

知 ERG2系列路由器 IPSEC VPN多分支互通典型配置

IPSec VPN 史晓虎 2019-08-21 发表

组网及说明

1 配置需求或说明

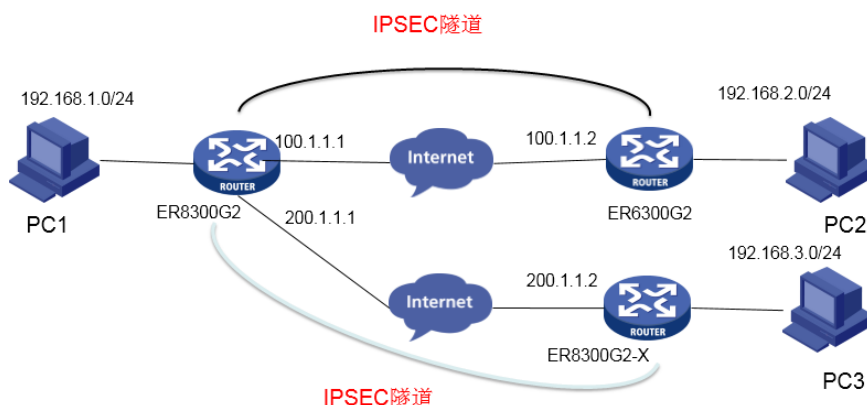
1.1 适用产品系列

本案例适用于如ER3200G2、ER5200G2、ER6300G2、ER8300G2等ERG2系列的路由器。

1.2 配置需求及实现的效果

在总部和分部之间分别建立安全隧道，对客户总部PC1所在的子网（192.168.1.0）与客户分支机构PC2所在的子网（192.168.2.0）和客户分支机构PC3所在的子网（192.168.3.0）之间的数据流进行安全保护。安全协议采用ESP协议，加密算法采用3DES，认证算法采用MD5。

2 组网图

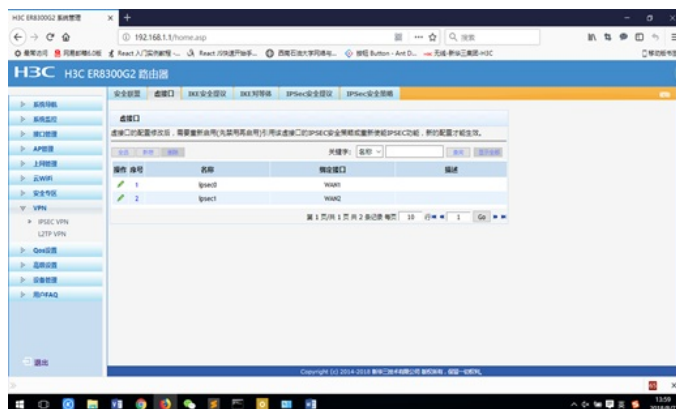


配置步骤

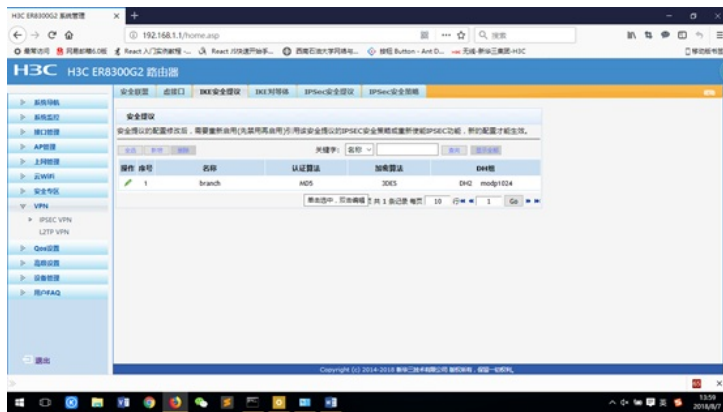
3 配置步骤

3.1 配置总部ER8300G2

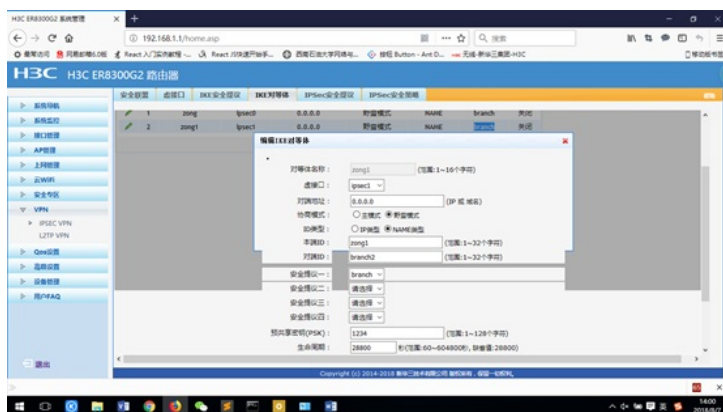
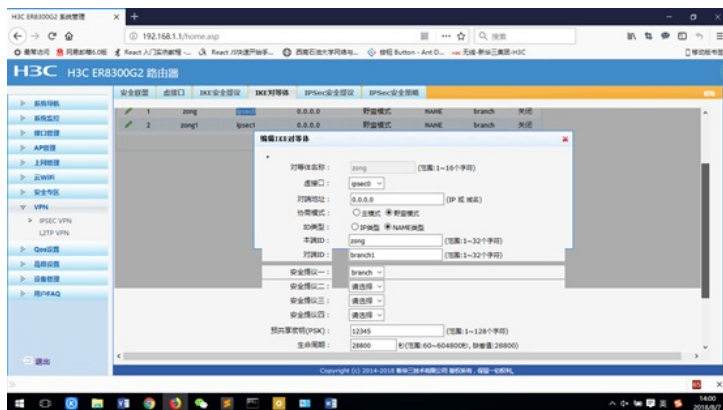
#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作



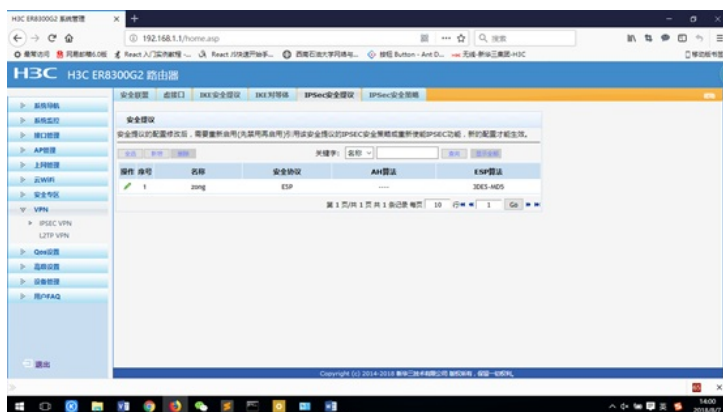
#选择“VPN→IPSEC VPN→IKE安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择野蛮模式，选择对应的虚接口。在“ID类型”选择NAME，并选择已创建的安全提议等信息，单击<增加>按钮完成操作

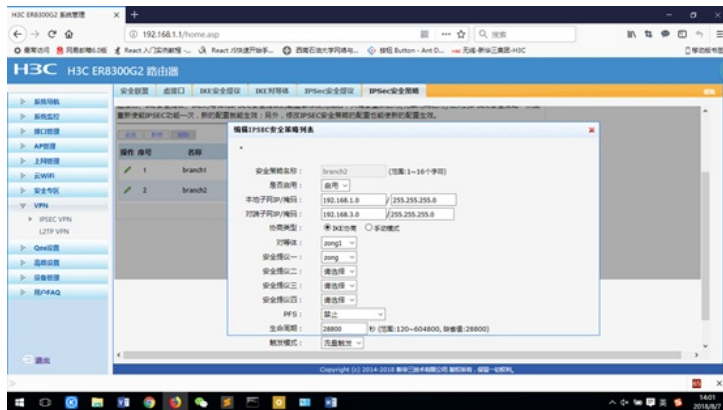
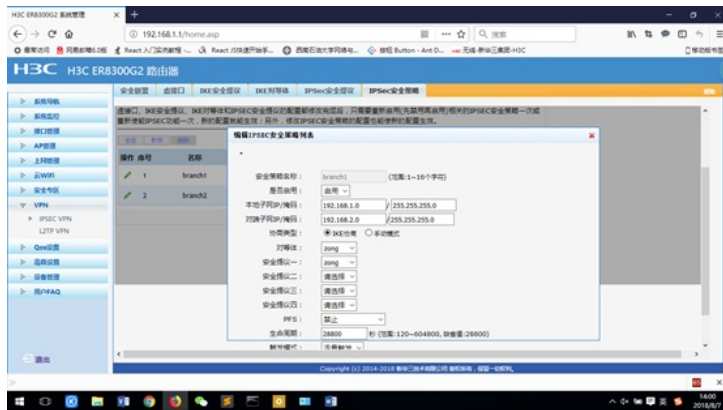


#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作

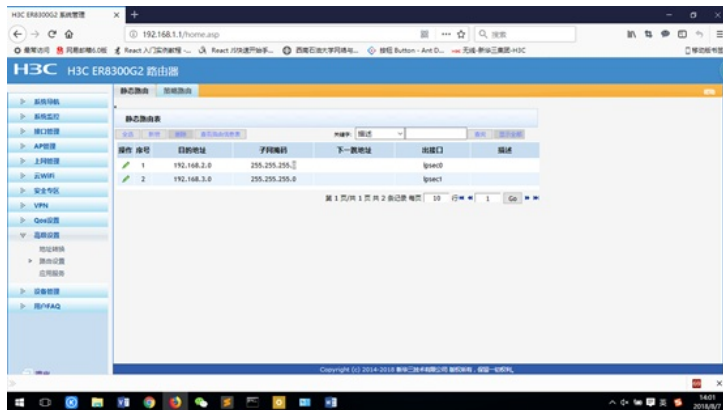


#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本

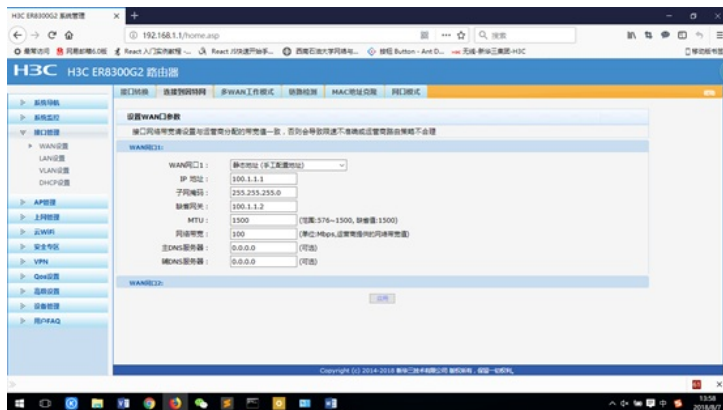
框中分别输入客户分支机构B和C所处的子网信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作

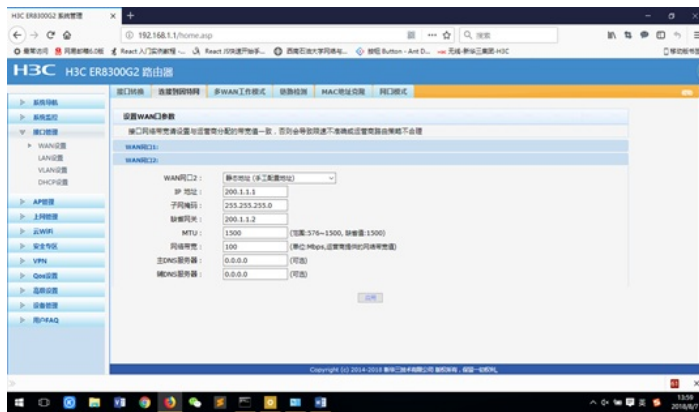


#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作

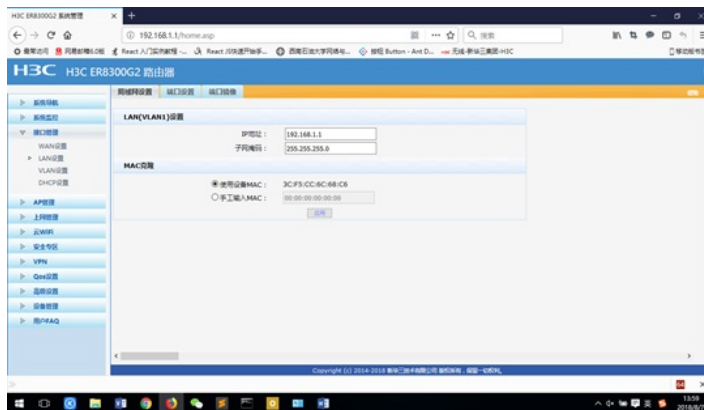


#为WAN口进行地址配置



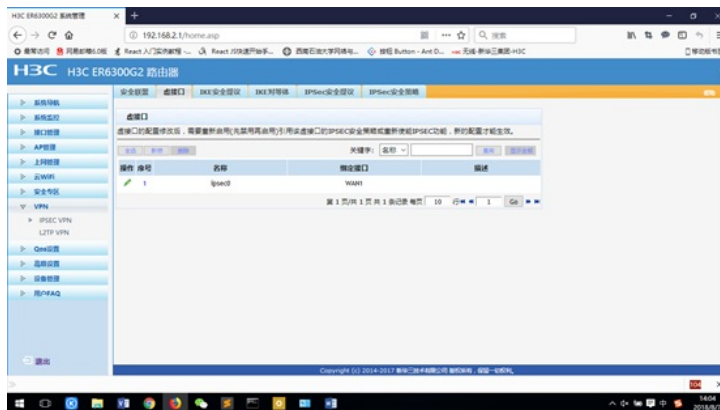


#为LAN口进行地址配置

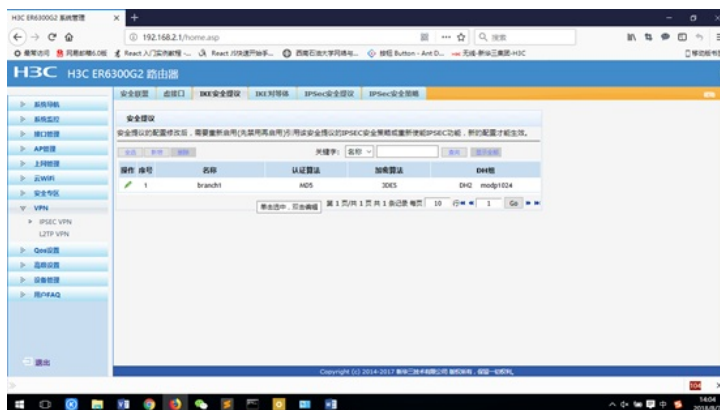


3.2配置分支 (B) ER6300G2

#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作

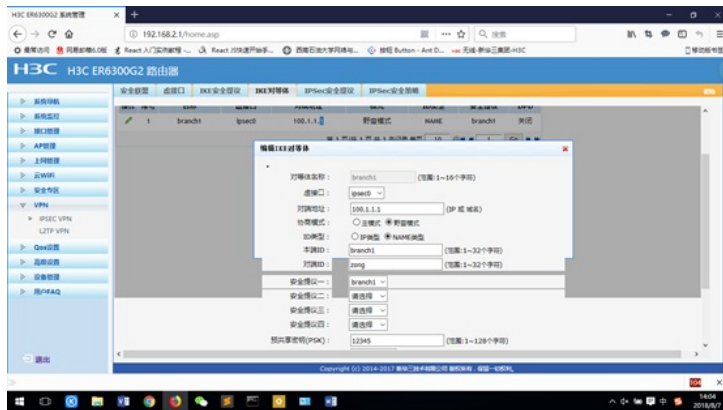


#选择“VPN→IPSEC VPN→IKE安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作

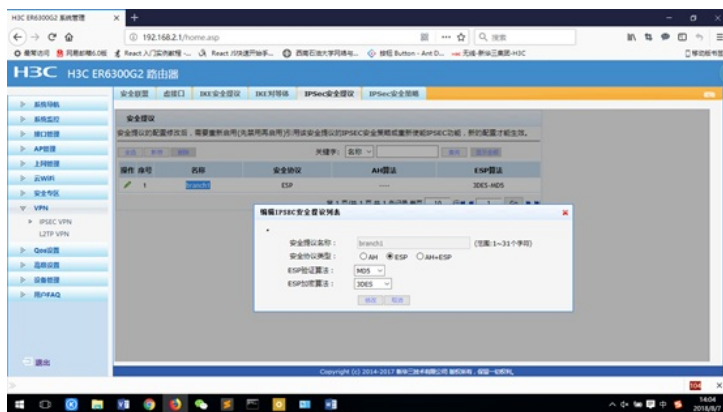


#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择

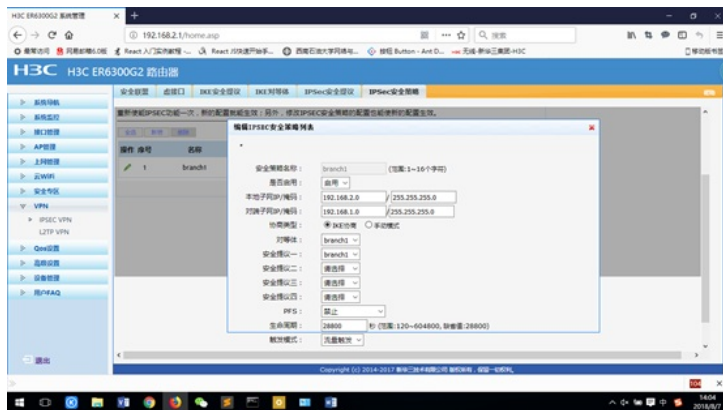
对应的虚接口。在“对端地址”文本框中输入IP地址，并选择已创建的安全提议等信息，单击<增加>按钮完成操作



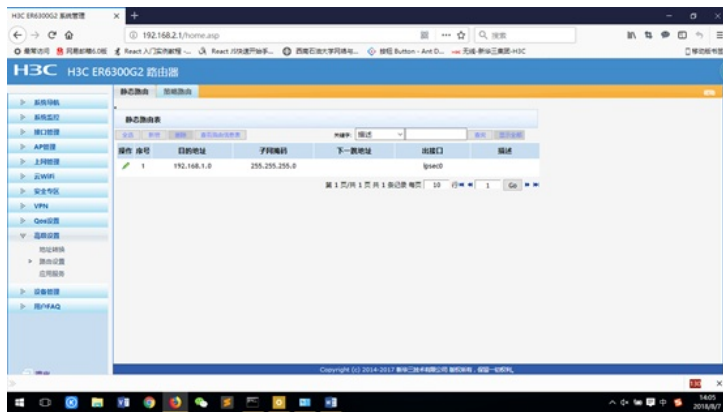
#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



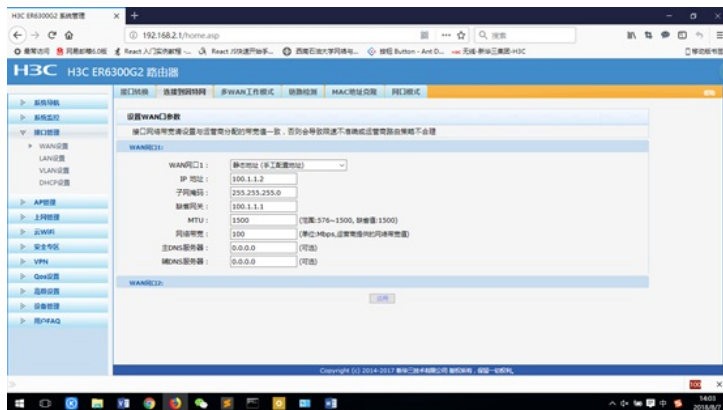
#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入对应信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作



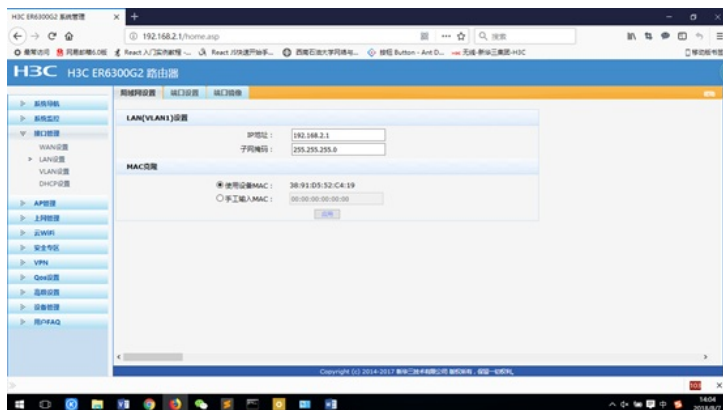
#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作



#为WAN口进行地址配置。



#为LAN口进行地址配置。



3.3配置分支 (C) ER300G2-X

#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作



#选择“VPN→IPSEC VPN→IKE安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



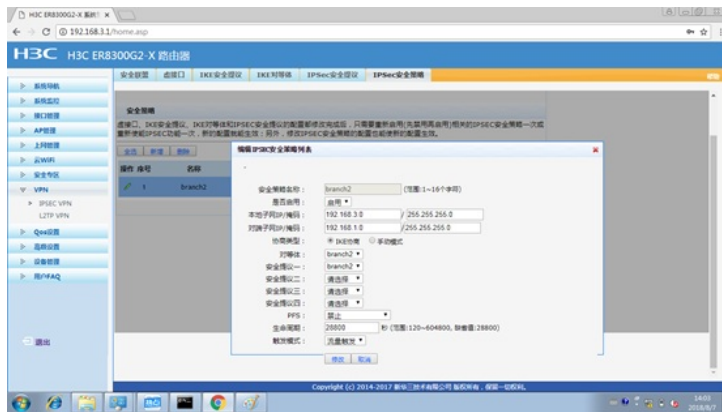
#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择对应的虚接口。在“对端地址”文本框中输入IP地址，并选择已创建的安全提议等信息，单击<增加>按钮完成操作



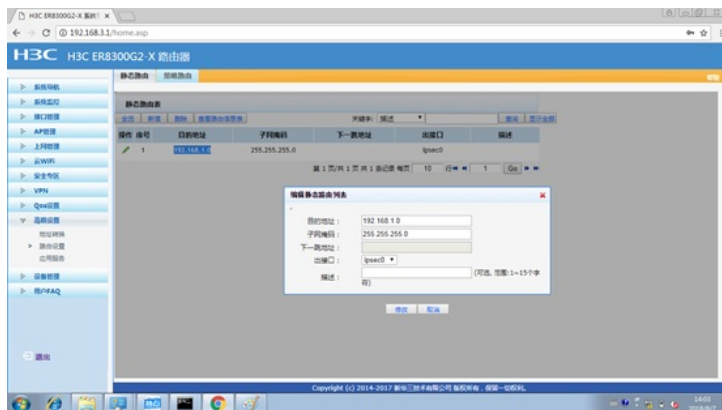
#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入对应信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作



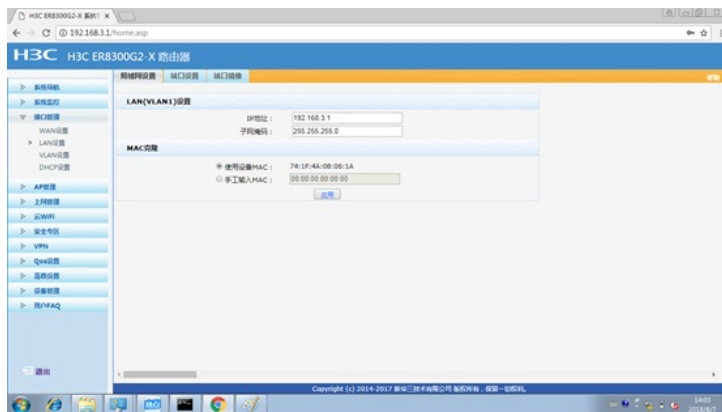
#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击“新增”按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击“增加”按钮完成操作



#为WAN口进行地址配置。



#为LAN口进行地址配置。



2 验证配置

#查看VPN状态


```
C:\windows\system32\cmd.exe

正在 Ping 100.1.1.1 具有 32 字节的数据:
来自 100.1.1.1 的回复: 字节=32 时间<1ms TTL=127

100.1.1.1 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
^C
C:\Users\yys8936>ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
请求超时。
来自 192.168.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.1 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.1 的回复: 字节=32 时间<1ms TTL=127

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 3, 丢失 = 1 (25% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\yys8936>
```

名称	方向	源地址	目的地址	动作	策略名称
branch2	out	200.1.1.1 →200.1.1.2	---	---	ESP SPI
branch2	in	200.1.1.2 ←200.1.1.1	---	---	ESP SPI
branch1	in	100.1.1.1 →100.1.1.2	---	---	ESP SPI
branch1	in	100.1.1.2 →100.1.1.1	---	---	ESP SPI

名称	方向	隧道名称	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
branch1	in	100.1.1.1 ⇨100.1.1.2	----	----	0x720b0d0	3DES, MD5	192.168.1.0/24 ⇨192.168.2.0/24
branch1	out	100.1.1.2 ⇨100.1.1.1	----	----	0xa001340c	3DES, MD5	192.168.2.0/24 ⇨192.168.1.0/24



配置关键点