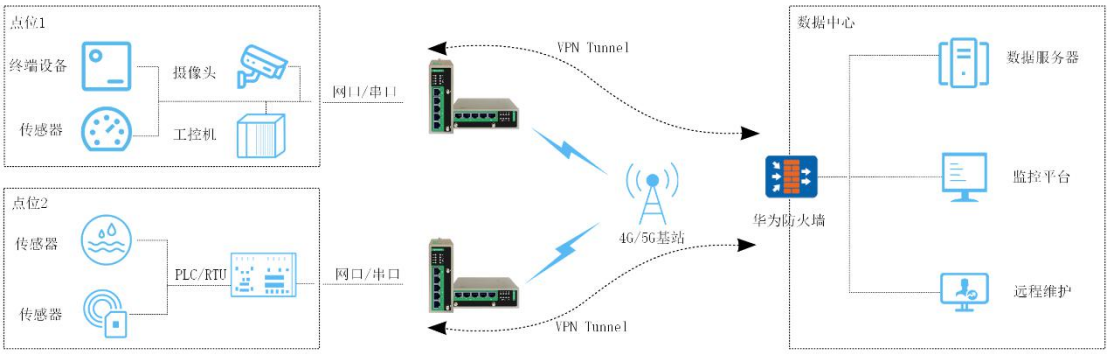
ORB305 与华为防火墙构建 IPsec VPN 配置指导手册

东用科技有限公司

发布日期 2020-08-21



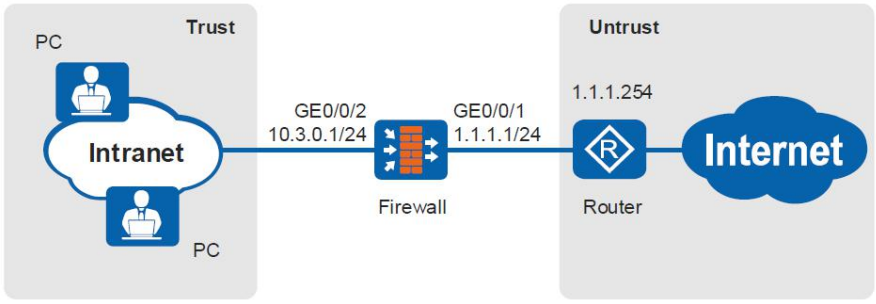
IPsec VPN 组网拓扑：

一、 华为防火墙端配置指导(此处以多数客户使用专线上网形式为例)

1、 将专网网线插入防火墙 1 接口。

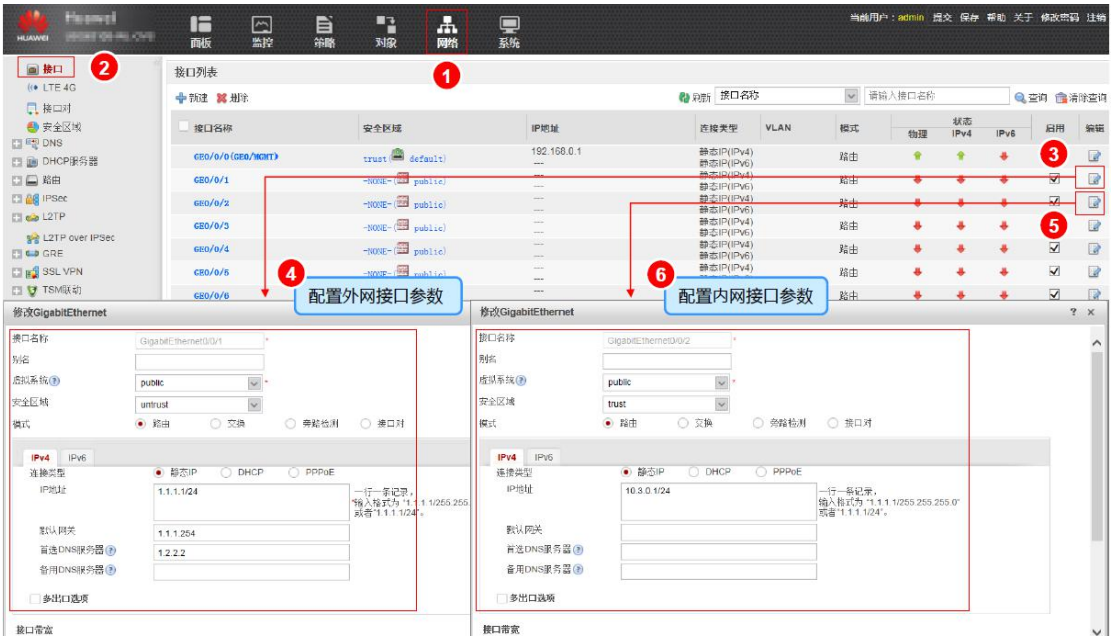
2、 使用网线连接 PC 与 0 接口，登录防火墙 web 界面：

3、防火墙通过静态 IP 接入互联网（网关地址、DNS 服务器地址请向运营商索取）：

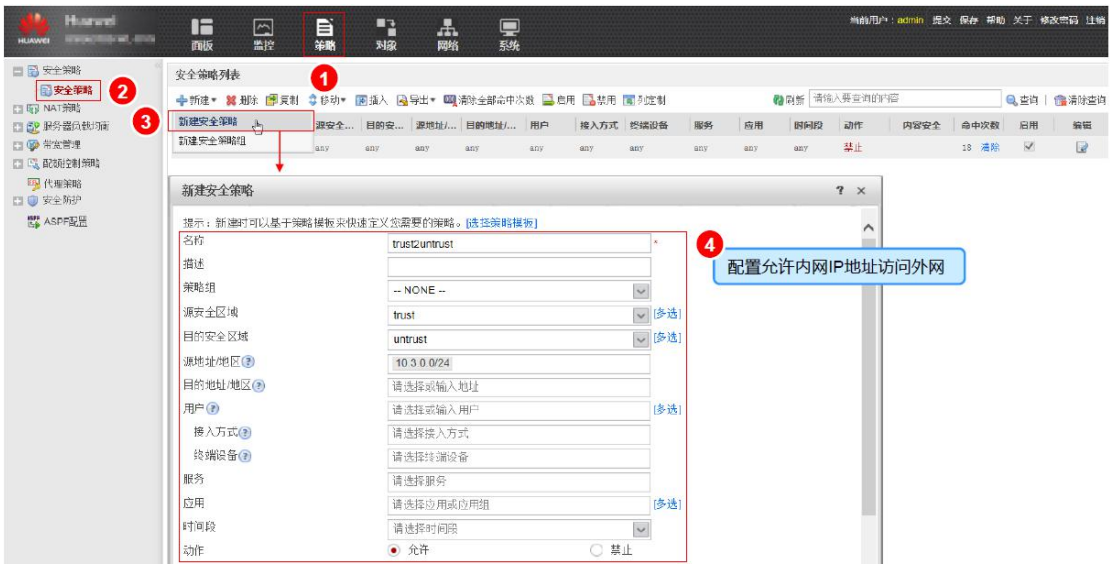


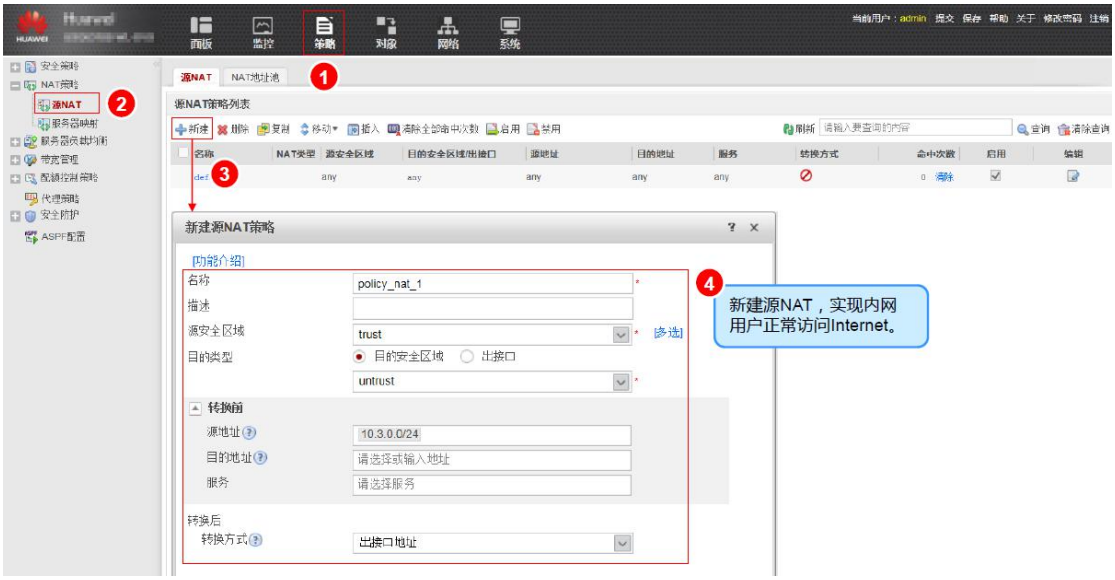
局域网内所有PC都部署在10.3.0.0/24网段，均通过DHCP动态获得IP地址。
企业从运营商处获取的固定IP地址为1.1.1.1/24。企业需利用防火墙接入互联网。

项目	数据	说明
DNS服务器	1.2.2.2/24	向运营商获取。
网关地址	1.1.1.254/24	向运营商获取。



4、开启防火墙 DHCP 服务器：





5、配置防火墙安全策略与源 NAT 以允许内网访问外网：

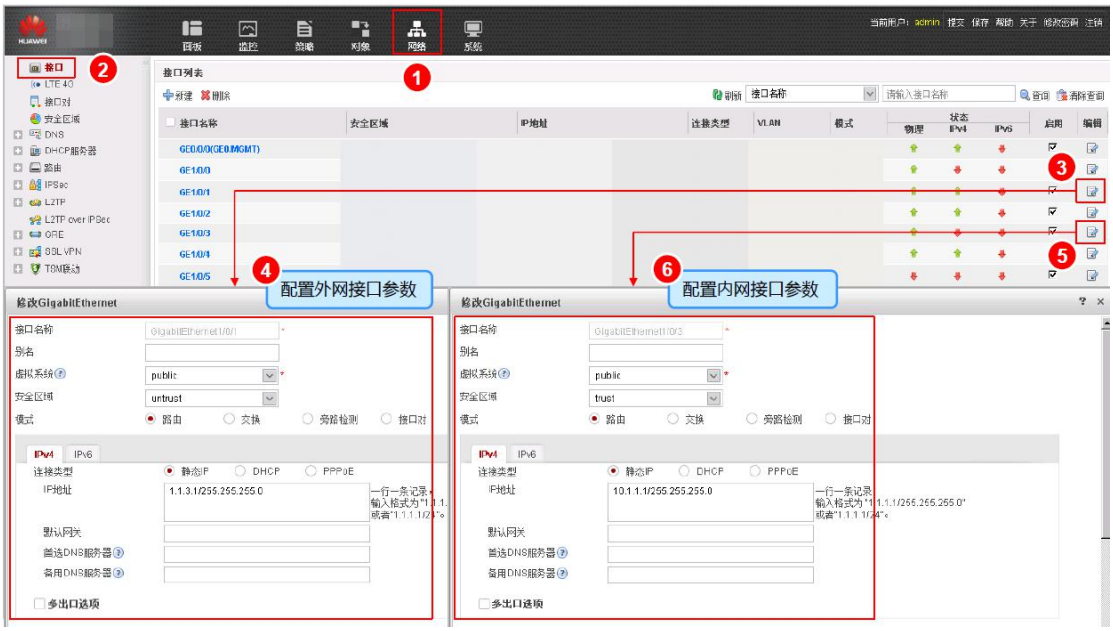
2 在内网PC上执行命令**ipconfig /all**，PC正确分配到IP地址和DNS地址。

```
C:\> ipconfig /all

Windows IP Configuration

        Host Name                       : test
        Primary Dns Suffix  . . . . . . . : test.com
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : test.com
Ethernet adapter 1 :

        Connection-specific DNS Suffix  . : dhcpserver.com
        Description . . . . . . . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-1B-B9-7A-7D-61
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.3.0.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.3.0.1
        DHCP Server . . . . . . . . . . . : 10.3.0.1
        DNS Servers . . . . . . . . . . . : 1.2.2.2
        Lease Obtained. . . . . . . . . . : 2014年10月16日 15:00:00
        Lease Expires . . . . . . . . . . : 2014年10月17日 15:00:00
```

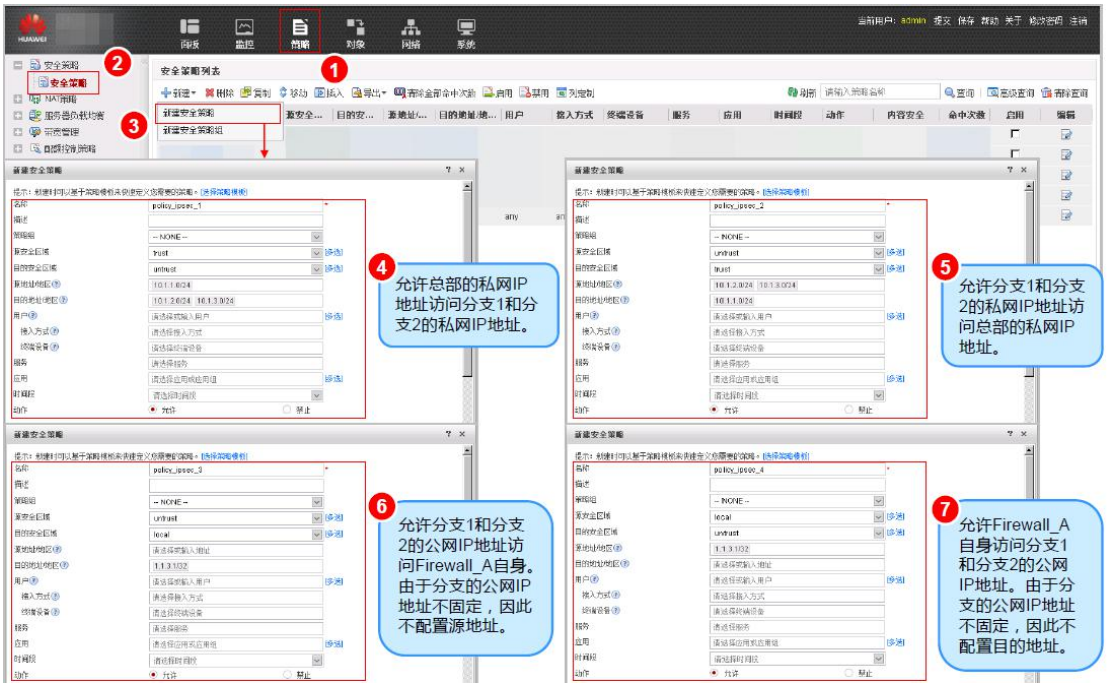
3 局域网内PC能通过域名访问Internet

6、配置点到多点 IPsec 服务器（不指定对端 IP）：

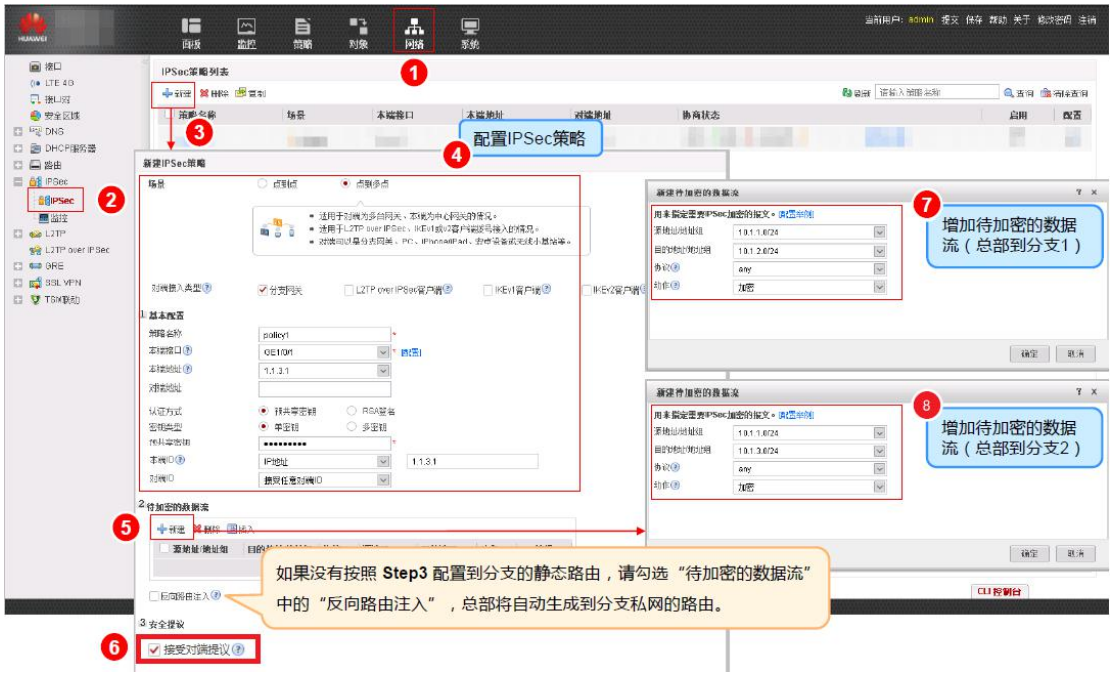
配置内外网接口参数



在策略→安全策略配置安全策略，在网络→路由→静态路由添加路由，允许外部 IPsec 客户端与作为 IPsec 服务器的防火墙和防火墙内网之间通信



7、在网络→IPsec→IPsec→新建配置 IPsec 服务器策略并应用



二、 ORB305 路由器端配置指导：

1、 将 SIM 卡插入路由器卡槽

2、 给设备上电，登入路由器 web 页面（默认为 192.168.2.1）

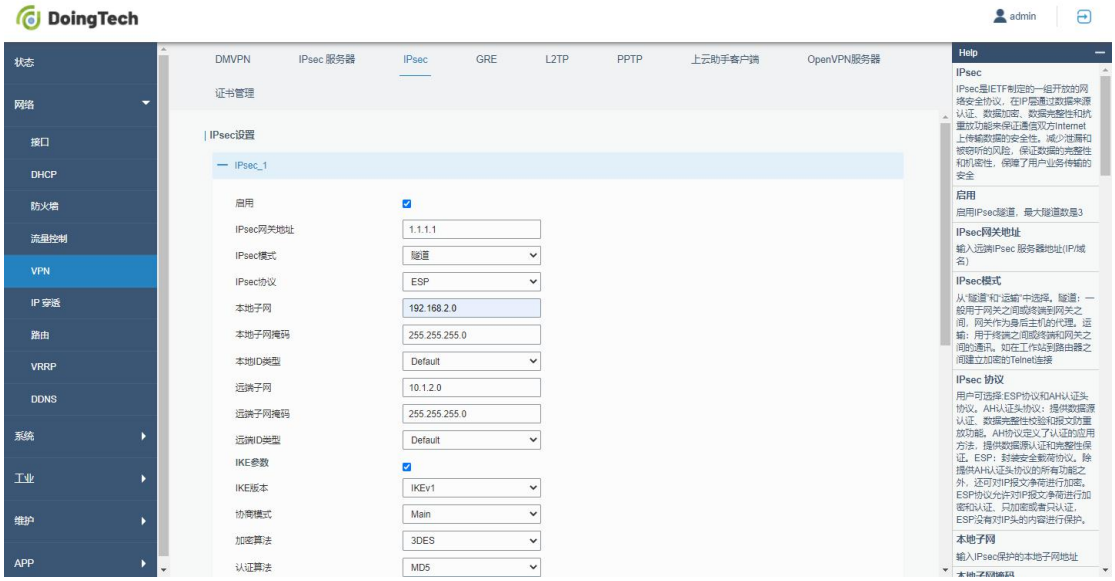
3、 进入网络→接口→连链路备份界面启用对应 SIM 卡并上调链路优先级，保存配置

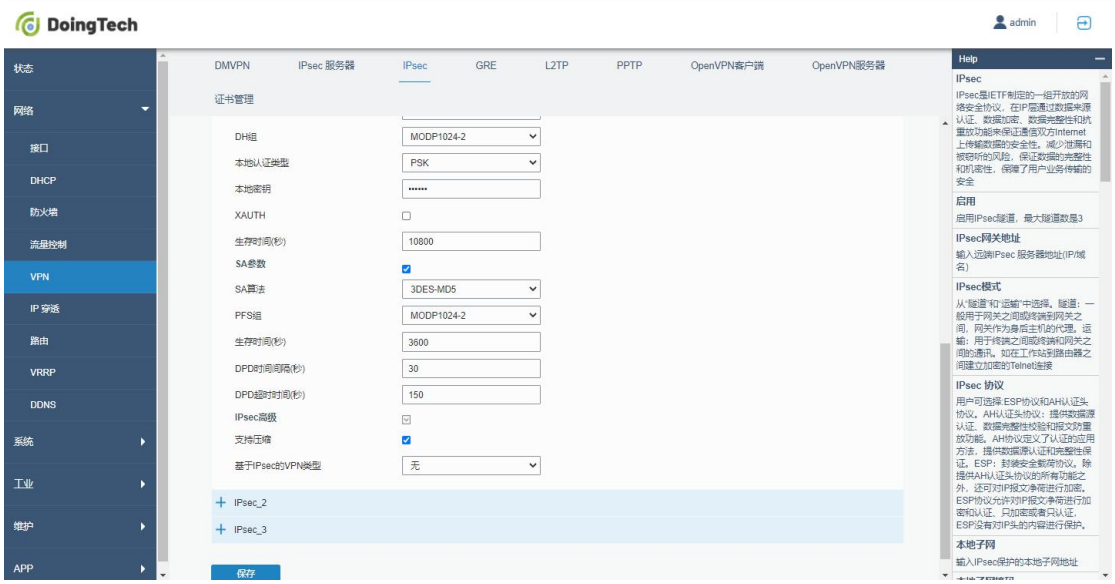
4、 对应 SIM 卡拨号成功，当前链路变为绿色

5、 进入网络→VPN→IPsec 界面进行路由器（IPsec VPN 客户端）配置

IPsec_1 参数配置	
启用	勾选
IPsec 网关地址	填入华为防火墙获得的公网地址（例如 1.1.1.1）
IPsec 模式	隧道（缺省）
IPsec 协议	ESP（缺省）
本地子网	路由器 LAN 口子网（例如 192.168.2.0/24）
本地 ID 类型	Default（缺省）
远端子网	华为防火墙内网地址（例如 10.1.2.0/24）
远端 ID 类型	Default（缺省）
IKE 参数	勾选
IKE 版本	IKEv1（缺省）
协商模式	Main（缺省）
加密算法	3DES
认证算法	MD5
DH 组	MODP1024-2
本地认证类型	PSK（缺省）
本地密钥	填写华为服务器配置 IPsec 策略时设置的密钥
XAUTH	不勾选（缺省）
生存时间（秒）	10800（缺省）
SA 参数	勾选

SA 算法	3DES-MD5
PFS 组	MODP1024-2
生存时间（秒）	3600（缺省）
DPD 时间间隔（秒）	30（缺省）
DPD 超时时间（秒）	150（缺省）
IPsec 高级	展开
支持压缩	勾选
基于 IPsec 的 VPN 类型	无
专家选项	空（缺省）





保存并应用配置后即可进入状态→VPN 页面看到 IPsec VPN 状态为已连接


DoingTech
admin
状态
网络
系统
概况
蜂窝
网络
VPN
路由信息
主机列表
客户端
名称
状态
本地IP
远端IP
ipsec_1
已连接
192.168.2.0/24
10.1.2.0/24
Help
客户端
名称
显示已经启用的VPN客户端的名称
状态
显示开启的客户端是否与服务器连接
本地IP