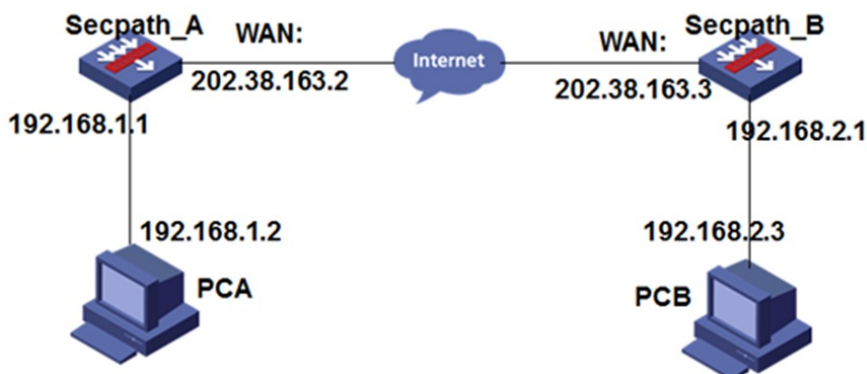


### 组网及说明

总公司与分公司都有公网地址，但不希望内网地址与数据包在公网上明文传输，因此建立IPsec VPN

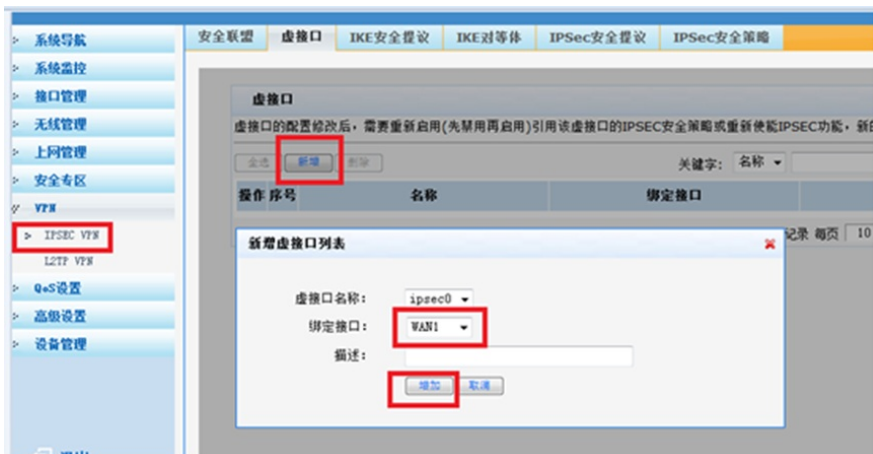


### 配置步骤

#### 1. 设置虚接口

VPN→VPN设置→虚接口

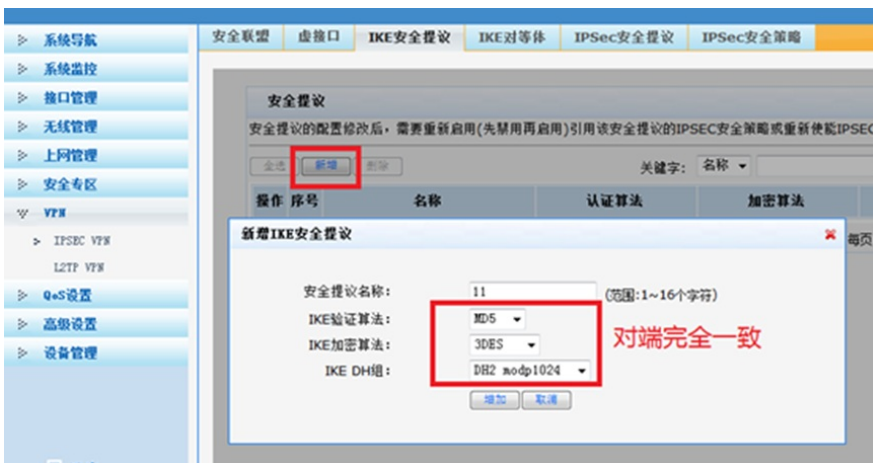
选择一个虚接口名称和与其相应的WAN口绑定，单击<增加>按钮。



#### 2. 设置IKE安全提议

VPN→VPN设置→IKE安全提议

输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮。

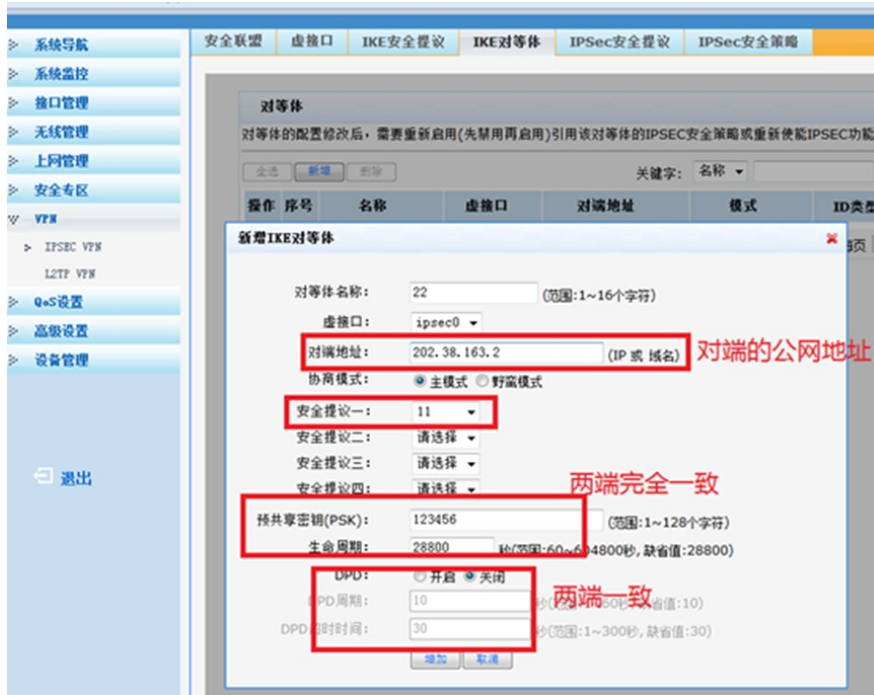


#### 3. 设置IKE对等体

VPN→VPN设置→IKE对等体

输入对等体名称，选择对应的虚接口ipsec0。在“对端地址”文本框中输入Router A的IP地址，

并选择已创建的安全提议等信息，单击<增加>按钮。



#### 4设置IPSec安全提议

VPN→VPN设置→IPSec安全提议

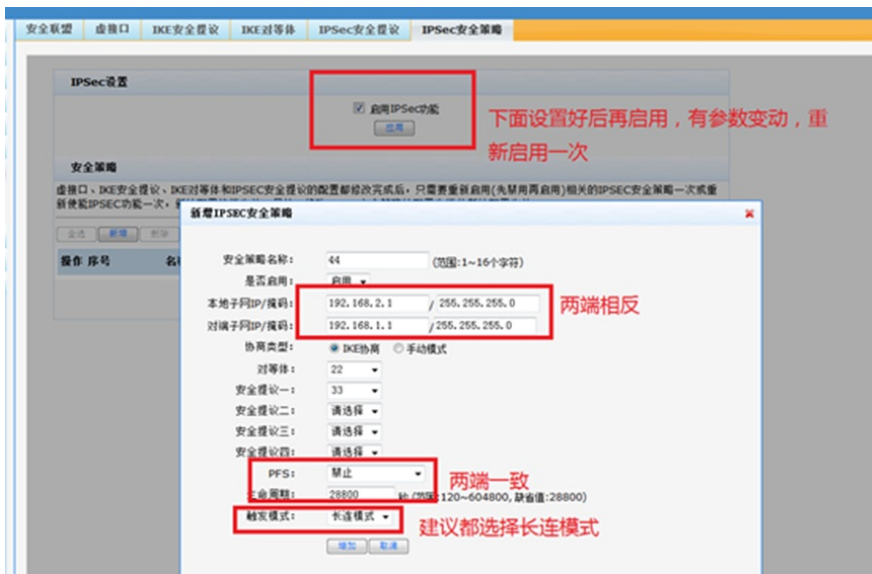
输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮



#### 5设置IPSec安全策略

VPN→VPN设置→IPSec安全策略

输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入客户分支机构A和B所处的子网信息，并选择协商类型为“IKE协商”、对等体为“22”、安全提议为“33”，PFS两端设置一致，单击<增加>按钮。

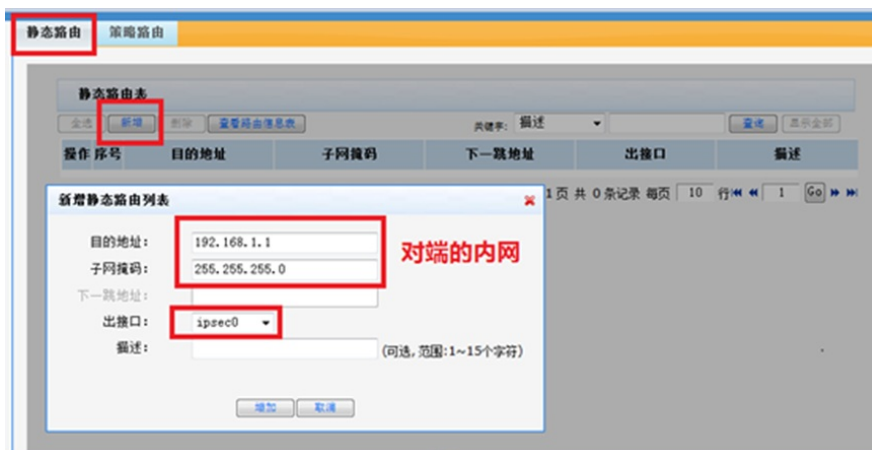


## 6设置路由

高级设置→路由设置→静态路由

需要为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通。一般情况下，只需要为隧道报文配置静态路由即可。

配置静态路由时，指定目的地址网段后不需要指定下一跳地址，直接配置使用正确的IPSec虚接口即可。



## 7配置成功如下

A:



B:

安全联盟							
安全联盟SA							
通过安全联盟SA，IPSec能够对不同的数据流提供不同级别的安全保护。在这里可以查询到相应隧道当前状态，了解隧道建立的各个参数。							
刷新							
名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
44	out	202.38.163.2 =>202.38.163.3	----	----	0x66740de3	3DES_MD5	192.168.1.0/24 =>192.168.2.0/24
44	in	202.38.163.3 =>202.38.163.2	----	----	0xd9c5c1c1	3DES_MD5	192.168.2.0/24 =>192.168.1.0/24

第 1 页 / 共 1 页 共 2 条记录 每页 10 行

### ★温馨提示

以上案例中的IP都是固定的，如果IP地址不是固定，则可以申请一个动态域名，登录到路由器界面，会生成一个域名，这个域名会绑定上公网IP，如图：

DDNS IPv4 DNS Server

动态域名配置

如果您在网上申请的主机名为xxxx，那么请在下面“注册的主机名”输入框中配置“主机名+域名”的格式，例如配置xxxx.3322.org，刷新页面可查看注册状态。

WAN1 DNS:  禁用  启用

用户名: pseudo (范围: 1~31个字符)

密码: \*\*\*\*\* (范围: 1~31个字符)

注册的主机名: pseudo (范围: 1~63个字符)

DDNS服务器地址: pubyun.com 网址链接: www.pubyun.com

当前地址: 10.100.13.12 状态: 域名

WAN2

保存

“注册的主机名”就是域名，“当前地址”就是线路上的公网地址，可以用这个域名来取代公网的IP填写到路由器中。