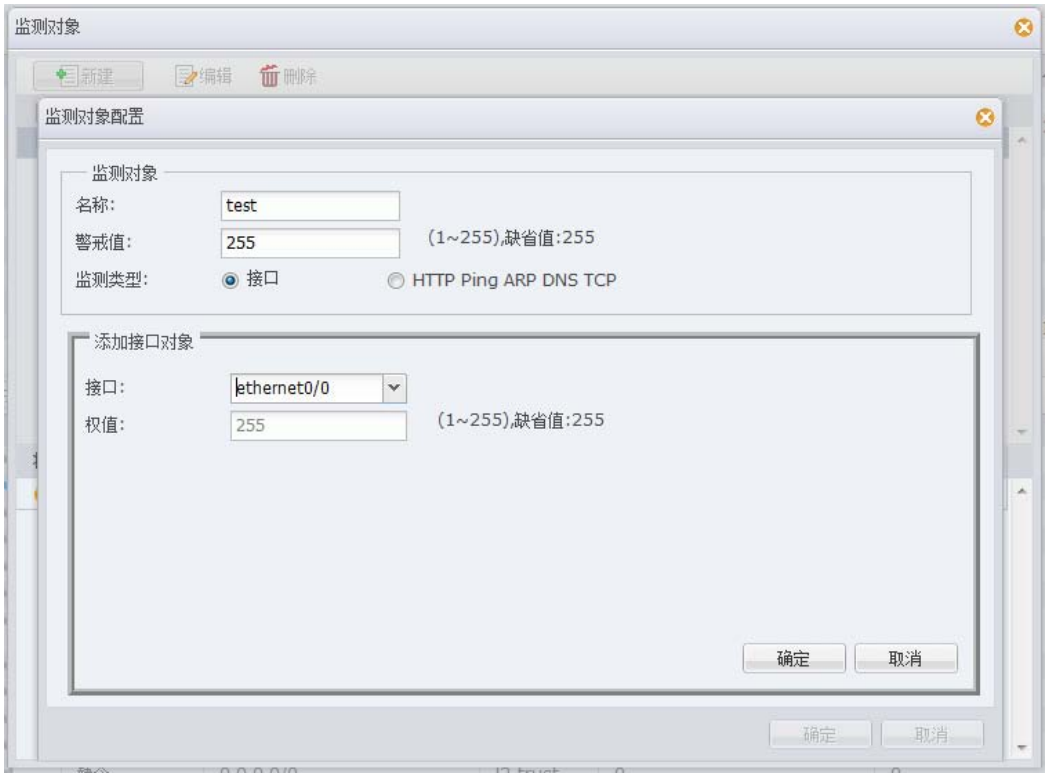


3. 配置检测对象

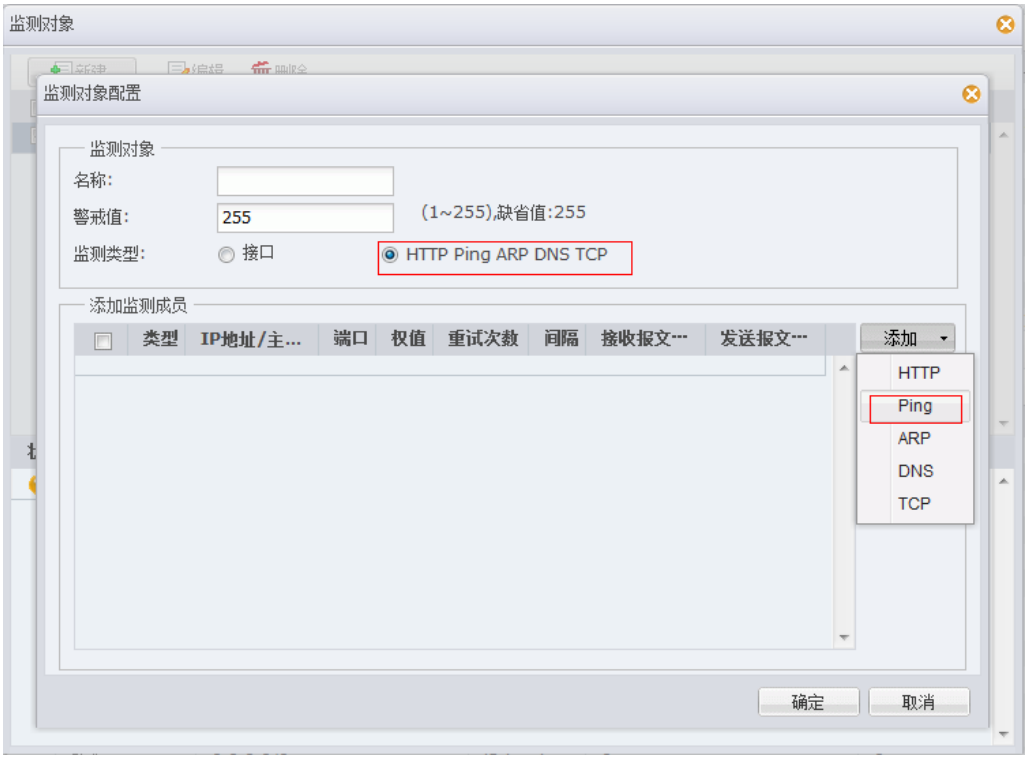
点击对象用户中的监测对象按钮，进入配置界面：

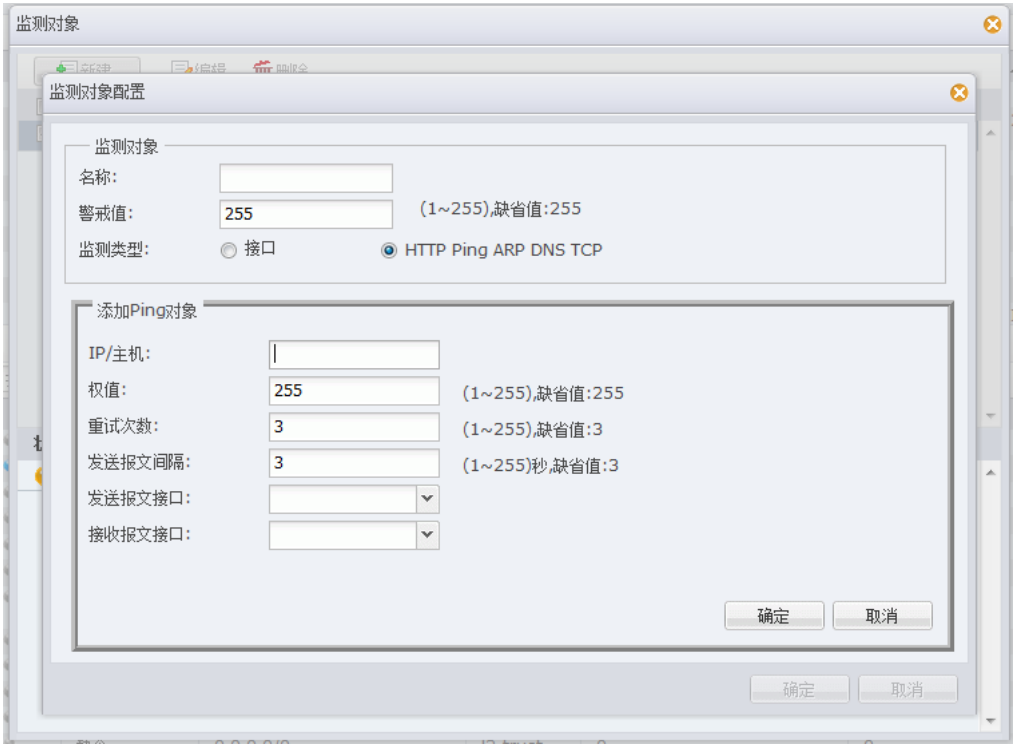
监测接口的物理状态，可以添加多个接口，每个接口有一个权值，该数值表示该接口 DOWN 后将释放的数值，当所有释放的权值累计数值大于等于警戒值的时候，该检测对象就生效，权值和警戒值都可以自行调整：





监测链路逻辑状态，可以配置多种形式的探测，这里用 ping 举例，单机添加，Ping，名字自取，如图配置中，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：

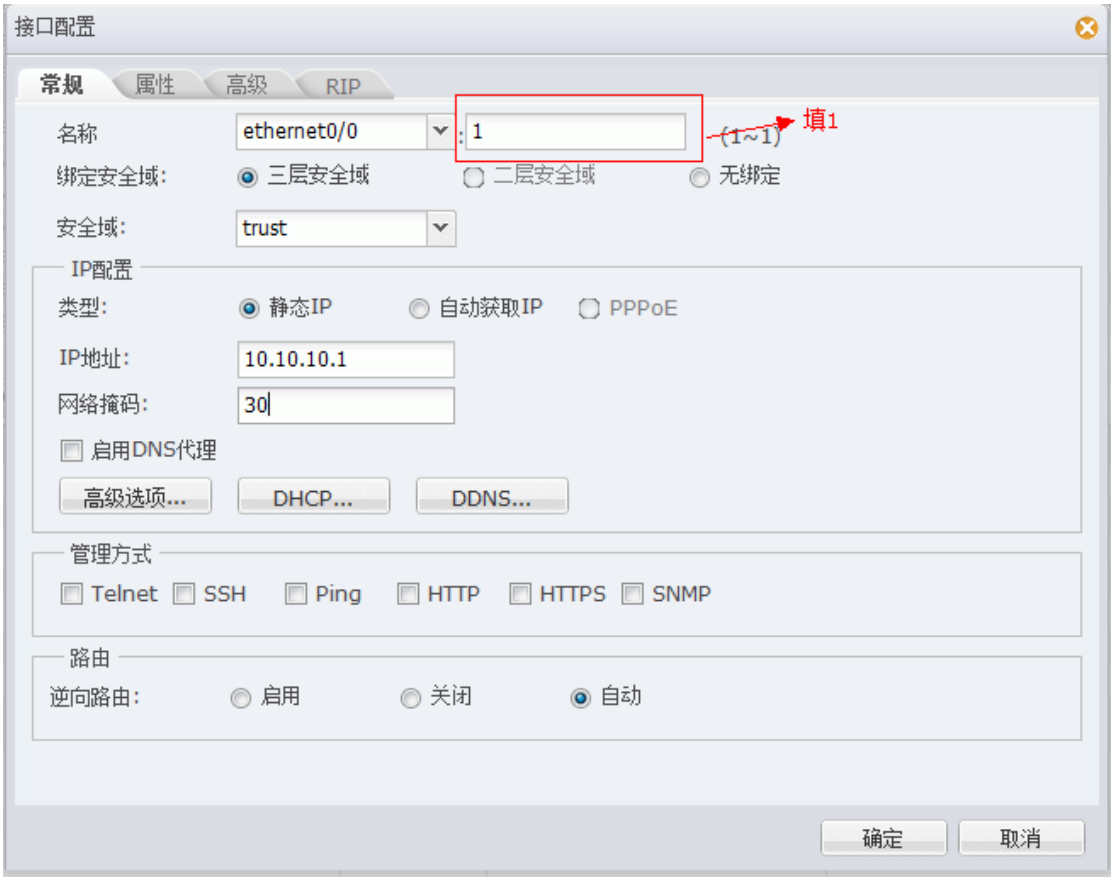




4. 配置接口

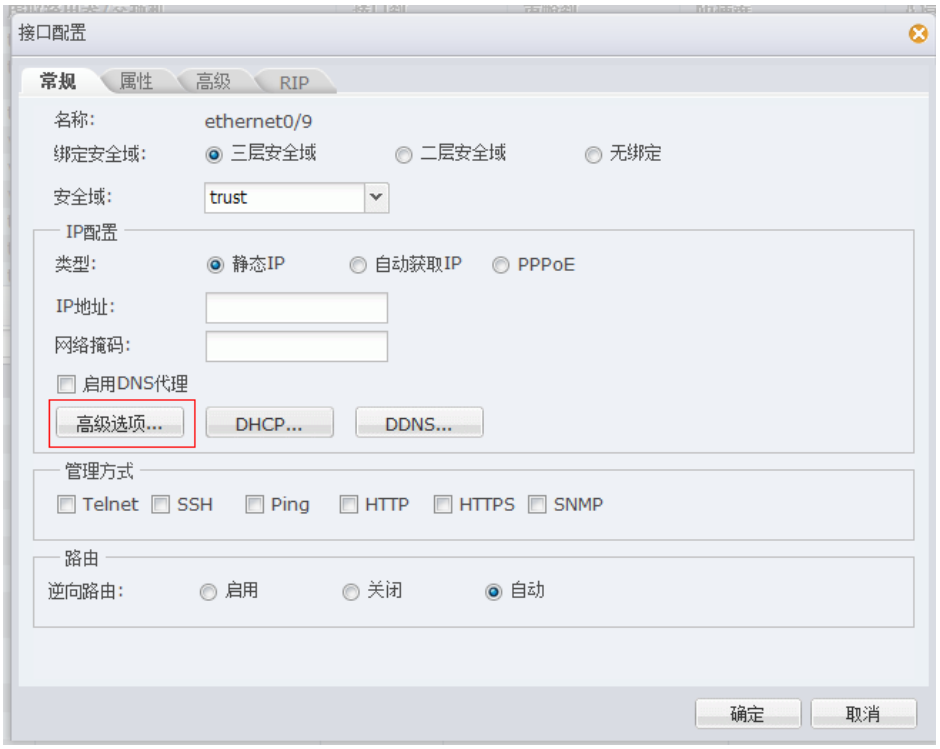
在 AP 模式下，配置方式和普通上网一致，直接在接口上进行配置即可。

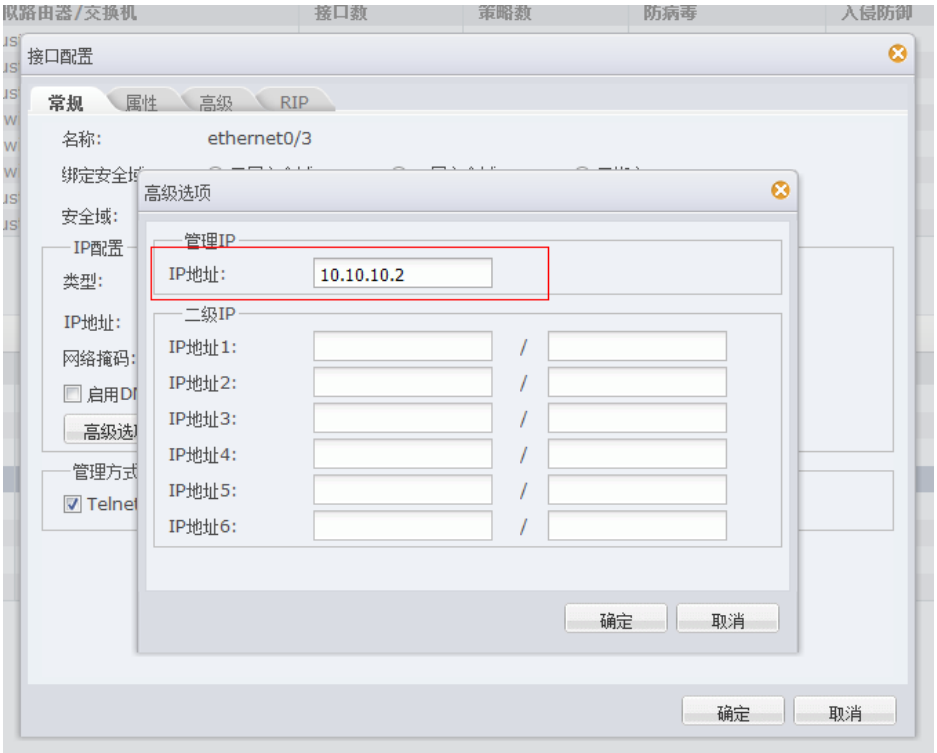
在 AA 模式下，组 0 正常配置，组 1 需要配置 VF 接口，如下：



5. 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,配置如下:





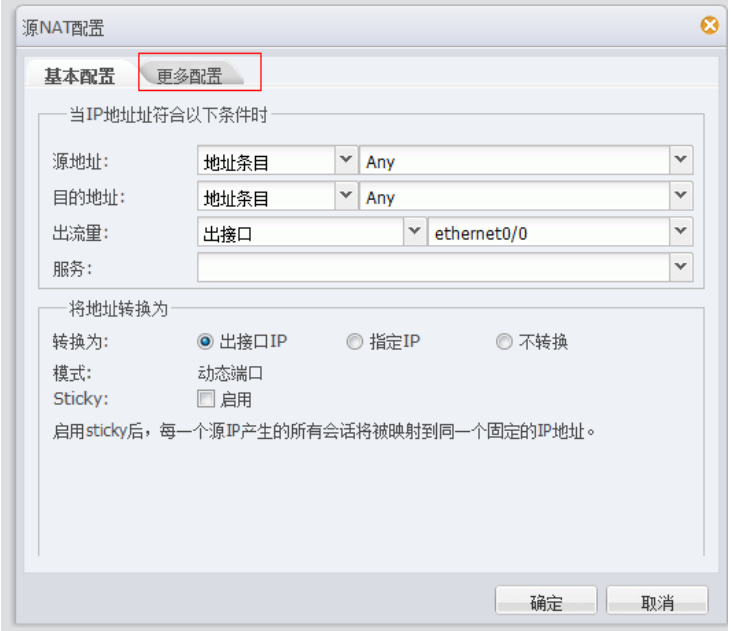
管理 IP 可以和接口 IP 在同一网段,也可以是单独的 IP,只需路由可达即可。

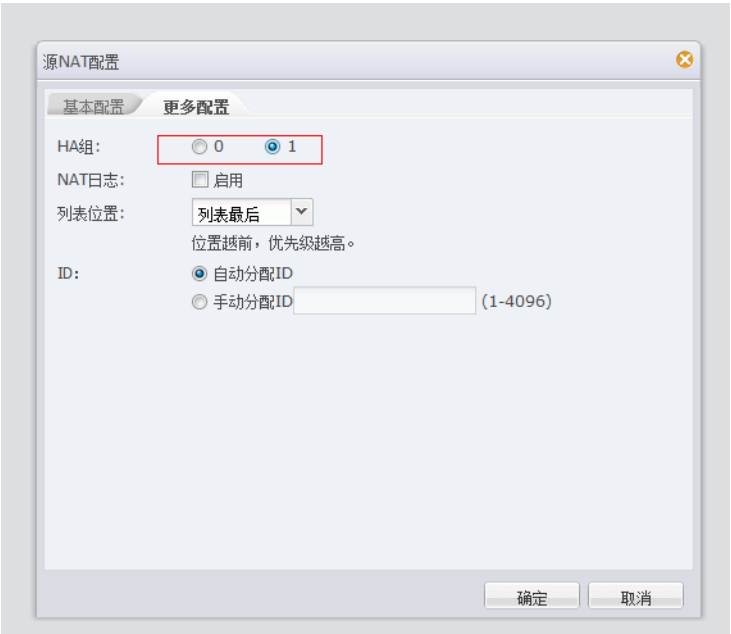
6. 配置 NAT

AP 模式下，配置 NAT 和普通配置一致，直接配置即可。

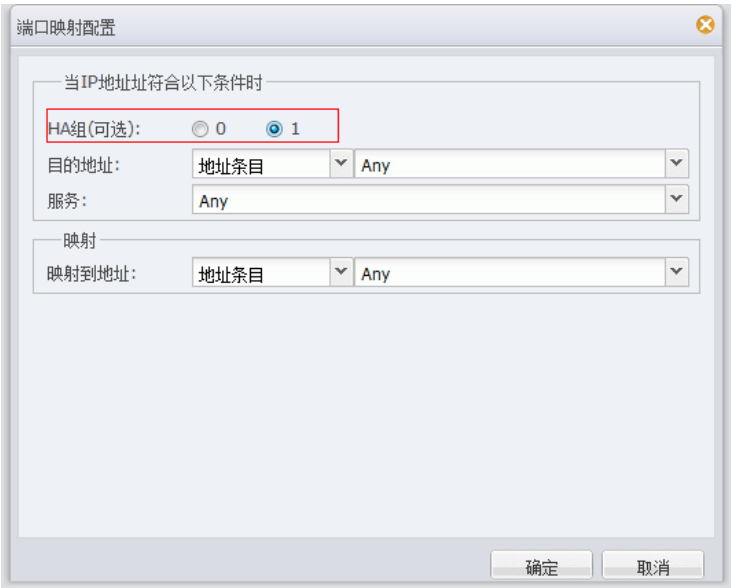
AA 模式下，组 0 配置 NAT 和普通配置一致，直接配置即可，组 1 配置 NAT 是需要选择组 1，如下：

SNAT：





DNAT:



7. 正常配置路由以及策略,确保网络的通畅。