
ERG2 系列路由器 IPSEC VPN 多分支互通典型配置

目录

ERG2 系列路由器 IPSEC VPN 多分支互通典型配置.....	1
1 配置需求或说明.....	1
1.1 适用产品系列.....	1
1.2 配置需求及实现的效果.....	1
2 组网图.....	2
3 配置步骤.....	2
3.1 配置总部 ER8300G2.....	2
3.2 配置分支（B）ER6300G2.....	8
3.3 配置分支（C）ER8300G2-X.....	12
4 验证配置.....	15

1 配置需求或说明

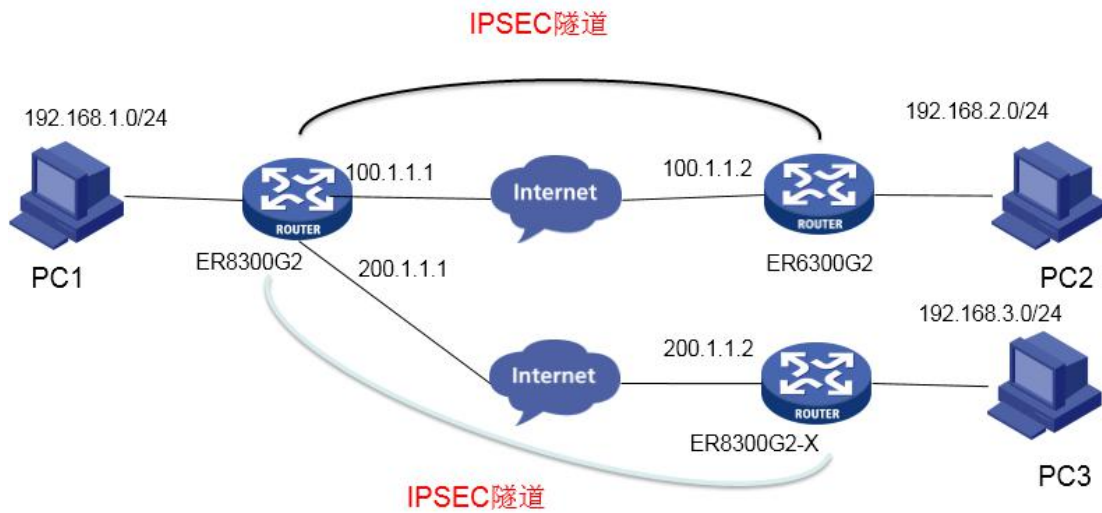
1.1 适用产品系列

本案例适用于ERG2 产品系列路由器：ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等。

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。

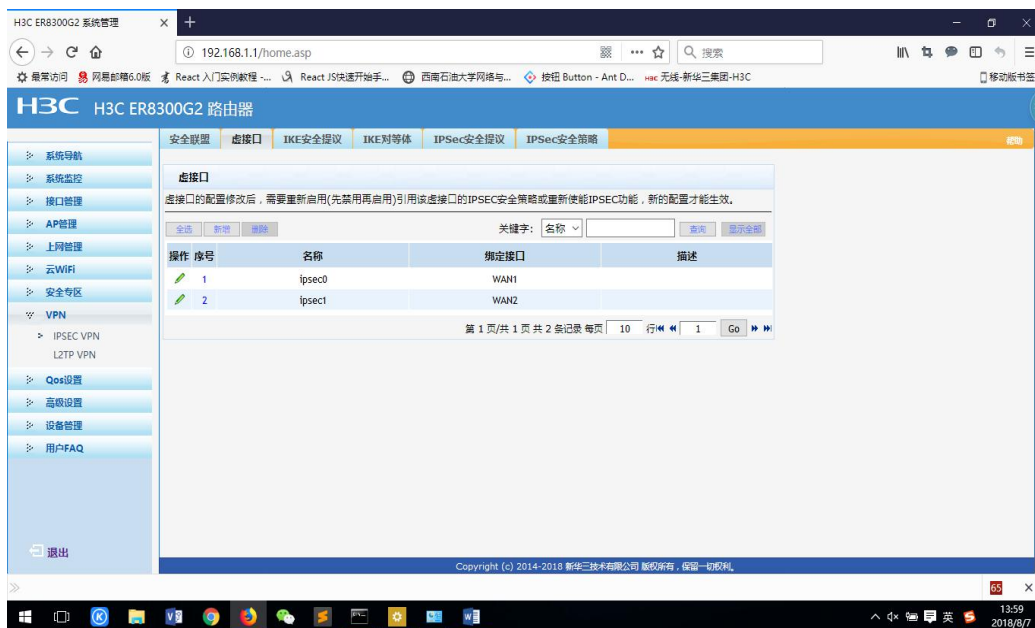
2 组网图



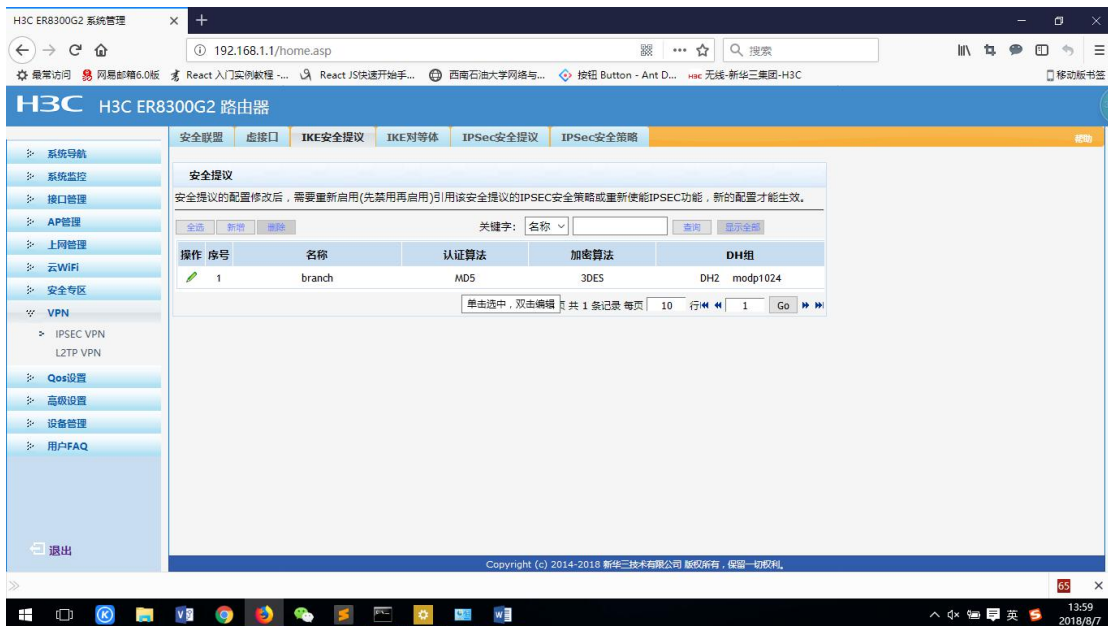
3 配置步骤

3.1 配置总部 ER8300G2

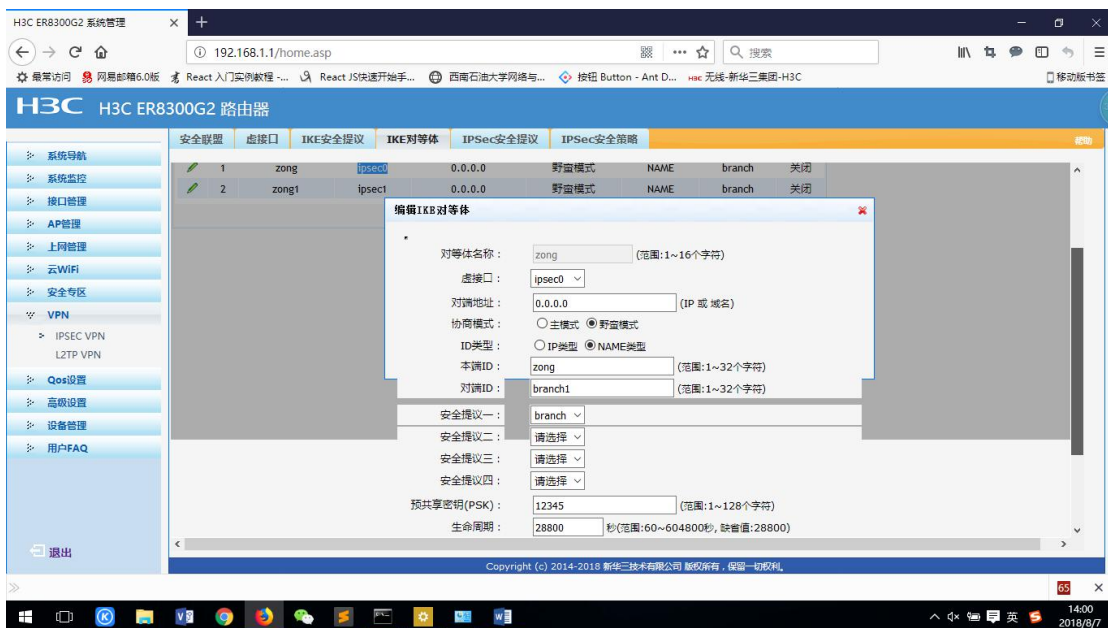
#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作

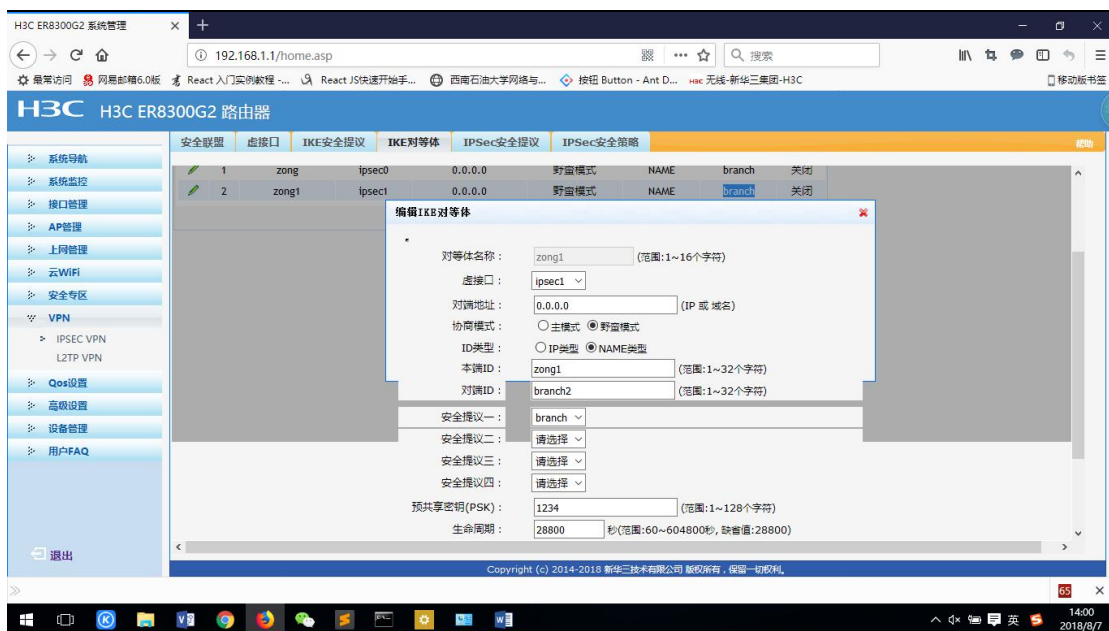


#选择“VPN→IPSEC VPN→IKE安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作

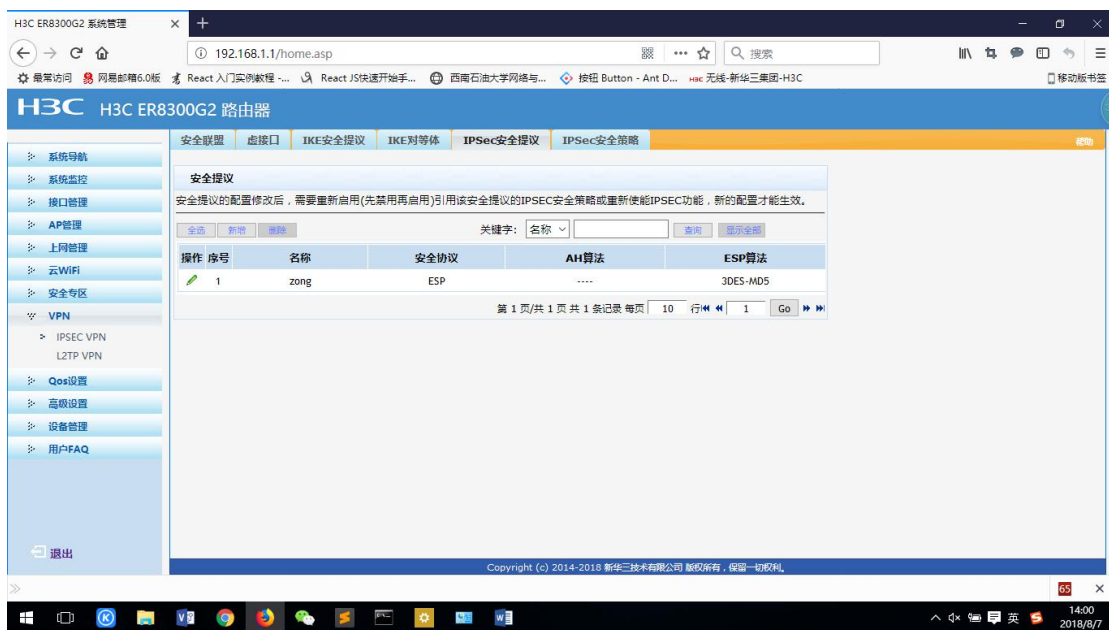


#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择野蛮模式，选择对应的虚接口。在“ID类型”选择NAME，并选择已创建的安全提议等信息，单击<增加>按钮完成操作

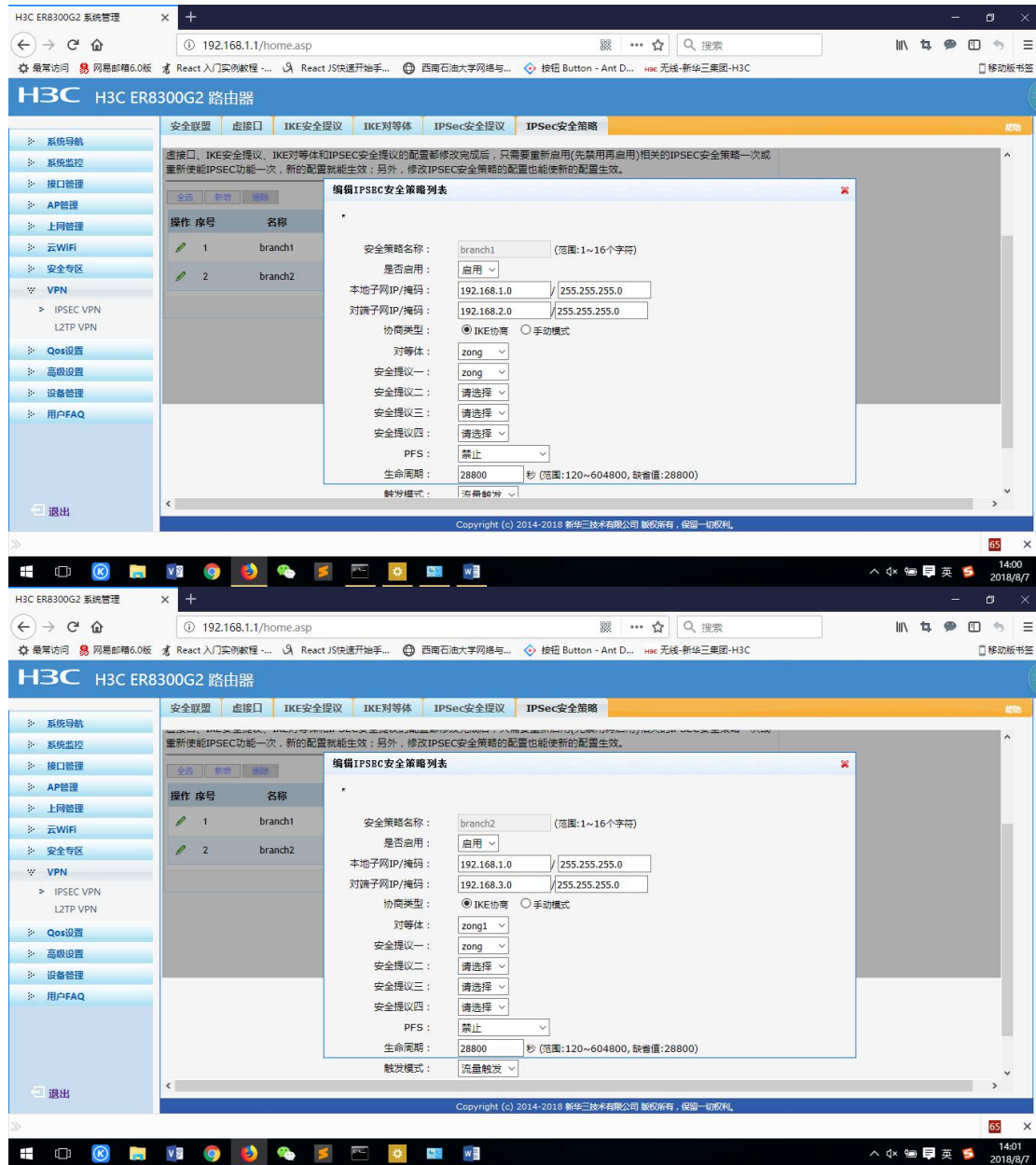




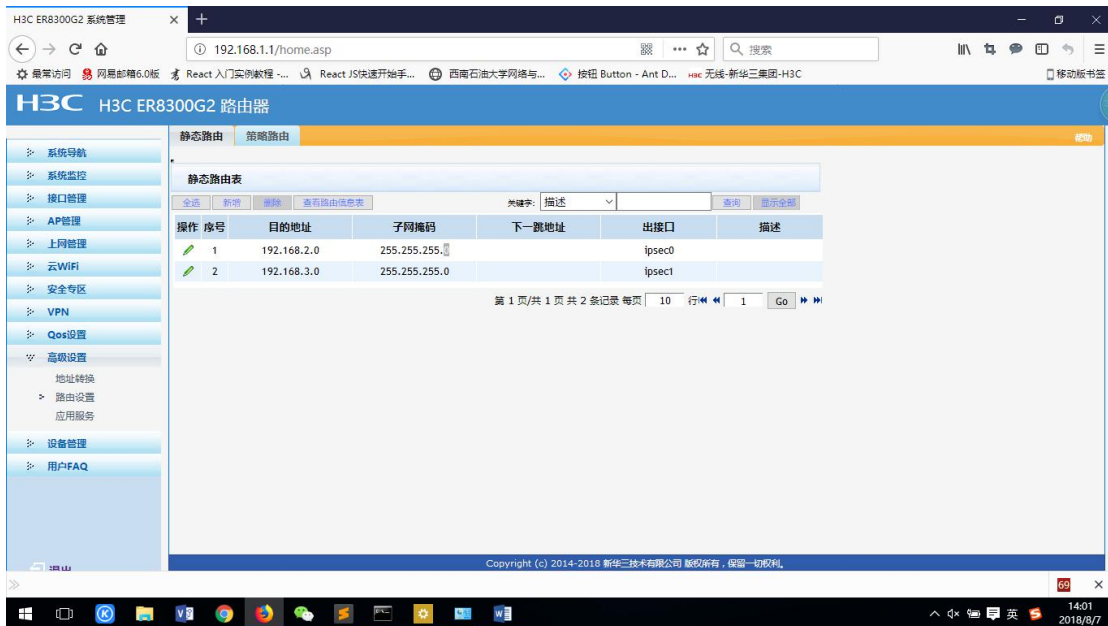
#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



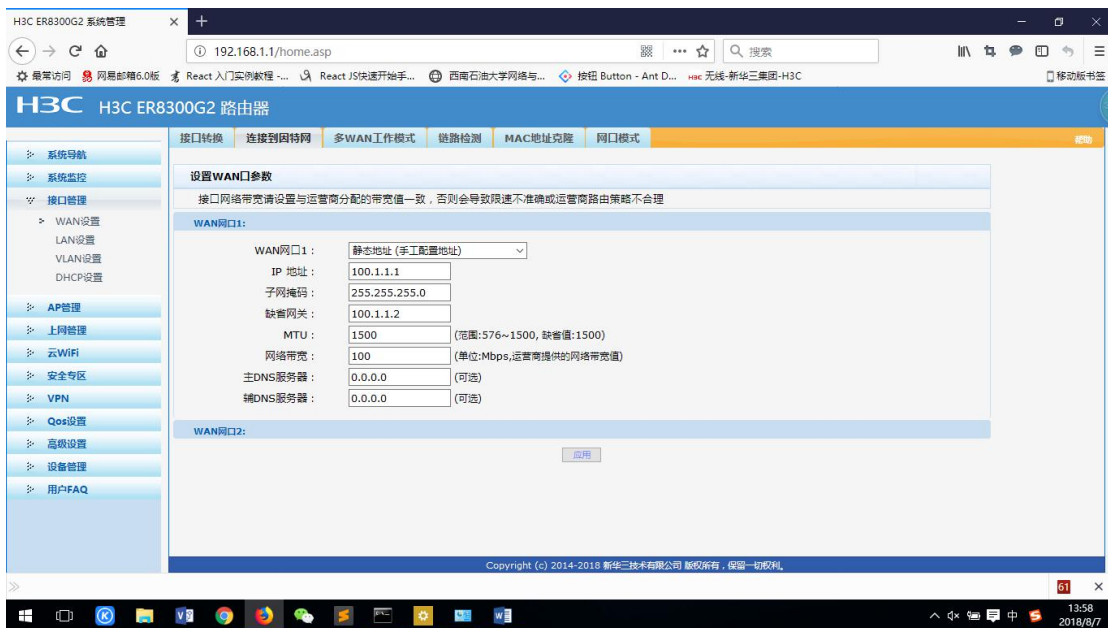
#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入客户分支机构B和C所处的子网信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作

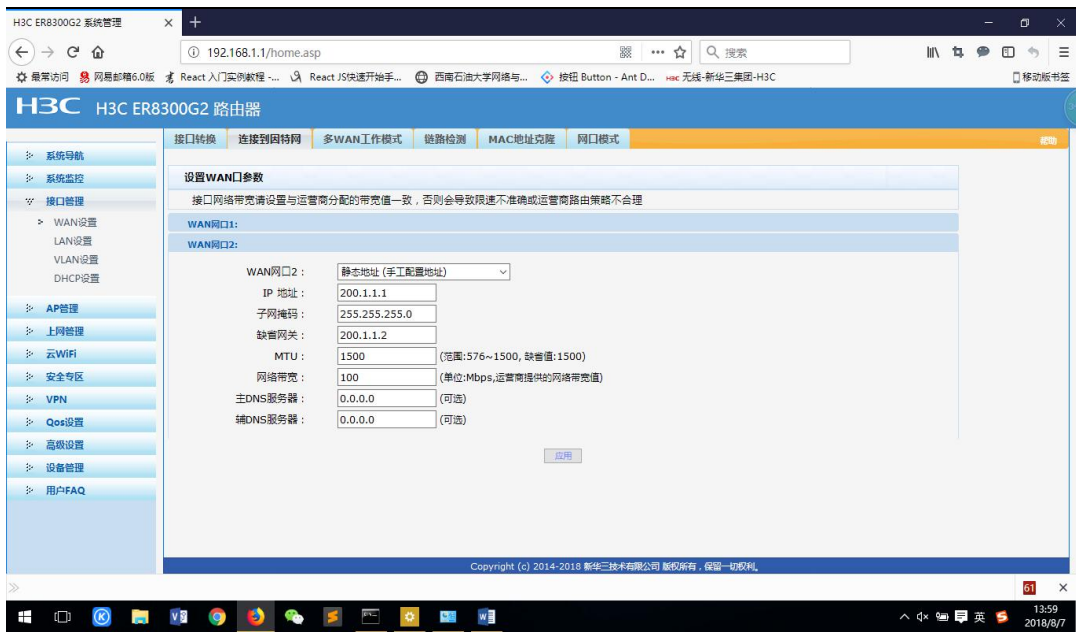


#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作

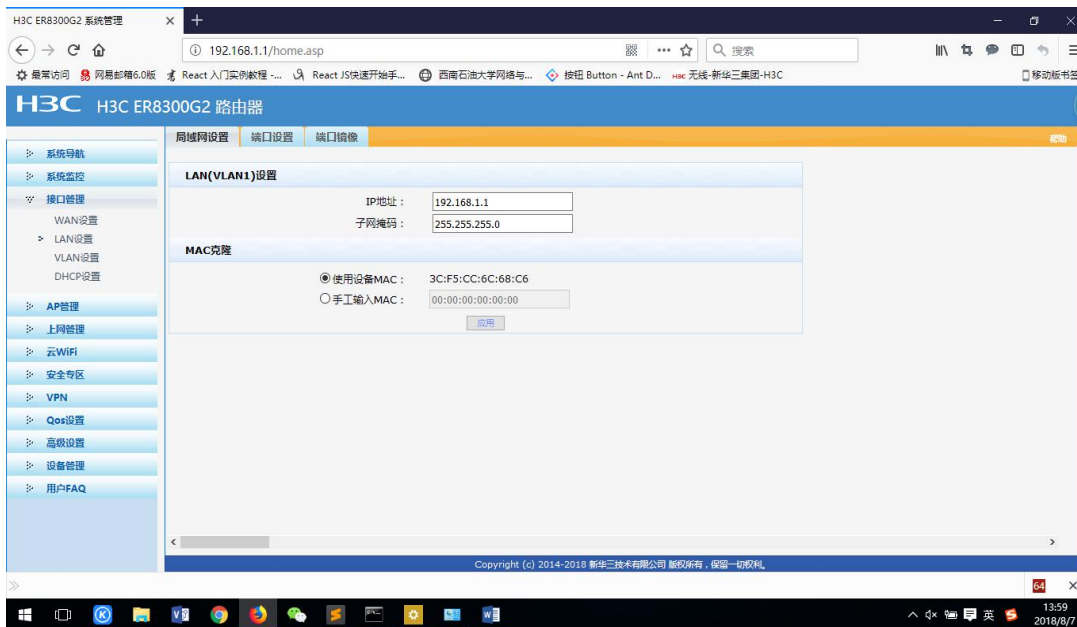


#为WAN口进行地址配置



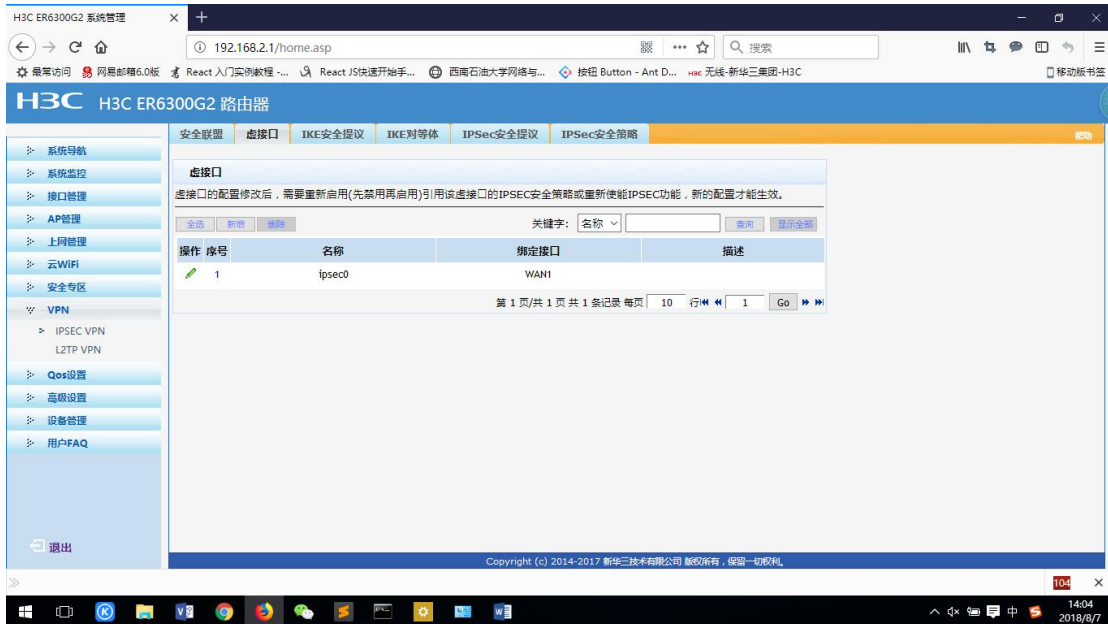


#为LAN口进行地址配置

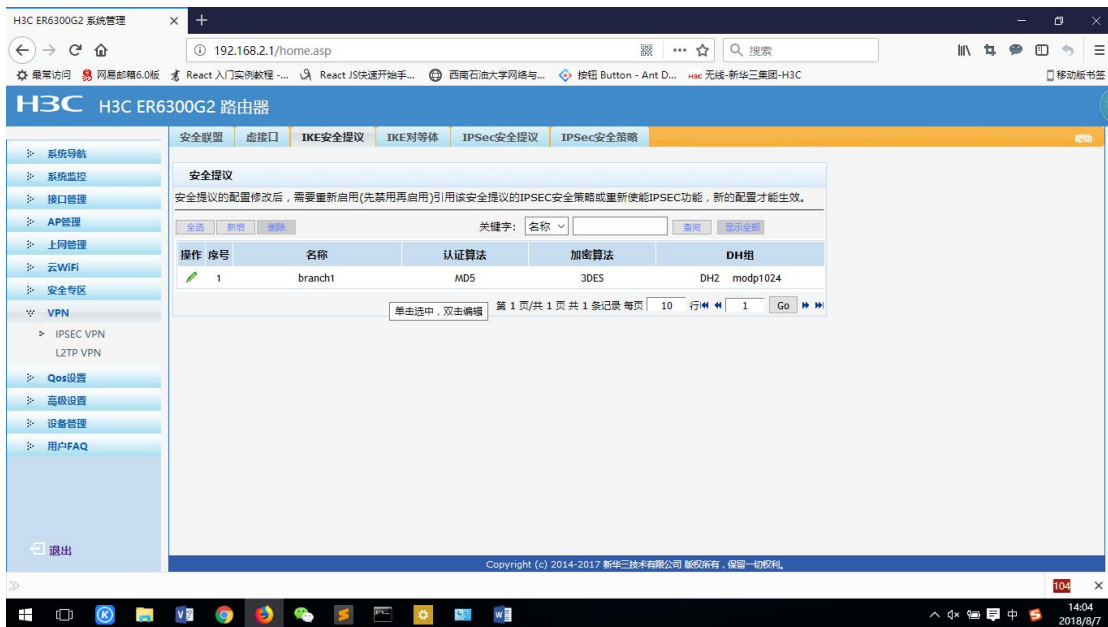


3.2 配置分支（B）ER6300G2

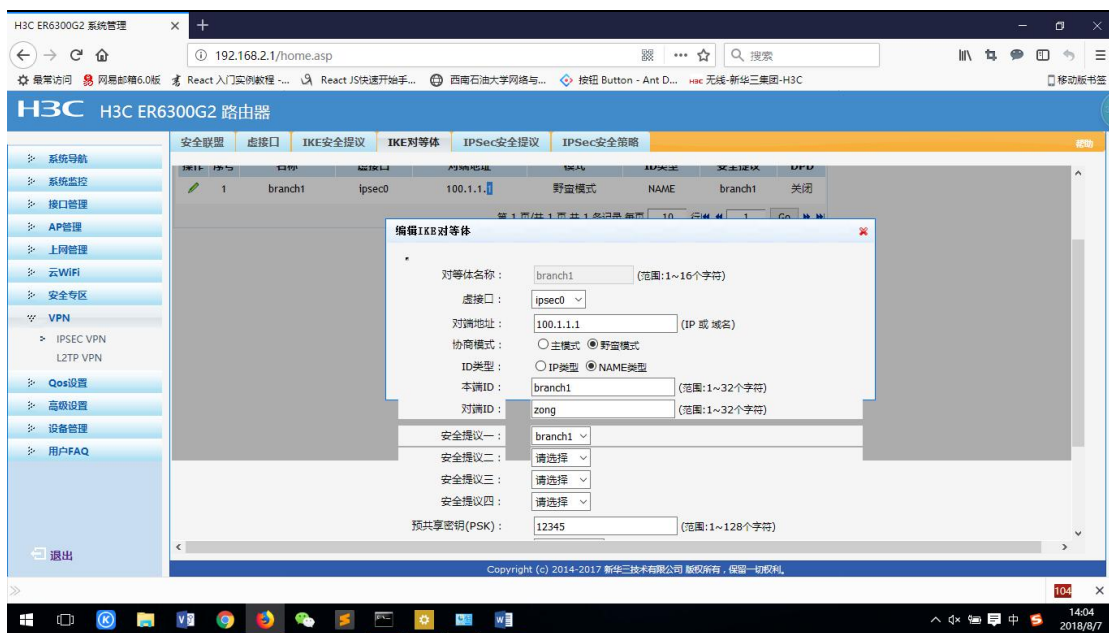
#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作



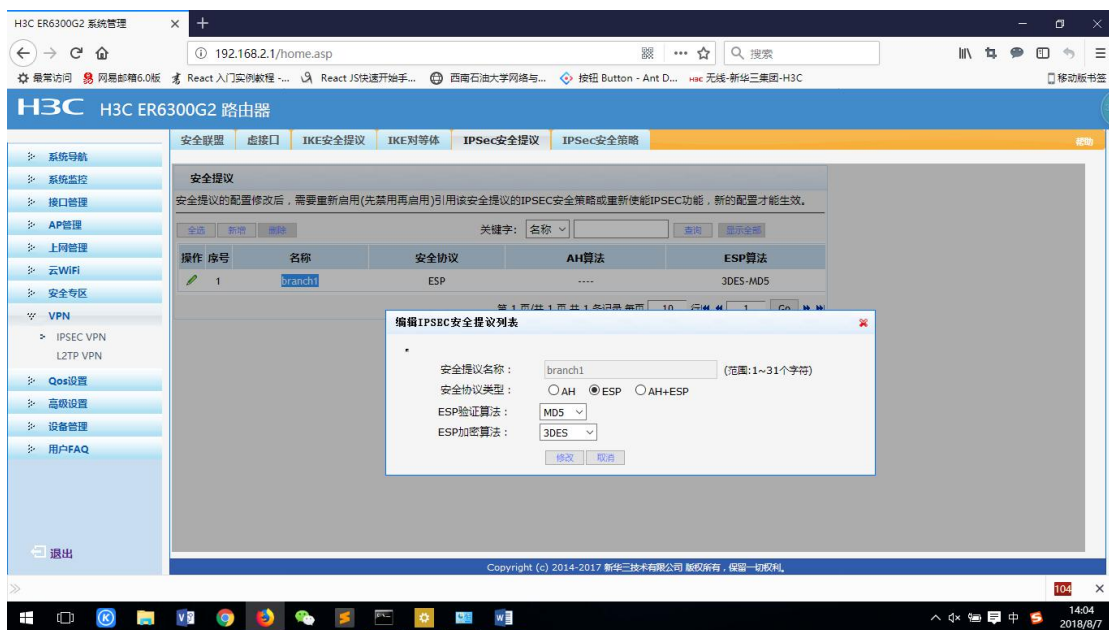
#选择“VPN→IPSEC VPN→IKE 安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



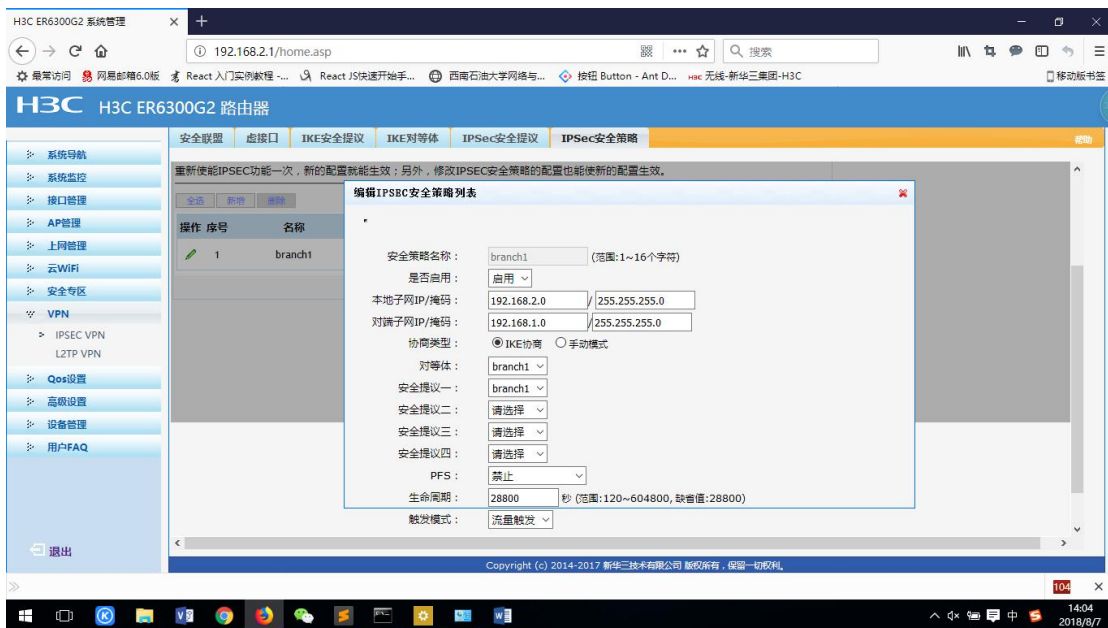
#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择对应的虚接口。在“对端地址”文本框中输入IP地址，并选择已创建的安全提议等信息，单击<增加>按钮完成操作



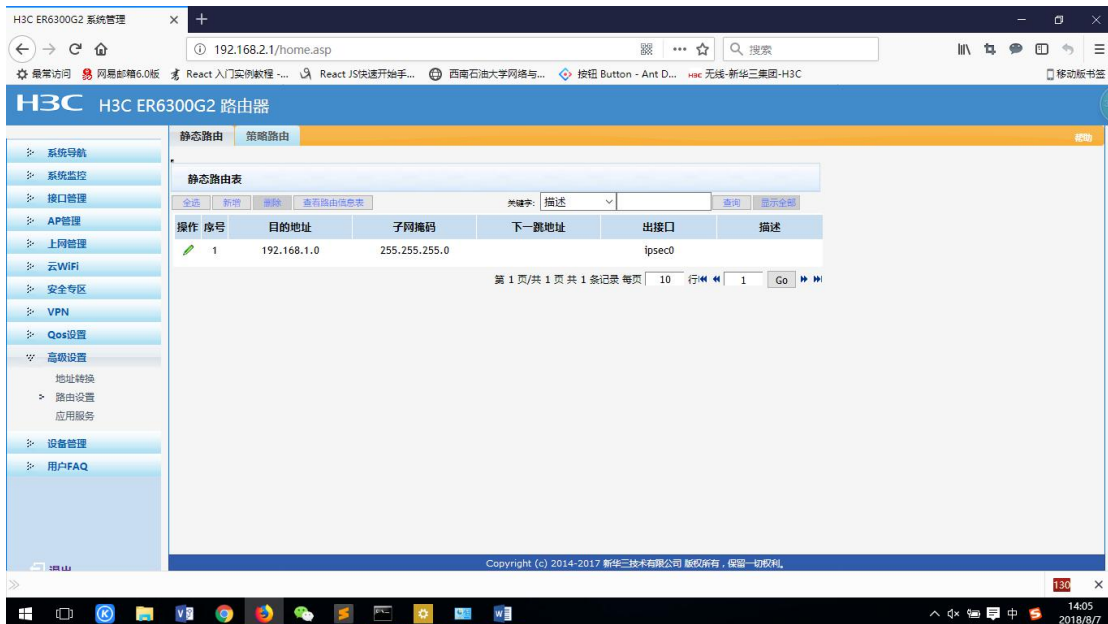
#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



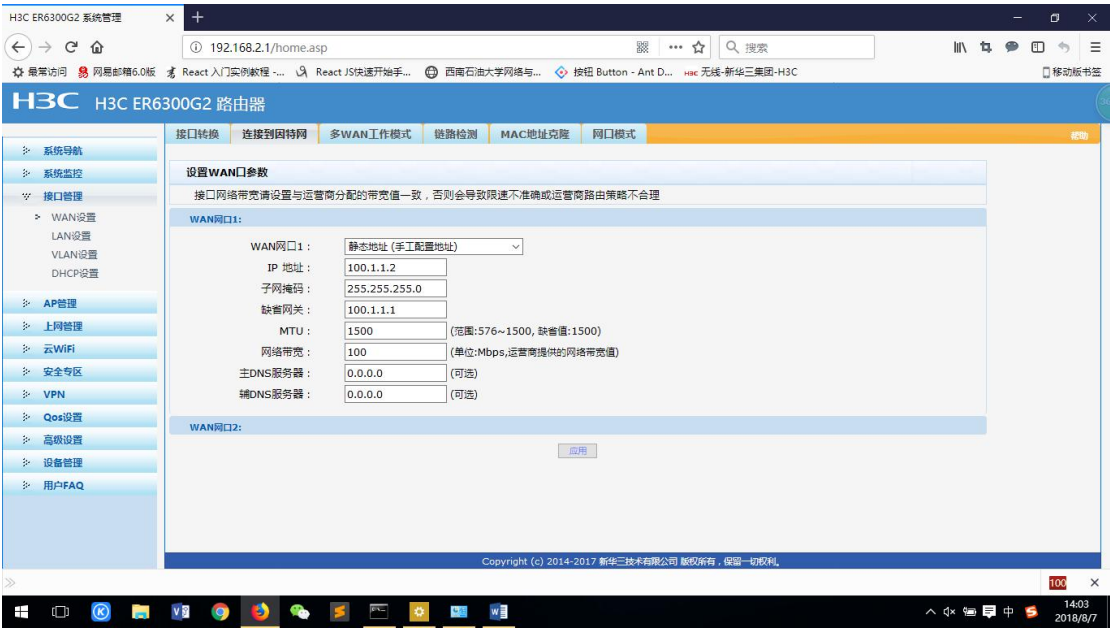
#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入对应信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作



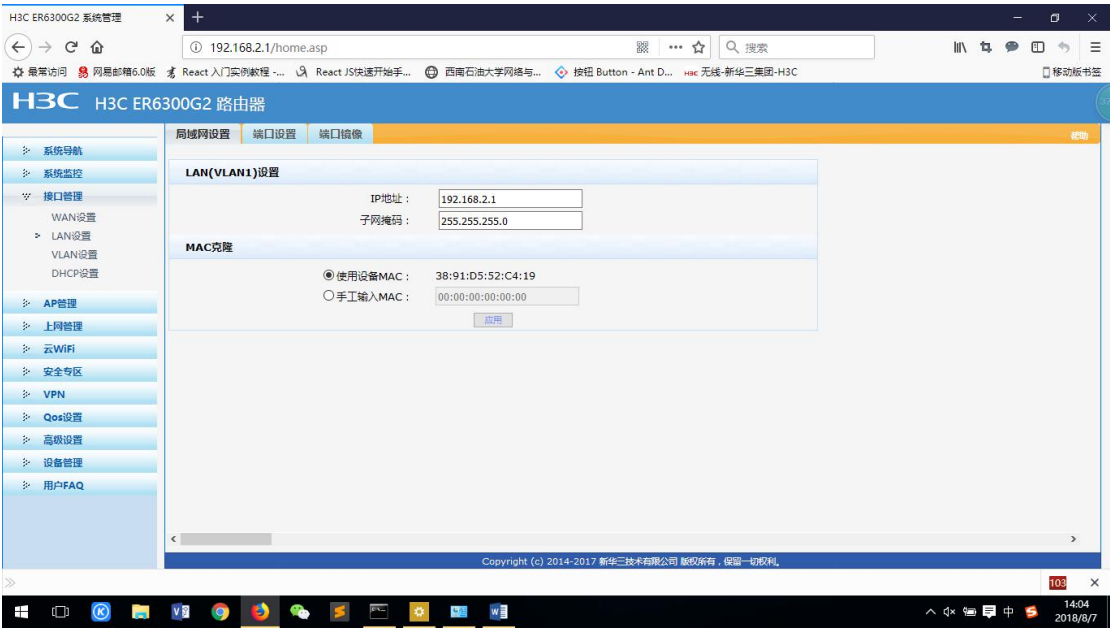
#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作



#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）ER8300G2-X

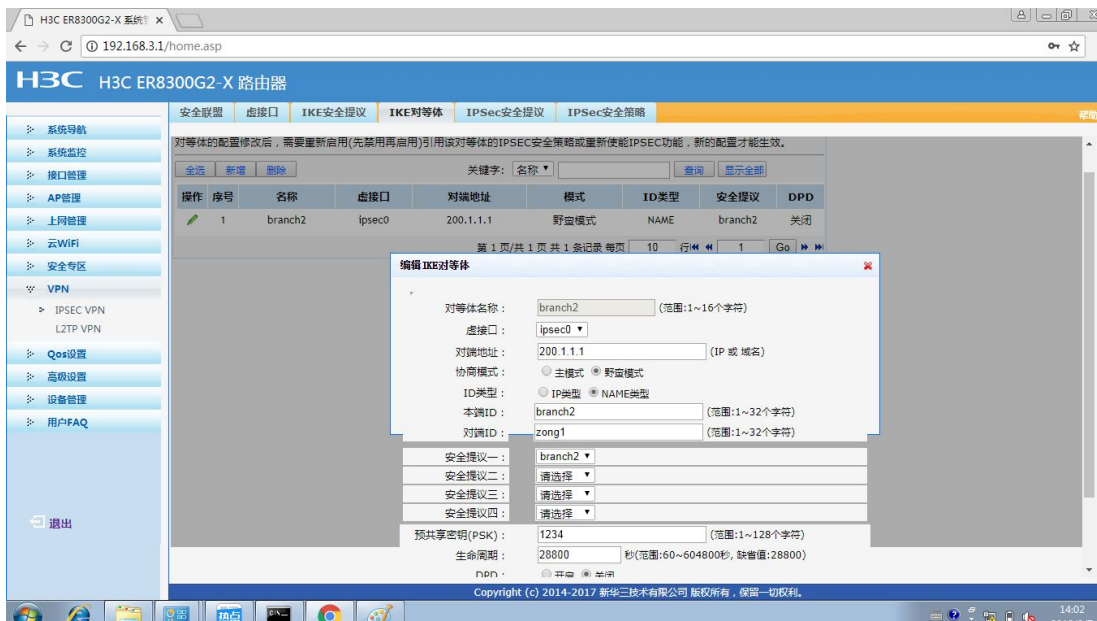
#选择“VPN→IPSEC VPN→虚接口”。单击<新增>按钮，在弹出的对话框中选择一个虚接口通道，并将其与对应的出接口进行绑定，单击<增加>按钮完成操作



#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



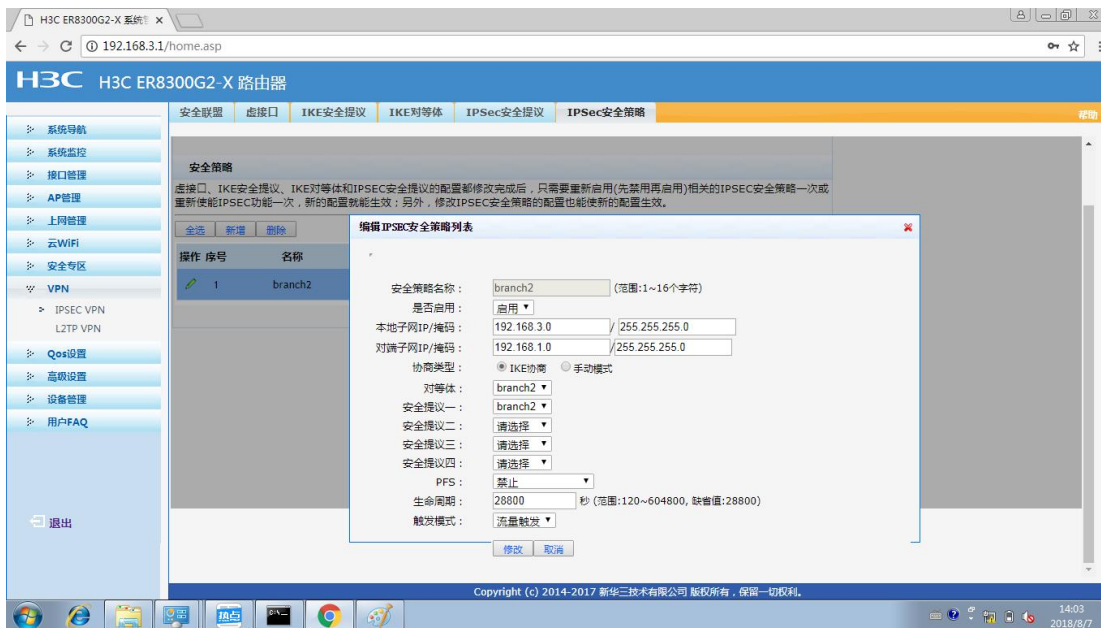
#选择“VPN→IPSEC VPN→IKE对等体”。单击<新增>按钮，在弹出的对话框中输入对等体名称，选择对应的虚接口。在“对端地址”文本框中输入IP地址，并选择已创建的安全提议等信息，单击<增加>按钮完成操作



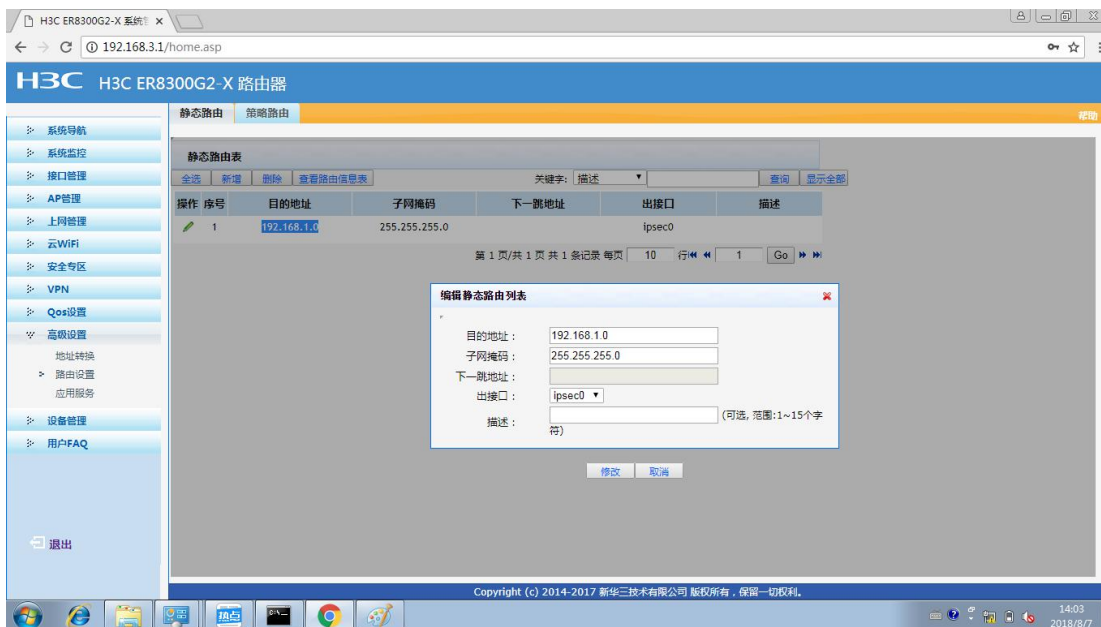
#选择“VPN→IPSEC VPN→IPSec安全提议”。单击<新增>按钮，在弹出的对话框中输入安全提议名称，选择安全协议类型为ESP，并设置验证算法和加密算法分别为MD5、3DES，单击<增加>按钮完成操作



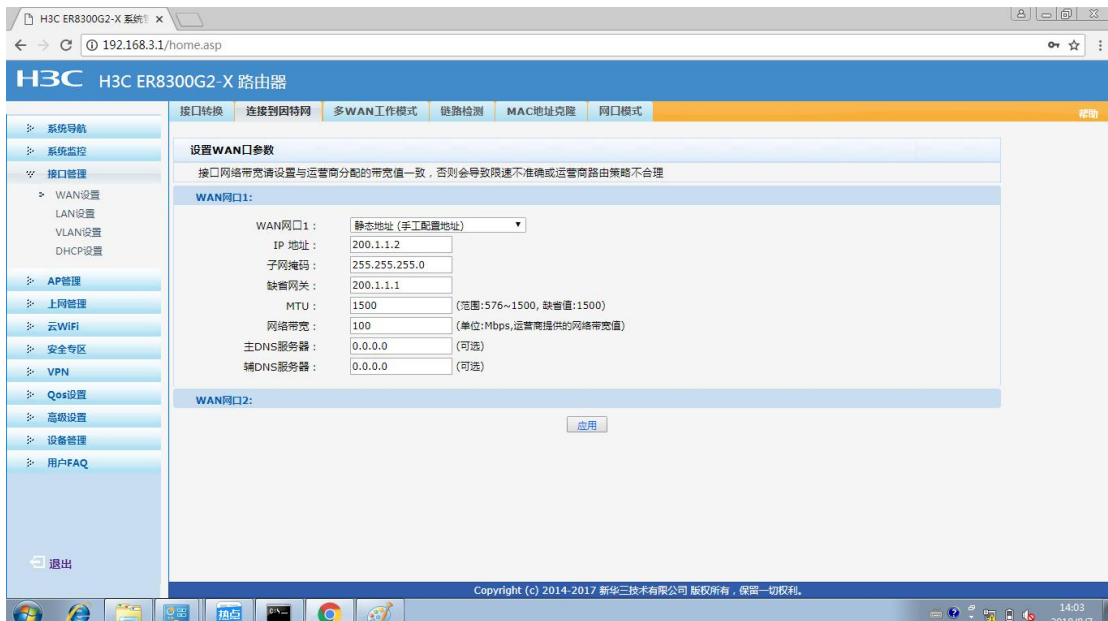
#选择“VPN→IPSEC VPN→IPSec安全策略”。选中“启用IPSec功能”复选框，单击<应用>按钮生效。单击<新增>按钮，在弹出的对话框中输入安全策略名称，在“本地子网IP/掩码”和“对端子网IP/掩码”文本框中分别输入对应信息，并选择协商类型，对等体，安全提议，单击<增加>按钮完成操作



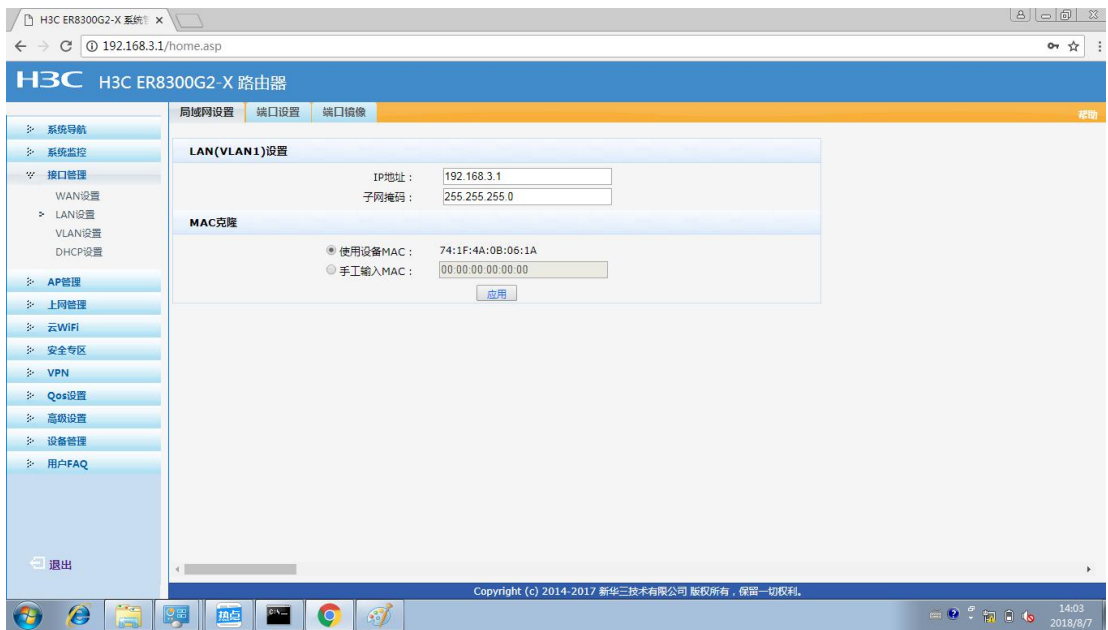
#为经过IPSec VPN隧道处理的报文设置路由，才能使隧道两端互通（一般情况下，只需要为隧道报文配置静态路由即可）。选择“高级设置→路由设置→静态路由”，单击<新增>按钮，在弹出的对话框中，设置目的地址、子网掩码等参数，单击<增加>按钮完成操作



#为WAN口进行地址配置。



#为LAN口进行地址配置。



4 验证配置

#查看VPN状态

两端均设置完成后，保护流ping后建立隧道。您可以通过选择路由器的“VPN→IPSEC VPN→安全联盟”页面，并单击<刷新>按钮来查看相应的隧道是否已成功建立。

```
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\yys0936>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\yys0936>
半:
```

总部隧道建立图

H3C ER8300G2 系统管理

192.168.1.1/home.asp

最新访问 网易邮箱6.0版 React入门教程... React JS快速上手... 西南石油大学网络与... 按钮 Button - Ant D... H3C 无线-新华三集团-H3C

H3C H3C ER8300G2 路由器

系统导航

系统监控

接口管理

AP管理

上网管理

云WiFi

安全专区

VPN

IPSec VPN

L2TP VPN

Qos设置

高级设置

设备管理

用户FAQ

退出

安全联盟

虚接口

IKE安全提议

IKE对等体

IPSec安全提议

IPSec安全策略

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
branch2	out	200.1.1.1 =>200.1.1.2	----	----	0xc263438e	3DES_MD5	192.168.1.0/24 =>192.168.3.0/24
branch2	in	200.1.1.2 =>200.1.1.1	----	----	0xa083345d	3DES_MD5	192.168.3.0/24 =>192.168.1.0/24
branch1	out	100.1.1.1 =>100.1.1.2	----	----	0x726bde50	3DES_MD5	192.168.1.0/24 =>192.168.2.0/24
branch1	in	100.1.1.2 =>100.1.1.1	----	----	0xa083345c	3DES_MD5	192.168.2.0/24 =>192.168.1.0/24

第 1 页/共 1 页 共 4 条记录 每页 10 行 1 Go

Copyright (c) 2014-2018 新华三技术有限公司 版权所有，保留一切权利。

65

13:59 2018/8/7

分支B隧道建立图

The screenshot shows the H3C ER6300G2 router management interface. The left sidebar contains navigation options: 系统导航, 系统监控, 接口管理, AP管理, 上网管理, 云WiFi, 安全专区, VPN, IPSEC VPN, L2TP VPN, Qos设置, 高级设置, 设备管理, 用户FAQ, and 退出. The main content area is titled '安全联盟SA' and displays a table of tunnel configurations. The table has columns: 名称, 方向, 隧道两端, AH SPI, AH 算法, ESP SPI, ESP 算法, and 数据流. The data shows two entries for 'branch1' with 'in' and 'out' directions, both using '100.1.1.1' and '100.1.1.2' as endpoints. The AH SPI is '----', AH 算法 is '----', ESP SPI is '0x726bde50' for 'in' and '0xa083345c' for 'out', and ESP 算法 is '3DES_MD5'. The data flow is '192.168.1.0/24 => 192.168.2.0/24' for 'in' and '192.168.2.0/24 => 192.168.1.0/24' for 'out'. The page footer indicates 'Copyright (c) 2014-2017 新华三技术有限公司 版权所有, 保留一切权利.'

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
branch1	in	100.1.1.1 =>100.1.1.2	----	----	0x726bde50	3DES_MD5	192.168.1.0/24 =>192.168.2.0/24
branch1	out	100.1.1.2 =>100.1.1.1	----	----	0xa083345c	3DES_MD5	192.168.2.0/24 =>192.168.1.0/24

分支C隧道建立图

The screenshot shows the H3C ER8300G2-X router management interface. The left sidebar contains navigation options: 系统导航, 系统监控, 接口管理, AP管理, 上网管理, 云WiFi, 安全专区, VPN, IPSEC VPN, L2TP VPN, Qos设置, 高级设置, 设备管理, 用户FAQ, and 退出. The main content area is titled '安全联盟SA' and displays a table of tunnel configurations. The table has columns: 名称, 方向, 隧道两端, AH SPI, AH 算法, ESP SPI, ESP 算法, and 数据流. The data shows two entries for 'branch2' with 'out' and 'in' directions, both using '200.1.1.2' and '200.1.1.1' as endpoints. The AH SPI is '----', AH 算法 is '----', ESP SPI is '0xa083345d' for 'out' and '0xc263438e' for 'in', and ESP 算法 is '3DES_MD5'. The data flow is '192.168.3.0/24 => 192.168.1.0/24' for 'out' and '192.168.1.0/24 => 192.168.3.0/24' for 'in'. The page footer indicates 'Copyright (c) 2014-2017 新华三技术有限公司 版权所有, 保留一切权利.'

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
branch2	out	200.1.1.2 =>200.1.1.1	----	----	0xa083345d	3DES_MD5	192.168.3.0/24 =>192.168.1.0/24
branch2	in	200.1.1.1 =>200.1.1.2	----	----	0xc263438e	3DES_MD5	192.168.1.0/24 =>192.168.3.0/24