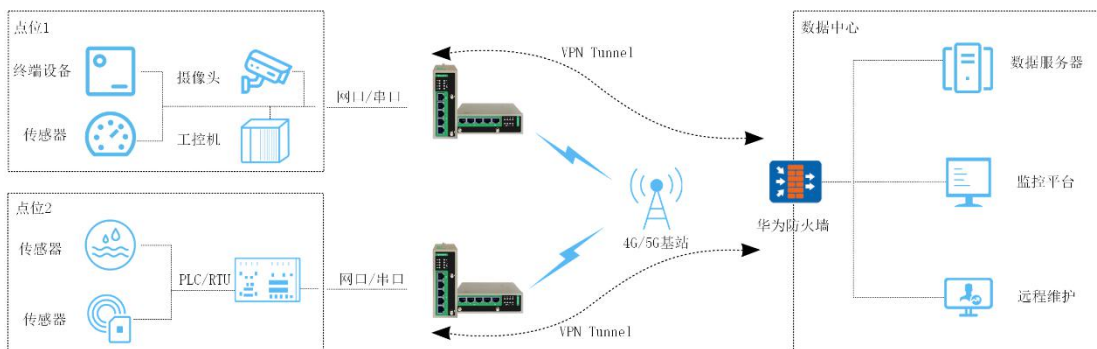


# ORB305 与华为防火墙构建 IPsec VPN 配置指导手册

东用科技有限公司

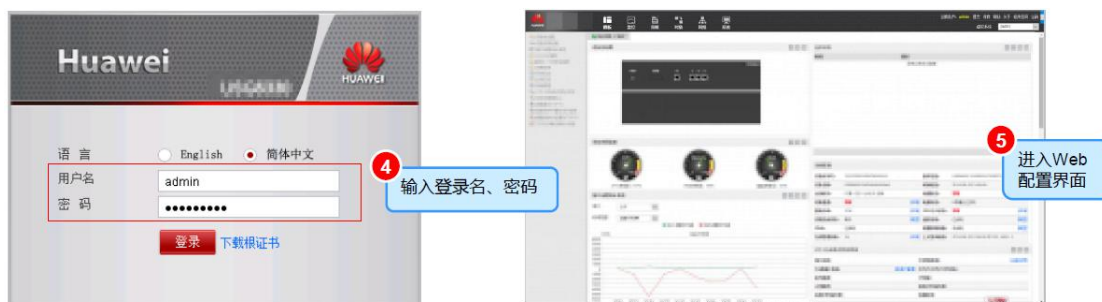
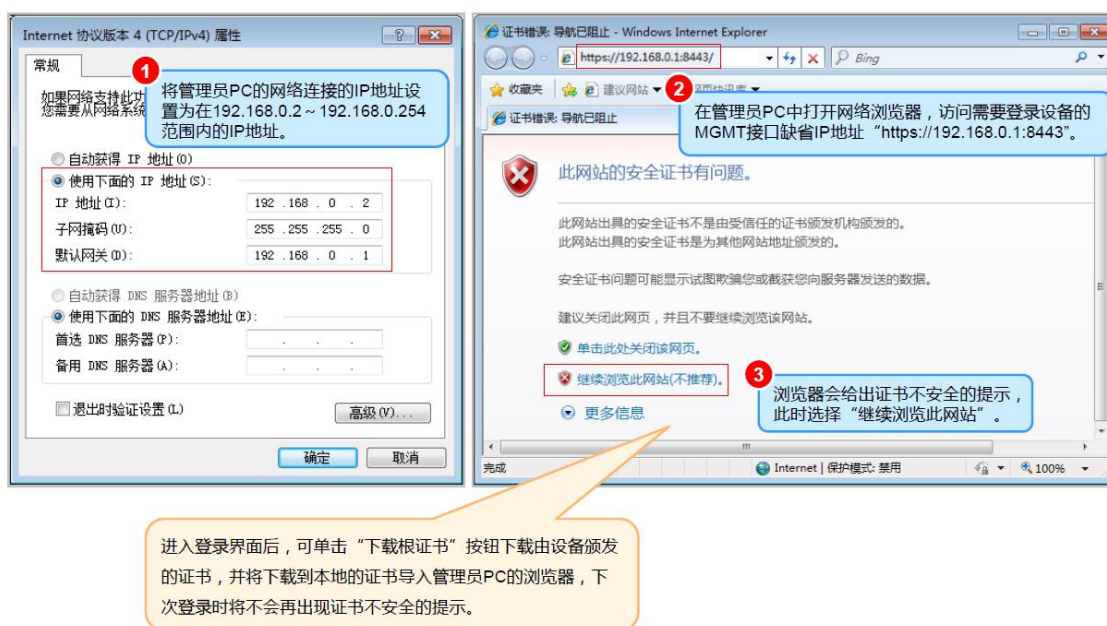
发布日期 2020-08-21



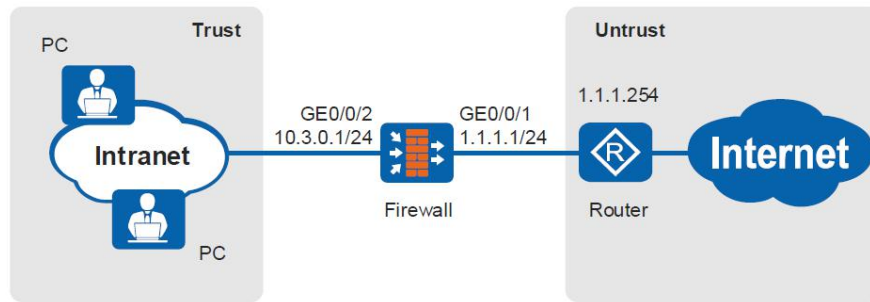
## IPsec VPN 组网拓扑：

### 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。

配置外网接口参数

配置内网接口参数

配置内网接口GE0/0/2的DHCP服务，使其为局域网内的PC分配IP地址。

4、开启防火墙 DHCP 服务器：

The screenshots illustrate the configuration steps for allowing internal network access to the Internet:

- Step 1:** In the 'Security Policy List' (安全策略列表), click 'Add' (新增) to create a new security policy.
- Step 2:** In the 'New Security Policy' (新建安全策略) dialog, configure the policy name to 'trust-untrust' and the description to '配置允许内网IP地址访问外网' (Configure to allow internal network IP addresses to access the Internet).
- Step 3:** In the 'New Source NAT Policy' (新建源NAT策略) dialog, configure the policy name to 'policy\_nat\_1' and the description to '新建源NAT，实现内网用户正常访问Internet。' (New source NAT, enabling normal Internet access for internal network users).
- Step 4:** In the 'Interface List' (接口列表), ensure the physical status and IPv4 status of the GigabitEthernet 0/0/1 interface are 'Up' (indicated by green up arrows).

## 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
```

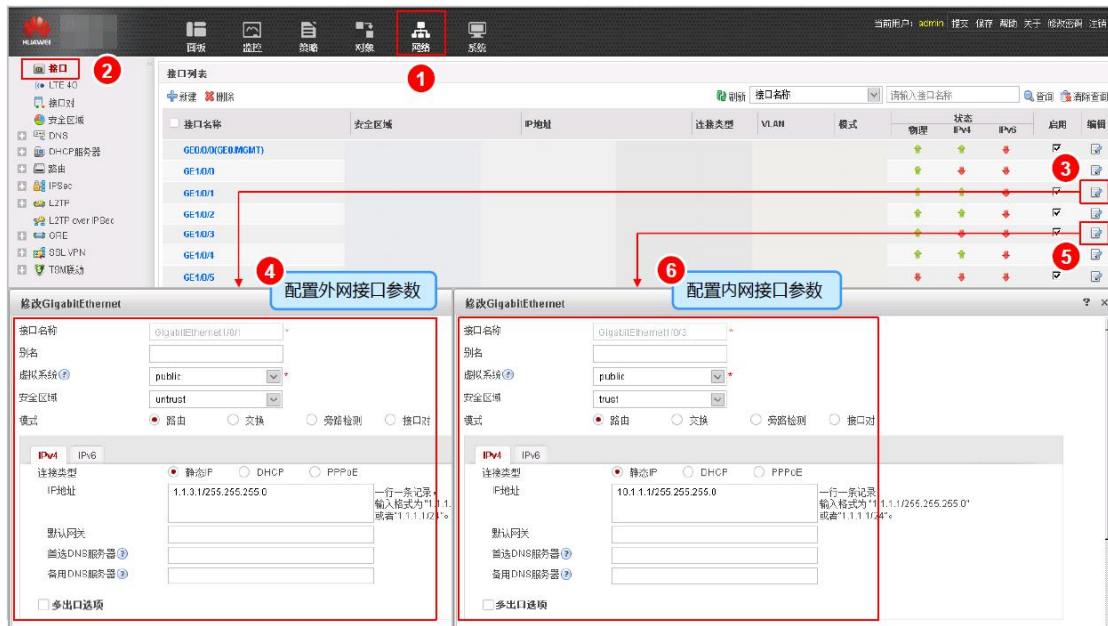
3

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



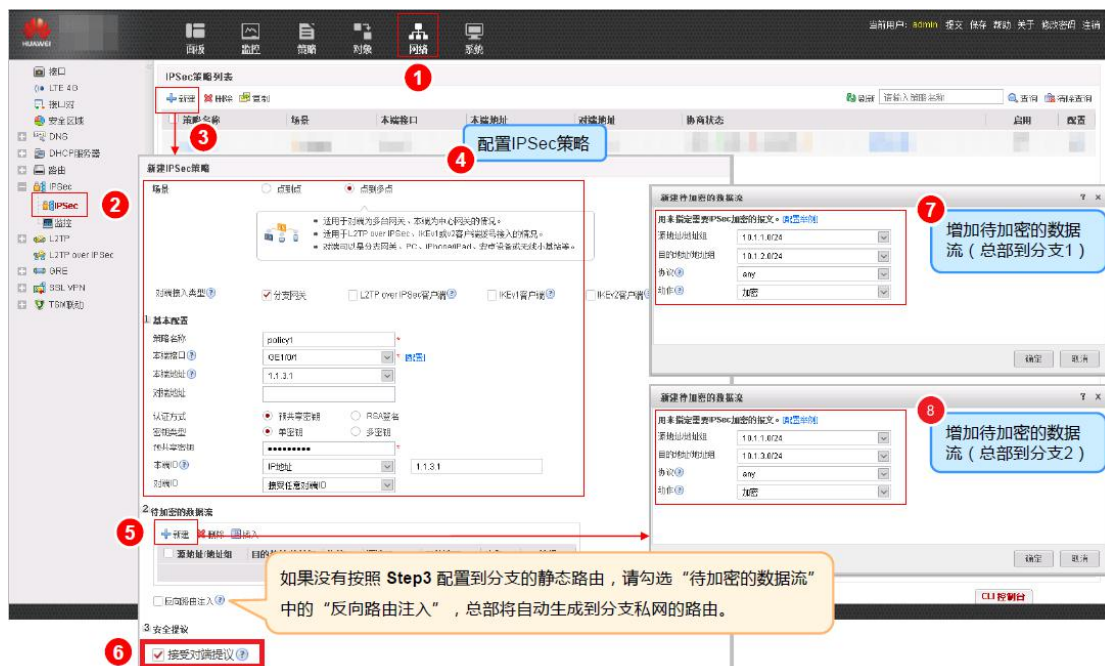


在策略→安全策略配置安全策略，在网络→路由→静态路由添加路由，允许外部 IPsec 客户端与作为 IPsec 服务器的防火墙和防火墙内网之间通信





## 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）

状态 网络 接口 DHCP 防火墙 流量控制 VPN IP 穿越 路由 VRRP DNS 系统 工业 维护 APP

DMVPN IPsec 服务器 IPsec GRE L2TP PPTP 上云助手客户端 OpenVPN 服务器

证书管理

IPsec 设置

IPsec\_1

启用 ☒

IPsec 网关地址 1.1.1.1

IPsec 模式 隧道

IPsec 协议 ESP

本地子网 192.168.2.0

本地子网掩码 255.255.255.0

本地 ID 类型 Default

远端子网 10.1.2.0

远端子网掩码 255.255.255.0

远端 ID 类型 Default

IKE 参数 ☒

IKE 版本 IKEv1

协商模式 Main

加密算法 3DES

认证算法 MD5

Help

IPsec

IPsec 是 IETF 制定的一组开放的网络安全协议。在 IP 层通过数据源认证、数据加密、数据完整性和抗重放功能来保证通信双方 Internet 上传输数据的安全性。减少窃听和篡改的风险。保证数据的完整性和机密性。保障了用户业务传输的安全。

启用

启用 IPsec 隧道。最大隧道数 3

IPsec 网关地址

输入远端 IPsec 服务器地址 (IP 域名)

IPsec 模式

从“隧道”和“远端”中选择。隧道：一般用于网关之间或终端网关之间。网关作为身份主机的代理。远端：用于终端之间或终端和网关之间的通信。如在工作站到路由器之间建立加密的 Telnet 连接。

IPsec 协议

用户可选择 ESP 协议和 AH 认证头协议。AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。AH 协议定义了认证的通用方法，提供数据源认证和完整性保证。ESP：封装安全载荷协议。除提供 AH 认证头协议的所有功能之外，还可对 IP 报文内容进行加密。ESP 协议允许对 IP 报文内容进行加密和认证。只加密或者只认证。ESP 没有对 IP 头的内容进行保护。

本地子网

输入 IPsec 保护的本地子网地址

状态 网络 接口 DHCP 防火墙 流量控制 VPN IP 穿越 路由 VRRP DNS 系统 工业 维护 APP

DMVPN IPsec 服务器 IPsec GRE L2TP PPTP OpenVPN 客户端 OpenVPN 服务器

证书管理

IPsec 设置

IPsec\_1

启用 ☒

IPsec 网关地址 1.1.1.1

IPsec 模式 隧道

IPsec 协议 ESP

本地子网 192.168.2.0

本地子网掩码 255.255.255.0

本地 ID 类型 Default

远端子网 10.1.2.0

远端子网掩码 255.255.255.0

远端 ID 类型 Default

IKE 参数 ☒

IKE 版本 IKEv1

协商模式 Main

加密算法 3DES

认证算法 MD5

Help

IPsec

IPsec 是 IETF 制定的一组开放的网络安全协议。在 IP 层通过数据源认证、数据加密、数据完整性和抗重放功能来保证通信双方 Internet 上传输数据的安全性。减少窃听和篡改的风险。保证数据的完整性和机密性。保障了用户业务传输的安全。

启用

启用 IPsec 隧道。最大隧道数 3

IPsec 网关地址

输入远端 IPsec 服务器地址 (IP 域名)

IPsec 模式

从“隧道”和“远端”中选择。隧道：一般用于网关之间或终端网关之间。网关作为身份主机的代理。远端：用于终端之间或终端和网关之间的通信。如在工作站到路由器之间建立加密的 Telnet 连接。

IPsec 协议

用户可选择 ESP 协议和 AH 认证头协议。AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。AH 协议定义了认证的通用方法，提供数据源认证和完整性保证。ESP：封装安全载荷协议。除提供 AH 认证头协议的所有功能之外，还可对 IP 报文内容进行加密。ESP 协议允许对 IP 报文内容进行加密和认证。只加密或者只认证。ESP 没有对 IP 头的内容进行保护。

本地子网

输入 IPsec 保护的本地子网地址

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

配置

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