

ORB305 与 Cisco ASA 防火墙构建 IPSec 配置指导

北京东用科技有限公司

2020-09-11

前言

声明

- ⊕ 本手册为北京东用科技有限公司及其许可者版权所有,保留一切权利;
- ⊕ 未经本公司书面许可,任何单位和个人不得擅自复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途;
- ⊕ 对于本手册中出现的其它公司的商标、产品标识及商品名称,由各自权利人拥有;
- ⊕ 由于产品版本升级或其他原因,本手册内容有可能变更,北京东用科技保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利;
- ⊕ 本手册仅作为使用指导,东用科技尽全力在本手册中提供准确的信息,但并不确保手册内容完全没有错误;
- ⊕ 本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

修 订 记 录

版本	修订日期	修订说明	执行人
v1.0	2020-04	撰写	技术部

读者对象

本手册适合下列人员阅读:

- ⊕ 东用科技客户方网络工程师
- ⊕ 东用科技内部技术工程师

说明

- ⊕ 本手册举例说明部分的端口类型同实际可能不符,实际操作中需要按照各产品所支持的端口类型进行配置;
- ⊕ 本手册部分举例的显示信息中可能含有其它产品系列的内容 (如产品型号、描述等),具体显示信息请以实际使用的设备信息为准;

目录

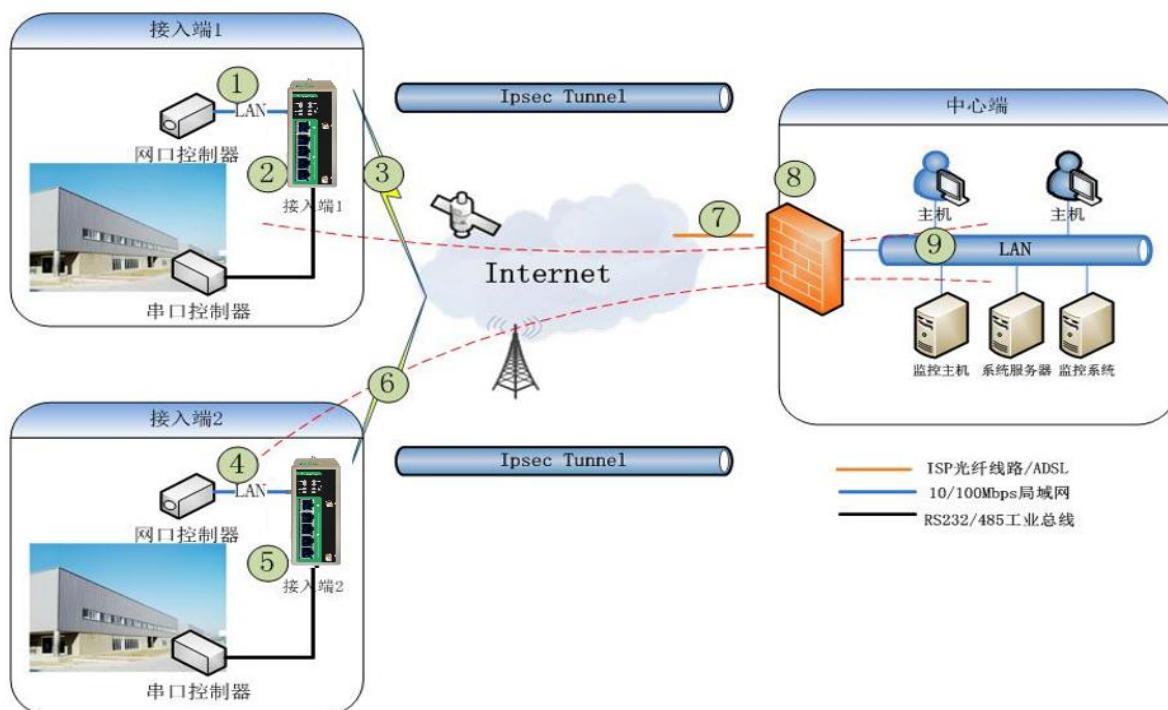
前言	2
1. 概述	5
2. 网络拓扑	5
2.1 网络拓扑	5
2.2 网络拓扑说明	6
3. 配置指导 (一台 ORB305)	6
3.1 中心端 Cisco ASA/PIX 基本配置	6
3.2 远端 ORB305 基本配置	8
3.2.1 远端 ORB305 WAN 口配置	8
3.2.2 远端 ORB305 LAN 口配置	9
3.3 IPSec VPN 配置	10
3.3.1 中心端 Cisco ASA/PIX IPSec VPN 配置	10
3.3.2 ORB305 路由器端配置：	11
3.4 验证	13
3.4.1 中心端验证	13
3.4.2 远端 ORB305 验证	15
4. 配置指导 (多台 ORB305)	16
4.1 中心端 Cisco ASA/PIX 防火墙配置	16
4.2 新增远端 ORB305 配置	16
4.2.1 新增远端 ORB305 WAN 口配置	16
4.2.2 新增远端 ORB305 LAN 口配置	17
4.2.3 新增远端 ORB305 IPSec VPN 配置	18
4.3 验证	20
4.3.1 中心端 Cisco ASA/PIX 防火墙验证	20
4.3.2 远端 ORB305 验证	22
5. 备注	22

1. 概述

本文档主要讲述了关于东用科技路由器 ORB305 与中心端 Cisco ASA/PIX 防火墙构建 LAN-to-LAN VPN 的方法。ORB 全系列产品均支持 VPN 功能，并与众多国际主流中心端设备厂商产品兼容。建立起 LAN-to-LAN VPN 之后便可以实现下位机—路由器 LAN 端与上位机—中心端设备 LAN 进行双向通信。

2. 网络拓扑

2.1 网络拓扑



1	接入端 1 的 LAN 端 IP 地址为 192.168.2.0/24 网段且不与接入端 2 LAN 重复
2	接入端的设备 ORB 系列路由器均支持 IPSec VPN
3	ORB305 通过有线或无线 PPPOE 拨号或固定 IP 形式获取外部 IP 地址

4	接入端 2 的 LAN 端 IP 地址为 192.168.3.0/24 网段且不与接入端 1 LAN 重复
5	接入端的设备 ORB 系列路由器均支持 IPSec VPN
6	ORB305 通过有线或无线 PPPOE 拨号或固定 IP 形式获取外部 IP 地址
7	中心端设备必须采用固定 IP 地址。地址为 173.17.99.100/24
8	中心端设备可以采用 cisco, juniper, 华为, H3C 等国际知名厂商支持 IPSec 的设备
9	中心端 LAN 端 IP 地址为 172.16.1.0/24 且不与建立通道的任何 LAN 重复

2.2 网络拓扑说明

- ⊕ 中心端设备为 Cisco ASA/PIX 防火墙, IOS 版本 8.0; 外部 IP 地址 173.17.99.100, 掩码 255.255.255.0; 内部 IP 地址 172.16.1.1, 掩码 255.255.255.0
- ⊕ 接入端 1 设备为 ORB305; 外部 IP 地址 193.169.99.100, 掩码 255.255.255.0; 内部 IP 地址 192.168.2.1, 掩码 255.255.255.0
- ⊕ 接入端 2 设备为 ORB305; 外部 IP 地址 193.169.99.101, 掩码 255.255.255.0; 内部 IP 地址 192.168.3.1, 掩码 255.255.255.0

3.配置指导

3.1 中心端 Cisco ASA/PIX 基本配置

Ciscoasa&pix#configure terminal //进入配置模式

Ciscoasa&pix(config)# interface ethernet 0/1 //进入内部接口的配置模式 (端口类型及端口号)

请以现场设备为准, 内部或外部接口可自行选择)

Ciscoasa&pix(config-if)#nameif inside //为内部接口关联一个 inside 的名称

Ciscoasa&pix(config-if)#ip address 172.16.1.1 255.255.255.0 //为内部接口配置 IP 地址

```
Ciscoasa&pix(config-if)#exit          //退出内部接口的配置模式

Ciscoasa&pix(config)# interface ethernet 0/0 //进入外部接口的配置模式 (端口类型及端口号  
请以现场设备为准，内部或外部接口可自行选择)

Ciscoasa&pix(config-if)#nameif outside      //为外部接口关联一个 outside 的名称

Ciscoasa&pix(config-if)#ip address 173.17.99.100 255.255.255.0 //为外部接口配置 IP 地址

Ciscoasa&pix(config-if)#exit          //退出外部接口的配置模式

Ciscoasa&pix(config)#route outside 0.0.0.0 0.0.0.0 173.17.99.1 //配置静态默认路由，  
173.17.99.1 为外部接口的网关地址，该地址一般为 ISP 提供

Ciscoasa&pix(config)#access-list permiticmp extended permit icmp any any //创建访问控制  
列表允许所有 icmp 报文，此条访问控制列表的目的是为了测试或排障时使用 ping 命令（防火墙默  
认是禁止任何 ICMP 包通过的）

Ciscoasa&pix(config)#access-group permiticmp in interface outside      //将访问控制列表应  
用到外部接口

Ciscoasa&pix(config)#access-list nonat extended permit ip 172.16.1.0 255.255.255.0  
192.168.2.0 255.255.255.0 //创建访问控制列表允许 172.16.1.0/24 网络到 192.168.2.0/24 网络，  
此条访问控制列表的目的是对 172.16.1.0/24 网络到 192.168.2.0/24 网络的数据包 IP 字段不进行地  
址转换(PAT)，172.16.1.0/24 是中心端内部网络，192.168.2.0/24 是远端内部网络

Ciscoasa&pix(config)#global (outside) 1 interface      //在外部接口(outside)上启用 PAT

Ciscoasa&pix(config)#nat (inside) 0 access-list nonat //对从内部接口进入的且匹配 nonat 访问  
控制列表的数据包 IP 字段不进行地址转换 (PAT)，序列号 0 代表不转换

Ciscoasa&pix(config)#nat (inside) 1 172.16.1.0 255.255.255.0 //对从内部接口进入的源地址为  
172.16.1.0/24 的数据包 IP 字段进行地址转换 (PAT)。注：防火墙在收到内部接口进入的数据包后会  
检查 IP 字段，并按照 NAT 条件顺序进行地址转换
```

Ciscoasa&pix(config)#write memory //保存配置

3.2 远端 ORB305 基本配置

3.2.1 远端 ORB305 WAN 口配置 (如无 WAN 口或采用 4G 拨号则跳过此步骤)

接通 ORB305 电源，用一根网线连接 ORB305 的 LAN 口和 PC，打开浏览器，输入网址 192.168.2.1 进入 ORB305web 页面，用户名 admin，密码 admin 点击登录。

进入“网络”->“接口”->“链路备份”将接口 WAN 链路勾选启用并将优先级置顶（此处以静态 IP 为例，其他拨号类型请参阅 ORB305-4G 系列工业路由器快速安装手册）。

优先级	启用规则	当前链路	接口	连接类型	IP	操作
1	<input checked="" type="checkbox"/>	●	WAN	静态IP	-	<input type="button"/> <input type="button"/> <input type="button"/>
2	<input checked="" type="checkbox"/>	●	Cellular-SIM1	DHCP	-	<input type="button"/> <input type="button"/> <input type="button"/>
3	<input checked="" type="checkbox"/>	●	Cellular-SIM2	-	-	<input type="button"/> <input type="button"/> <input type="button"/>

设置

恢复间隔: 300 秒
链路异常则重启:

保存

Help

- 启用: 启用链路Ping探测后，路由器会阶段性探测链路的连接状态。
- 目的地址(IPv4): 路由器 ping 主地址/域名来检测当前连接是否存活。
- 首选目的地址(IPv4): 路由器 ping 首用地址/域名来检测当前连接是否存在。
- Ping间隔: 路由器每隔一个Ping间隔对目的地址进行Ping探测。
- Ping重试间隔: 设置 Ping 的重试间隔时间，当 Ping 失败后，路由器每隔一个 Ping 重试间隔再重新 Ping。
- Ping超时: 发送Ping命令后等待应答的超时时间。
- 最大重试次数: 连续Ping失败并达到最大重试次数。

进入“广域网”选择拨号类型为“静态 IP”并配置 IP 地址以及其它网口信息。

Help

- 启用
- 启用WAN功能
- 网口
- 当前设置为WAN口的以太网口
- 拨号类型
- 选择WAN口上网的方式。可选静态地址、DHCP客户机、PPPoE
- IPv4地址
- 设置可以访问互联网的IPv4地址，如192.168.1.2
- 子网掩码
- 设置WAN口的子网掩码。如果子网掩码填的是IPv4地址(Pv4)的格式，则访问网络是优先使用IPv4(Pv4)的地址。
- IPv4网关
- 设置WAN口的IPv4地址的网关
- IPv6地址
- 设置可以访问互联网的IPv6地址，默认地址为：路由器根据WAN口MAC地址生成的IPv6地址
- 前缀长度
- 设置IPv6前缀长度以标识网段中全局单播IPv6地址的位数。如，在2001:0D88:0000:0000::/64中，64用来标识在该网段中的前64位。
- IPv6网关

3.2.2 远端 ORB305 LAN 口配置

进入“网络”->“接口”->“网桥”如图使用缺省配置即可。

Help

- 网桥设置
- 名称
- 显示网桥名称，默认为Bridge0且不可更改
- STP
- 开启/关闭STP
- IP地址
- 设置网桥的IP地址
- 子网掩码
- 设置网桥的子网掩码

至此 ORB305 基本配置完成

3.3 IPSec VPN 配置

3.3.1 中心端 Cisco ASA/PIX IPSec VPN 配置

```
Ciscoasa&pix# configure terminal
```

```
Ciscoasa&pix(config)#isakmp enable outside //在外部接口 (outside) 开启 isakmp.
```

```
Ciscoasa&pix(config)#crypto isakmp policy 10 //定义 IKE 策略优先级 (1 为优先级)
```

```
Ciscoasa&pix(config-isakmp-policy)## encr 3des //定义加密算法
```

```
Ciscoasa&pix(config-isakmp-policy)# hash md5 //定义散列算法
```

```
Ciscoasa&pix(config-isakmp-policy)# authentication pre-share //定义认证方式
```

```
Ciscoasa&pix(config-isakmp-policy)# group 2 //定义密钥交换协议/算法标示符
```

```
Ciscoasa&pix(config-isakmp-policy)#exit //退出 IKE 策略配置模式
```

```
Ciscoasa&pix(config)#crypto IPSec transform-set cisco esp-3des esp-md5-hmac // 创建  
IPSec 转换集 cisco
```

```
Ciscoasa&pix(config)#crypto isakmp nat-traversal //开启防火墙的 NAT-T 功能
```

```
Ciscoasa&pix(config)#crypto dynamic-map dymap 1 set transform-set cisco //创建动态映射  
dymap 并关联转换集, 1 为序列号
```

```
Ciscoasa&pix(config)#crypto dynamic-map dymap 1 set reverse-route //为动态映射开启  
RRI (reverse-route injection) 反向路由注入
```

```
Ciscoasa&pix(config)#crypto dynamic-map dymap 1 match address nonat //为动态映射关  
联兴趣流量
```

```
Ciscoasa&pix(config)#crypto dynamic-map dymap 1 set pfs group2 //为动态映射开  
启 pfs (perfect forward secrecy) 完美向前加密
```

```
Ciscoasa&pix(config)#crypto map finalmap 10 IPSec-isakmp dynamic dymap //创建映射并调
```

用动态映射

```
Ciscoasa&pix(config)#crypto map finalmap interface outside //在外部接口(outside)上应
```

用映射

```
Ciscoasa&pix(config)#tunnel-group-map default-group DefaultL2LGroup //创建默认隧道组
```

```
Ciscoasa&pix(config)#tunnel-group DefaultL2LGroup IPSec-attributes //进入默认隧道组配
```

置模式

```
Ciscoasa&pix(config-tunnel-IPSec)# pre-shared-key cisco //设置默认隧道组的与共享
```

密钥

```
Ciscoasa&pix(config-tunnel-IPSec)# exit //退出默认隧道组配置模式
```

```
Ciscoasa&pix#write memory //保存配置
```

至此中心端 Cisco ASA/PIX 防火墙 IPSec VPN 配置结束

3.3.2 ORB305 路由器端配置：

- 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	填入思科防火墙的公网地址（例如 173.17.99.100）
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	填写中心端内网地址（例如 172.16.1.0/24）
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	填写思科防火墙配置 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）

IPsec 是 IETF 制定的一组开放的网络安全协议。在 IP 层通过数据报头源认证、数据加密、数据完整性检查以及对称密钥保证通信双方 Internet 上传输的数据是安全的，减少了因窃听和中间人攻击而造成的安全隐患。IPsec 提供了用户业务操作的安全。

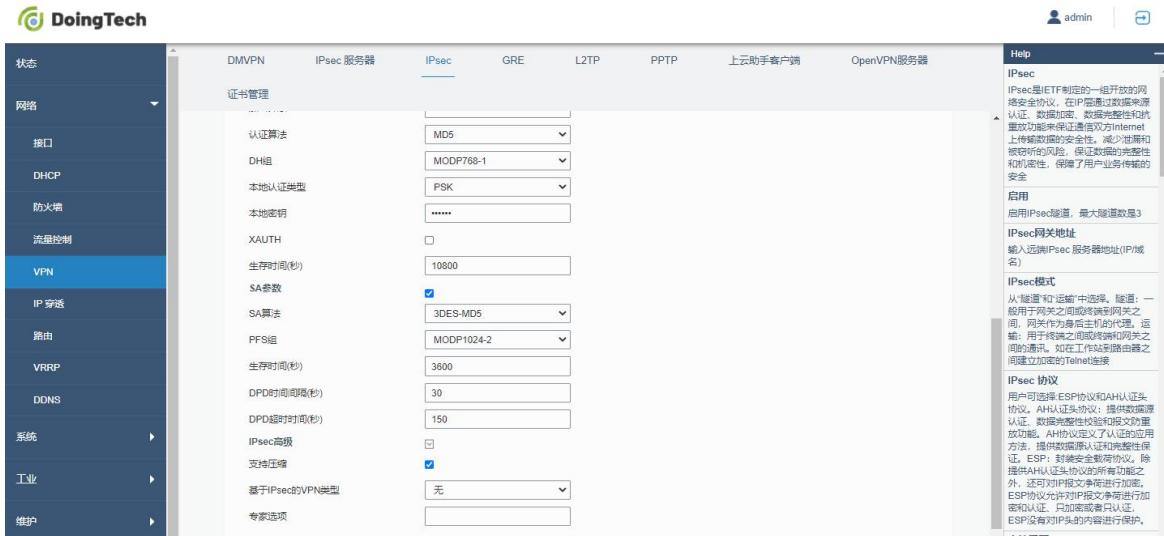
启用 IPsec 隧道，最大隧道数是 3。

IPsec 网关地址：输入远端 IPsec 服务器地址 (IP 地址或域名)。

IPsec 模式：从“隧道”和“运输”中选择。隧道：一般用于两个网关之间或网关到网关之间，网关作为两端主机的代理。运输：用于终端之间或终端到网关之间的通信。如果工作站到路由器之间建立隧道的话则使用隧道。

IPsec 协议：用户可以选择 ESP 协议和 AH 协议。AH 协议定义了认证的功能，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 协议头协议的所有功能之外，还可对对文件进行加密。ESP 支持多种加密算法，如 DES、3DES 和 AES 加密和认证，只支持密钥认证。ESP 会对 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



3.4 验证

3.4.1 中心端验证

Ciscoasa&pix(config)# show crypto isakmp sa

Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

1 IKE Peer: 193.169.99.100

Type : L2L Role : responder

Rekey : no State : MM_ACTIVE

如果出现上述显示则表示第一阶段协商成功

Ciscoasa&pix(config)# show crypto IPSec sa

interface: outside

Crypto map tag: dymp, seq num: 1, local addr: 173.17.99.100

access-list nonat permit ip 172.16.1.0 255.255.255.0 192.168.2.0 255.255.255.0

local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)

current_peer: 193.169.99.100

#pkts encaps: 105, #pkts encrypt: 105, #pkts digest: 105

#pkts decaps: 105, #pkts decrypt: 105, #pkts verify: 105

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 105, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#send errors: 0, #recv errors: 0

local crypto endpt.: 173.17.99.100, remote crypto endpt.: 193.169.99.100

path mtu 1500, IPSec overhead 58, media mtu 1500

current outbound spi: 1B7B60FB

inbound esp sas:

spi: 0xF33099AA (4080048554)

transform: esp-3des esp-md5-hmac none

in use settings ={L2L, Tunnel, PFS Group 2, }

slot: 0, conn_id: 12288, crypto-map: dymp

sa timing: remaining key lifetime (sec): 3493

IV size: 8 bytes

replay detection support: Y

outbound esp sas:

spi: 0x1B7B60FB (461070587)

transform: esp-3des esp-md5-hmac none

in use settings ={L2L, Tunnel, PFS Group 2, }

slot: 0, conn_id: 12288, crypto-map: dymap

sa timing: remaining key lifetime (sec): 3493

IV size: 8 bytes

replay detection support: Y

如出现上述显示则表示第二阶段协商成功，IPSec VPN 建立成功

3.4.2 远端 ORB305 验证

The screenshot shows the DoingTech web interface with the following details:

- Header:** DoingTech, admin, Help.
- Left Sidebar:** 状态, 网络, 系统.
- Top Navigation:** 概况, 蜂窝, 网络, **VPN**, 路由信息, 主机列表.
- Main Content:**
 - 客户端:** 表格列出了一个连接：

名称	状态	本地IP	远端IP
ipsec_1	已连接	192.168.2.0/24	172.16.1.1/24
- Right Sidebar (Help):**
 - 客户端:** 显示已经启用的VPN客户端的名称.
 - 名称:** 显示开启的客户端是否与服务器连接.
 - 状态:** 显示开启的客户端是否与服务器连接.
 - 本地IP:** 显示本地IP.

4. 配置指导 (多台 ORB305)

4.1 中心端 Cisco ASA/PIX 防火墙配置

只需增加一条访问控制列表，对中心端内网 172.16.1.0/24 网络到新增加的远端 ORB305 内网 192.168.3.0/24 网络的数据包 IP 字段不进行地址转换(PAT)，其他无需更改。

```
Ciscoasa&pix(config)#access-list nonat extended permit ip 172.16.1.0  
255.255.255.0 192.168.3.0 255.255.255.0
```

4.2 新增远端 ORB305 配置

4.2.1 新增远端 ORB305 WAN 口配置 (如无 WAN 口或采用 4G 拨号则跳过此步骤)

接通 ORB305 电源，用一根网线连接 ORB305 的 LAN 口和 PC，打开浏览器，输入 <http://192.168.3.1>，输入用户名 admin, 密码 admin

进入“网络”->“接口”->“链路备份”将接口 WAN 链路勾选启用并将优先级置顶（此处以静态 IP 为例，其他拨号类型请参阅 ORB305-4G 系列工业路由器快速安装手册）。

The screenshot shows the 'Link Backup' configuration page. On the left sidebar, '接口' (Interface) is selected. The main area displays a table with columns: 优先级 (Priority), 启用规则 (Enable Rule), 当前链路 (Current Link), 接口 (Interface), 连接类型 (Connection Type), IP, and 操作 (Operations). The table contains three rows:

优先级	启用规则	当前链路	接口	连接类型	IP	操作
1	<input checked="" type="checkbox"/>	●	WAN	静态IP	-	编辑 ↑ ↓
2	<input checked="" type="checkbox"/>	●	Cellular-SIM1	DHCP	-	编辑 ↑ ↓
3	<input checked="" type="checkbox"/>	●	Cellular-SIM2	-	-	编辑 ↑ ↓

右侧的 'Help' pane provides detailed explanations for various settings like 'Ping间隔' (Ping Interval) and 'Ping超时' (Ping Timeout).

进入“广域网”选择拨号类型为“静态 IP”并配置 IP 地址以及其它网口信息。

The screenshot shows the 'WAN' configuration page. On the left sidebar, '广域网' (WAN) is selected. The main area displays a configuration form for 'WAN_1'. The '接口' (Interface) dropdown is set to 'LAN1/WAN'. The '拨号类型' (Modem Type) dropdown is set to '静态IP地址' (Static IP Address). Other fields include:

- IPV4地址: 193.169.99.101
- 子网掩码: 255.255.255.0
- IPV4网关: 193.169.99.1
- IPV6 地址: fe80::26e1:24ff:fe12:9464
- 前缀长度: 64
- IPV6 网关: (empty)
- 最大传输单元: 1500
- 首选DNS: 8.8.8.8
- 备用DNS: (empty)
- 启用NAT:

右侧的 'Help' pane provides detailed explanations for various settings like 'IPV4地址' (IPV4 Address) and 'IPV6地址' (IPV6 Address).

4.2.2 新增远端 ORB305 LAN 口配置

进入“网络”->“接口”->“网桥”配置如图。

The screenshot shows the 'Bridge' configuration page. On the left sidebar, '网桥' (Bridge) is selected. The main area displays a configuration form for 'Bridge0'. The '名称' (Name) field is set to 'Bridge0'. Other fields include:

- STP:
- IP地址: 192.168.3.1
- 子网掩码: 255.255.255.0
- 最大传输单元 (MTU): 1500

右侧的 'Help' pane provides detailed explanations for various settings like '名称' (Name) and 'IP地址' (IP Address).

至此 ORB305 基本配置完成

4.2.3 新增远端 ORB305 IPSec VPN 配置

- 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	填入思科防火墙的公网地址（例如 173.17.99.100）
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 192.168.3.0/24）
本地 ID 类型	Default（缺省）
远端子网	填写中心端内网地址（例如 172.16.1.0/24）
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	填写思科防火墙配置 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)

IPsec_1 configuration details:

- 启用: 启用
- IPsec网关地址: 173.17.99.100
- IPsec模式: 路由
- IPsec协议: ESP
- 本地子网: 192.168.3.0
- 本地网掩码: 255.255.255.0
- 本地ID类型: Default
- 远端子网: 172.16.1.0
- 远端网掩码: 255.255.255.0
- 远端ID类型: Default
- IKE参数: IKEv1
- 协商模式: Main
- 加密算法: DES
- 认证算法: MD5

IPsec_1 configuration details (more advanced options):

- 认证算法: MD5
- DH组: MODP1024-2
- 本地认证类型: PSK
- 本地密钥: (redacted)
- XAUTH: (unchecked)
- 生存时间(秒): 10800
- SA参数: 启用
- SA算法: 3DES-MD5
- PFS组: MODP1024-2
- 生存时间(秒): 3600
- DPD时间间隔(秒): 30
- DPD超时时间(秒): 150
- IPsec高级: 展开
- 支持压缩: 勾选
- 基于IPsec的VPN类型: 无
- 专家选项: 空

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

名称	状态	本地IP	远端IP
ipsec_1	已连接	192.168.3.0/24	172.16.1.1/24

4.3 验证

4.3.1 中心端 Cisco ASA/PIX 防火墙验证

```
Ciscoasa&pix(config)# show crypto isakmp sa
```

```
Active SA: 2
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2
1  IKE Peer: 193.169.99.100 //此处显示已与原远端 ORB305 建立 IKE 第一阶段连接
    Type      : L2L          Role      : responder
    Rekey     : no           State     : MM_ACTIVE
2  IKE Peer: 193.169.99.101 //此处显示已与新增远端 ORB305 建立 IKE 第一阶段连接
    Type      : L2L          Role      : responder
    Rekey     : no           State     : MM_ACTIVE
```

```
Ciscoasa&pix(config)# show crypto IPSec sa
```

```
interface: outside
```

```
Crypto map tag: dymap, seq num: 1, local addr: 173.17.99.100
  access-list nonat permit ip 172.16.1.0 255.255.255.0 192.168.2.0 255.255.255.0
  local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
  current_peer: 193.169.99.100
  #pkts encaps: 49, #pkts encrypt: 49, #pkts digest: 49
  #pkts decaps: 49, #pkts decrypt: 49, #pkts verify: 49
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 49, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 173.17.99.100, remote crypto endpt.: 193.169.99.100
```

```
path mtu 1500, IPSec overhead 58, media mtu 1500
```

```
current outbound spi: B3975F0E
```

```
inbound esp sas:
```

```
  spi: 0xA2A296A4 (2728564388)
    transform: esp-3des esp-md5-hmac none
    in use settings ={L2L, Tunnel, PFS Group 2, }
    slot: 0, conn_id: 53248, crypto-map: dymap
    sa timing: remaining key lifetime (sec): 3312
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
```

```
spi: 0xB3975F0E (3013041934)
    transform: esp-3des esp-md5-hmac none
    in use settings ={L2L, Tunnel, PFS Group 2, }
    slot: 0, conn_id: 53248, crypto-map: dymp
    sa timing: remaining key lifetime (sec): 3312
    IV size: 8 bytes
    replay detection support: Y
Crypto map tag: dymp, seq num: 1, local addr: 173.17.99.100
    access-list nonat permit ip 172.16.1.0 255.255.255.0 192.168.3.0 255.255.255.0
    local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
    current_peer: 193.169.99.101
    #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
    #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #send errors: 0, #recv errors: 0
    local crypto endpt.: 173.17.99.100, remote crypto endpt.: 193.169.99.101
    path mtu 1500, IPSec overhead 58, media mtu 1500
    current outbound spi: 4B25DDD8
inbound esp sas:
    spi: 0x432AD3E6 (1126880230)
        transform: esp-3des esp-md5-hmac none
        in use settings ={L2L, Tunnel, PFS Group 2, }
        slot: 0, conn_id: 57344, crypto-map: dymp
        sa timing: remaining key lifetime (sec): 3392
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
    spi: 0x4B25DDD8 (1260772824)
        transform: esp-3des esp-md5-hmac none
        in use settings ={L2L, Tunnel, PFS Group 2, }
        slot: 0, conn_id: 57344, crypto-map: dymp
        sa timing: remaining key lifetime (sec): 3391
        IV size: 8 bytes
        replay detection support: Y
```

上述显示中心端 Cisco ASA/PIX 防火墙与两台远端 ORB305 建立的 IPSec vpn 工作正常

4.3.2 远端 ORB305 验证

第一台远端 ORB305



The screenshot shows the DoingTech management interface. The left sidebar has '状态' (Status), '网络' (Network) selected, and '系统' (System). The top navigation bar includes '概览' (Overview), '端口' (Ports), '网络' (Network), 'VPN' (selected), '路由信息' (Route Information), and '主机列表' (Host List). On the right, a 'Help' panel is open with sections for '客户端' (Client), '名称' (Name), '显示已经启用的VPN客户端的名称' (Display names of enabled VPN clients), '状态' (Status), '显示开启的客户端是否与服务器连接' (Display if client is connected to server), and '本地IP' (Local IP). The main content area shows a table for '客户端' (Clients) with columns: 名称 (Name), 状态 (Status), 本地IP (Local IP), and 远端IP (Remote IP). One entry is listed: ipsec_1, 已连接 (Connected), 192.168.2.0/24, 172.16.1. /24.

第二台远端 ORB305



This screenshot is identical to the one above, showing the DoingTech interface with the 'Network' tab selected. The 'Help' panel is also visible, and the '客户端' table shows the same connection information for 'ipsec_1': 已连接 (Connected), 192.168.3.0/24, 172.16.1. /24.

5. 备注

- ⊕ 中心 Cisco ASA/PIX 防火墙的 IOS 版本要求高于 8.0 且须支持 IPSec VPN；
- ⊕ 中心端外部接口建议采用静态 IP 地址, 如采用拨号方式可获取固定 IP 地址也可；
- ⊕ 远端 IP 地址采用静态和动态均可。