### 12.

**为实现对防火墙的安全管理，在防火墙 DCFW 的 Trust 安全域开启 PING,HTTP，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能;**

在对应的接口处进行配置就行了，记得打勾截图：



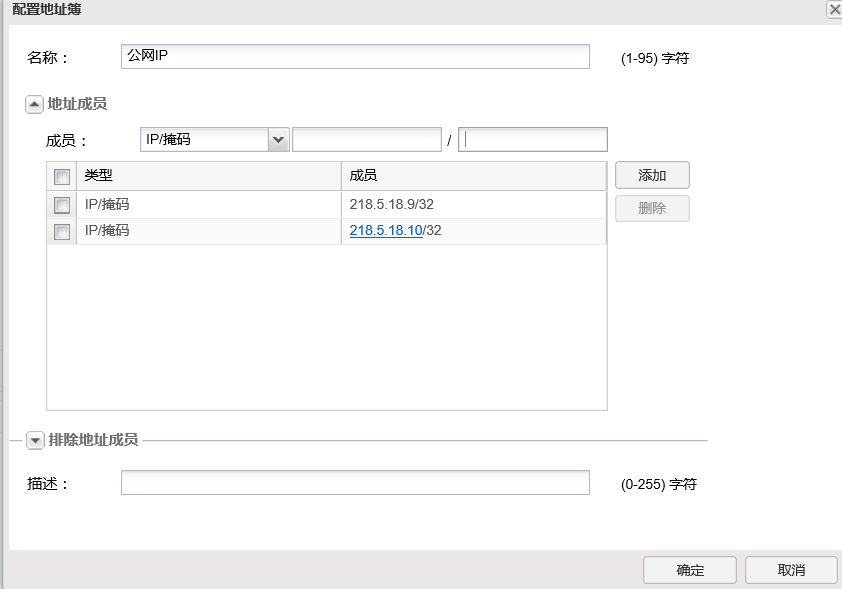




### 13.

**总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP：218.5.18.9、218.5.18.10；**

复用IP，也就是说，内网根据这两个IP进行映射，那我们首先应该去创建地址薄。



我们做了多条汇聚子接口，所以应该限制是哪些用户通过复用IP进行访问外网的，那么当然是我们配置了外网IP的子接口咯。所以这里的出接口设置为aggregate1.50。

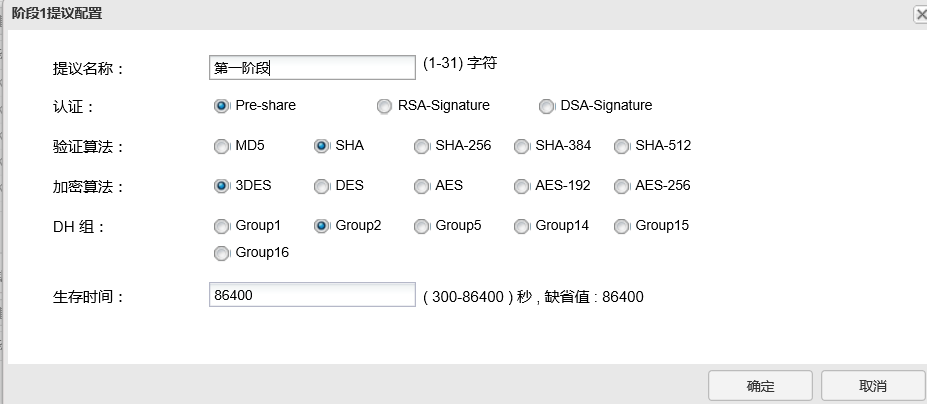
同时，应该指定NAT的转化条件，添加上我们创建的地址薄

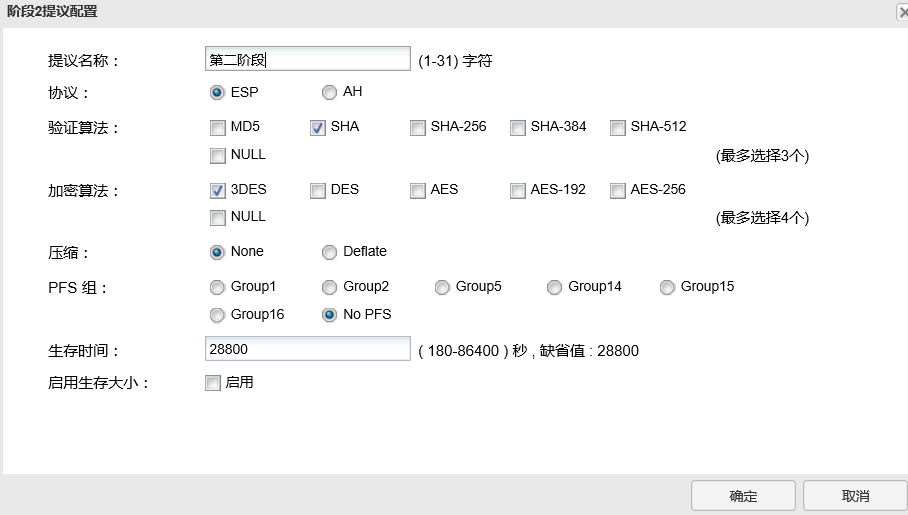


### 14.

**项目二期要启用云端路由器，需要在总部防火墙DCFW上完成以下预配：**  
**防火墙DCFW与云端路由器220.5.22.3建立GRE隧道，并使用IPSec保护GRE隧道，保证隧道两端2.2.2.2与VLAN20安全通信。**  
**第一阶段 采用pre-share认证 加密算法:3DES；**  
**第二阶段 采用ESP协议， 加密算法:3DES，预设共享秘钥 :DCN2014**

遇到加密认证的，大多数在VPN处，先配置认证算法：

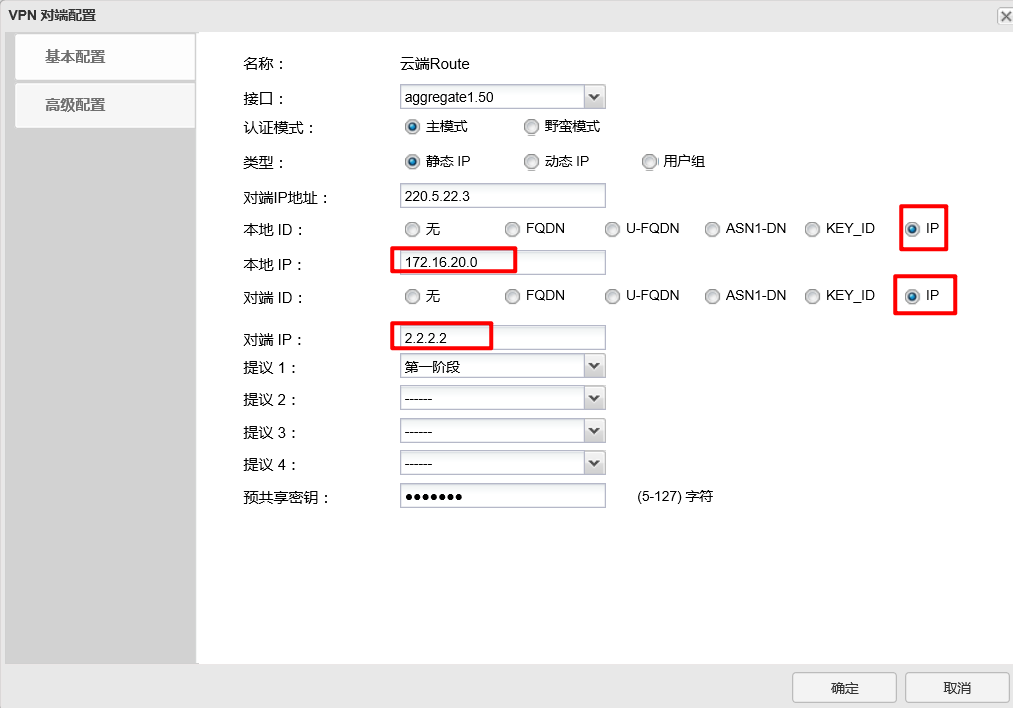




对于IPSec的配置，分为两端：一个是本端，另一个是对端

**“保证隧道两端2.2.2.2与VLAN20安全通信。”**

这就是对端ID了。记得勾选IP，同时提议1是在对端上面加的。



本端的配置，绑定对端，通知加上P2提议的加密算法



配置结果：



### 15.

**配置RIP完成云端路由器2.2.2.2、DCFW、总部核心交换机VLAN20的连通性，使用MD5认证，密钥为DCN2014；**

#### FW上面的配置：

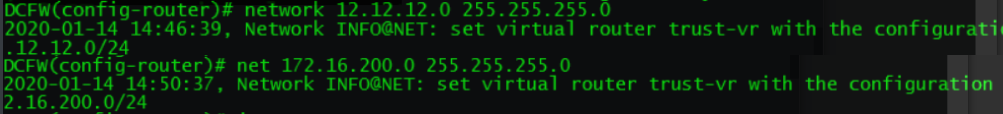
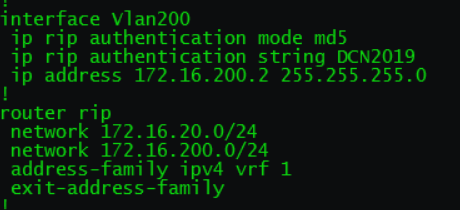


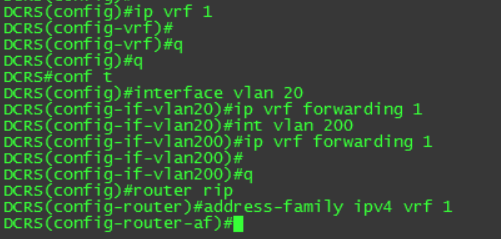
fig:  
fig:  
fig:

#### RS上面的配置：



### 16.

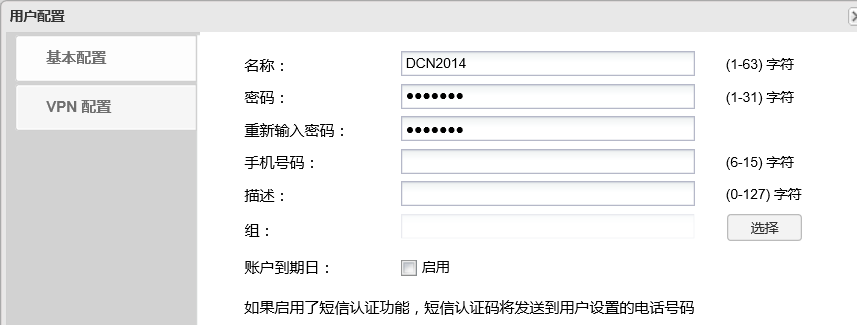
**总部核心交换机 DCRS 上使用某种技术，将 VLAN20 通过 RIP 连接云端路由器路由与本地其它用户访问 INTERNET 路由隔离；**



### 17.

**远程移动办公用户通过专线方式接入总部网络，在防火墙 DCFW 上配置，采用 SSL 方式实现仅允许对内网 VLAN 30 的访问，用户名密码均为 DCN2014，地址池参见地址表；**

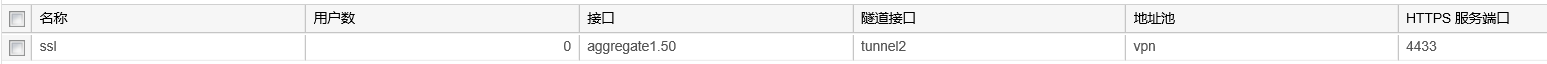
首先，去用户配置里面添加vlan30的用户





地址池就按照IP信息地址表配置，隧道接口、以及地址池（可自行分配）





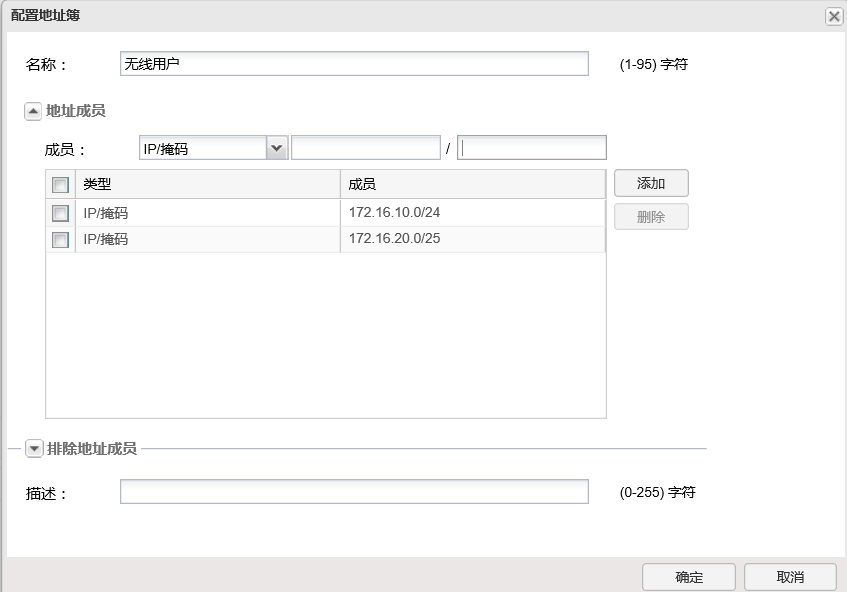
### 18.

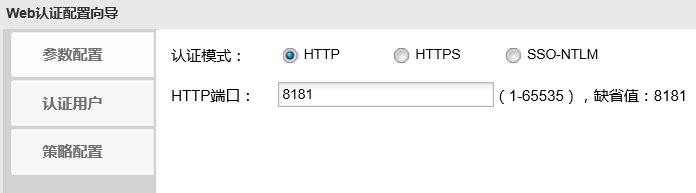
**出于安全考虑，无线用户移动性较强，无线用户访问 INTERNET 时需要采用认证，在防火墙上开启 WEB 认证，账号密码为Web2014;**

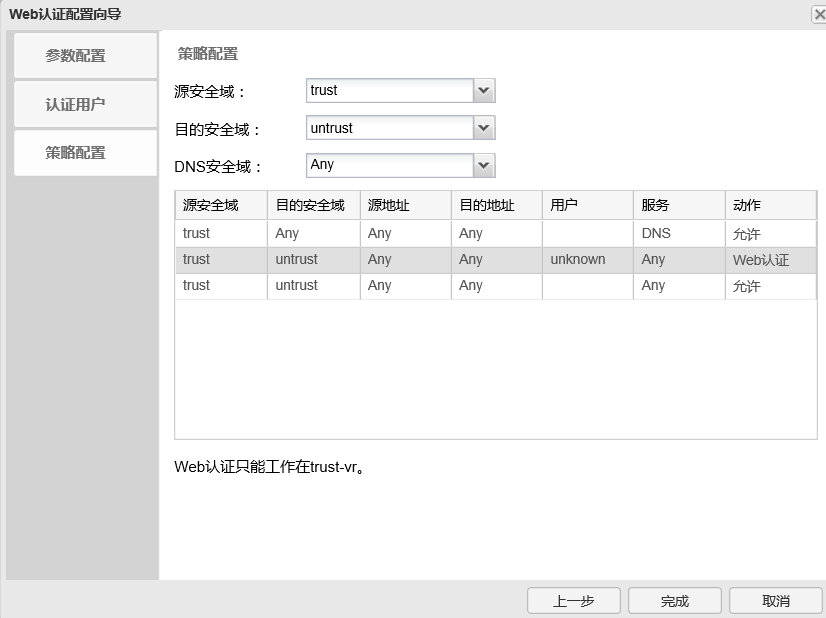
涉及到认证，还是要想到用户，于是要添加用户



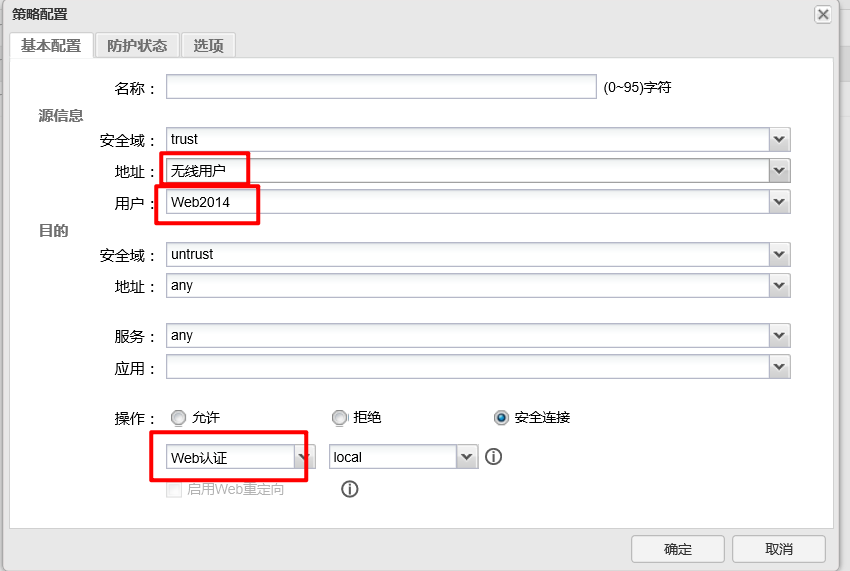
接着，配置地址薄，绑定无线用户的IP







然后，这里的用户限定是unknown，我们需要到策略里面将源信息中的用户配置为web2014，将地址改为地址薄中设置的无线用户。



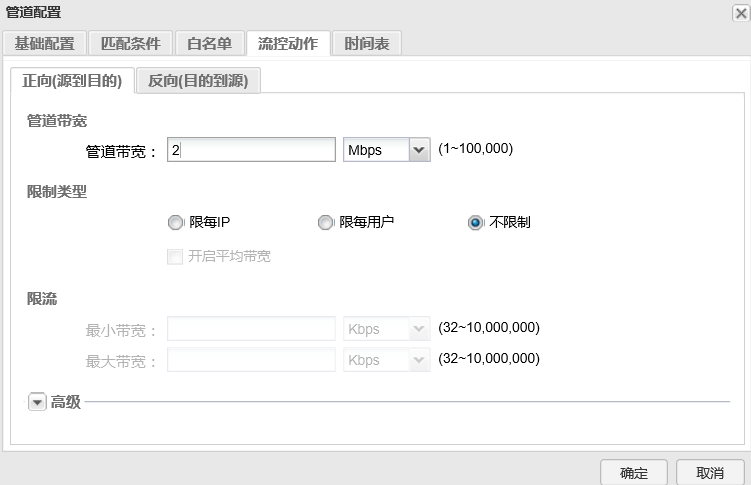


### 19.

**为了保证带宽的合理使用，通过流量管理功能将引流组应用数据流，上行最小带宽设置为 2M，下行最大带宽设置为 4M;**



上行也就是正向







### 20.

**为净化上网环境，要求在防火墙DCFW做相关配置，禁止无线用户周一至周五工作时间9：00-18：00的邮件内容中含有“病毒”、“赌博”的内容，且记录日志；**

添加时间表：





