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

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;

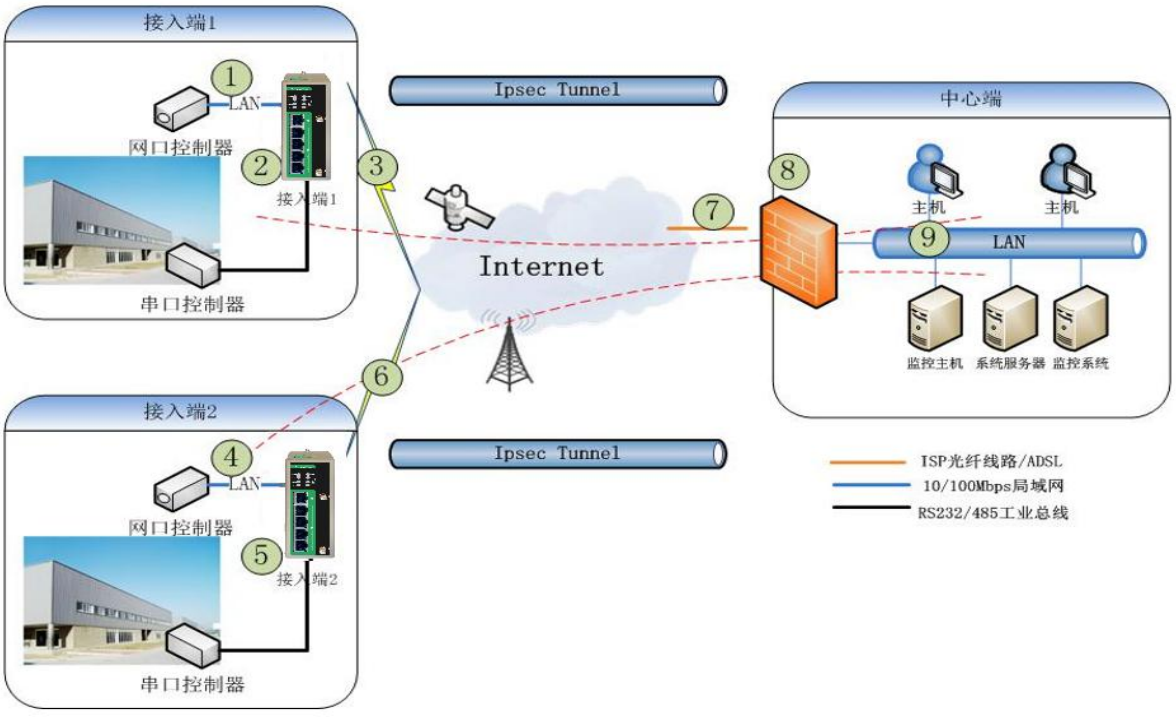
目录

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 2LAN 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 1LAN 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

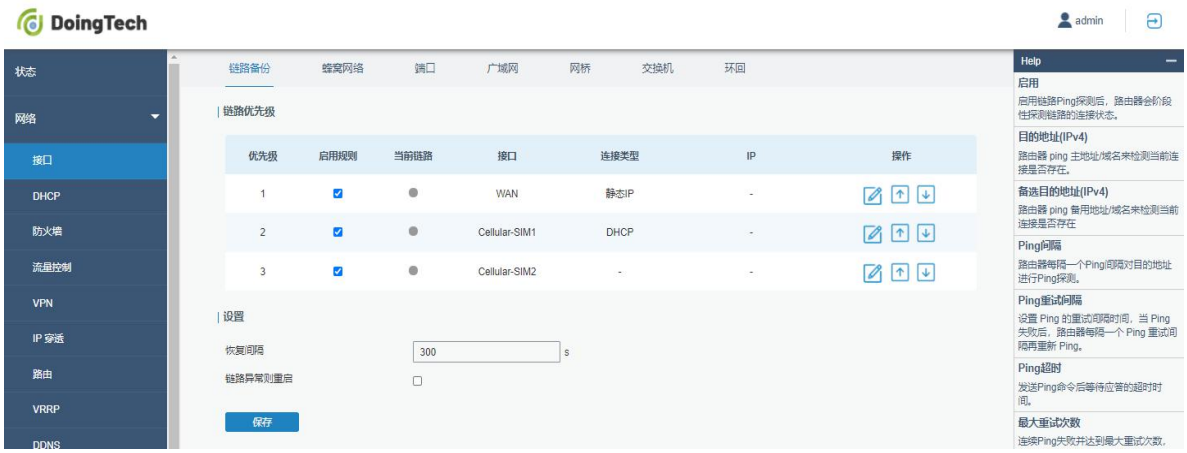
Ciscoasa&pix(config)#write memory //保存配置

3.2 远端 ORB305 基本配置

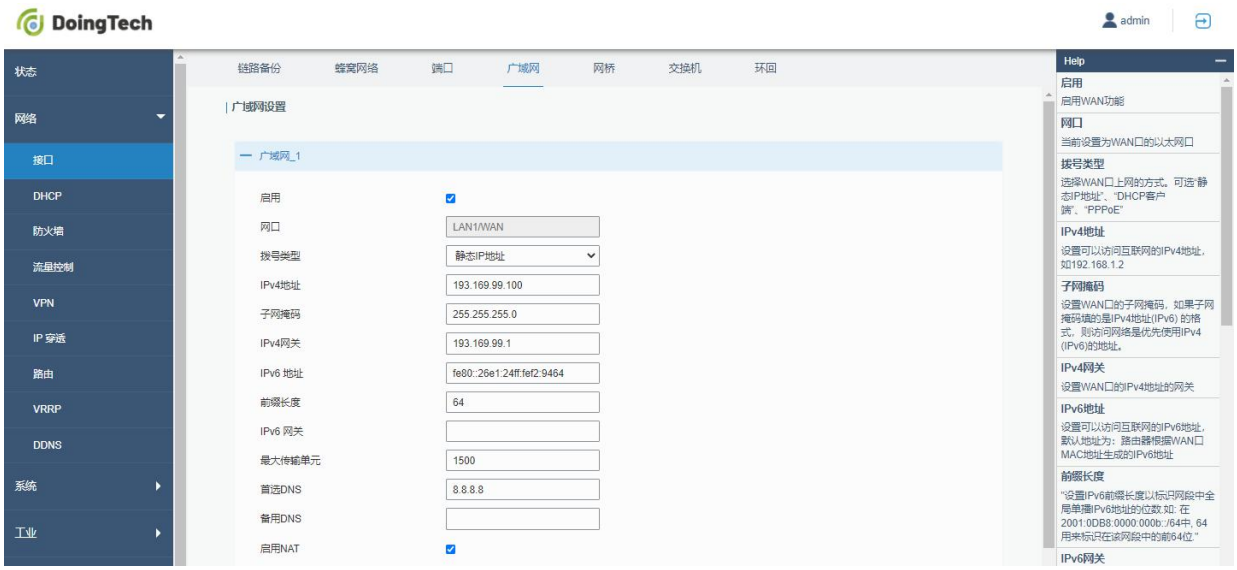
3.2.1 远端 ORB305 WAN 口配置（*如无 WAN 口或采用 4G 拨号则跳过此步骤*）

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）。



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。



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。

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）

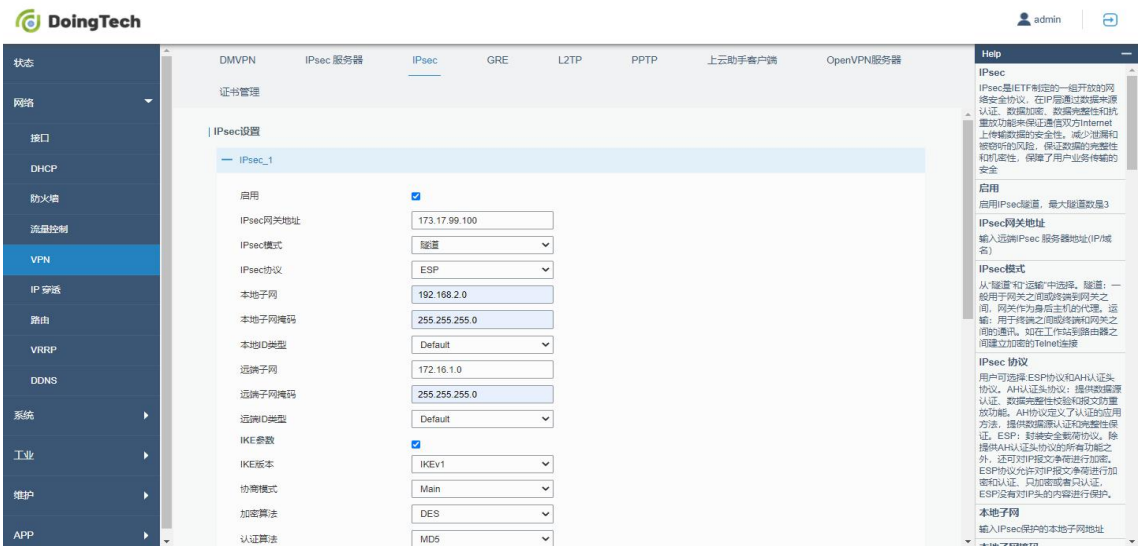
3、进入网络→接口→连链路备份界面启用对应 SIM 卡并上调链路优先级，保存配置

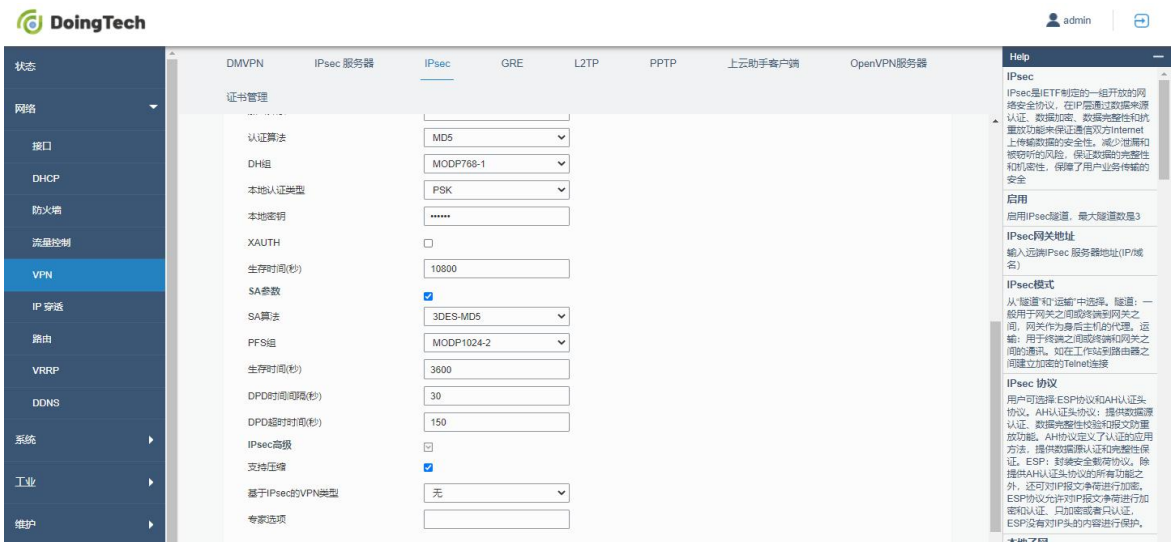
4、对应 SIM 卡拨号成功，当前链路变为绿色

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）





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: 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: 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: dymap

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

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。

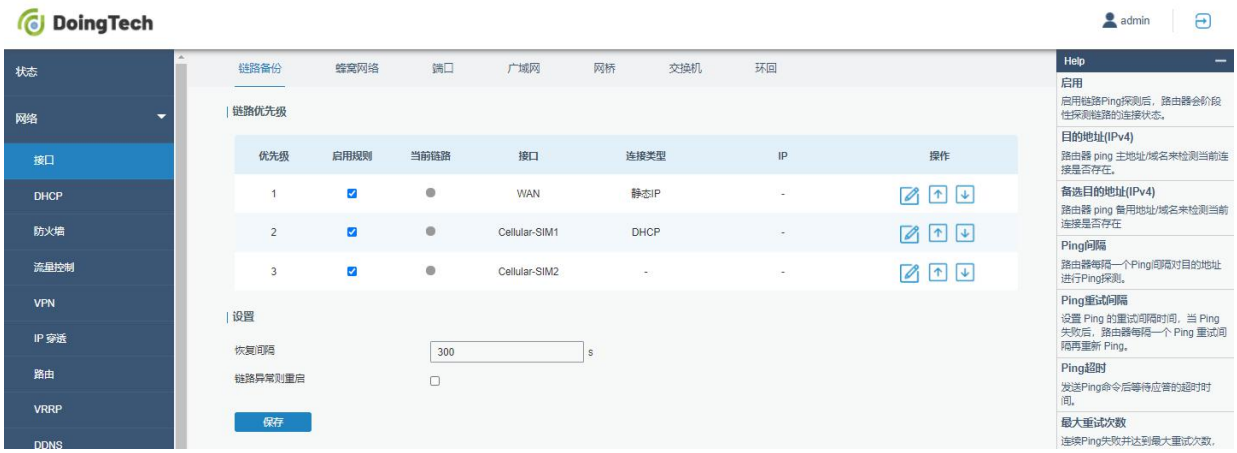
Ciscoasa&pix(config)#access-list nonat extended permit ip *172.16.1.0 255.255.255.0 192.168.3.0 255.255.255.0*

4.2 新增远端 ORB305 配置

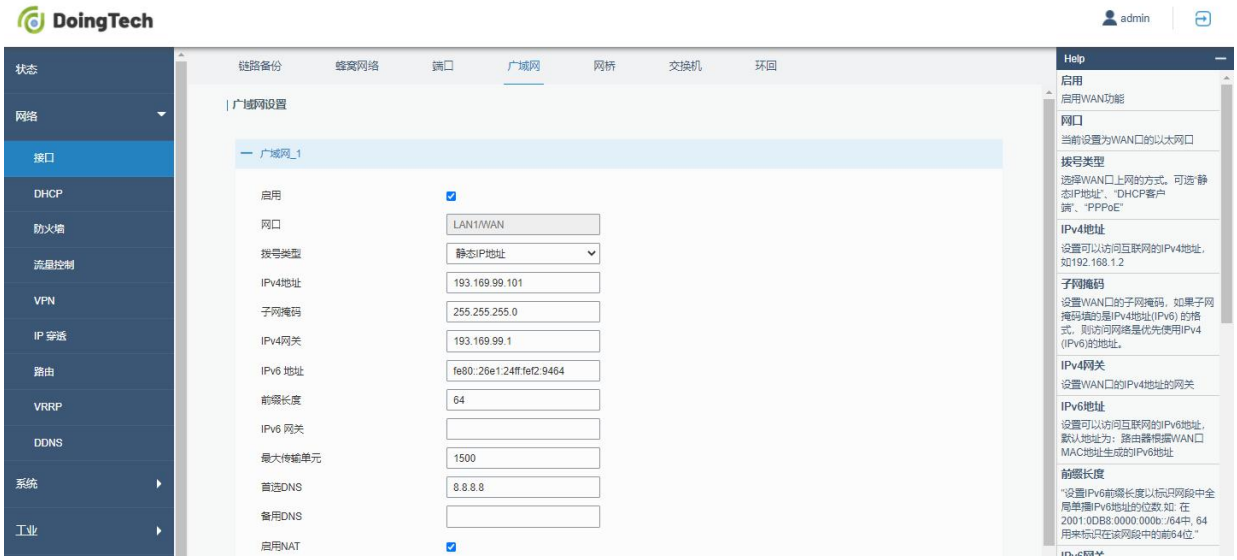
4.2.1 新增远端 ORB305 WAN 口配置（*如无 WAN 口或采用 4G 拨号则跳过此步骤*）

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）。



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。



4.2.2 新增远端 ORB305 LAN 口配置

进入“网络 ” -> “接口 ” -> “网桥”配置如图。

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）

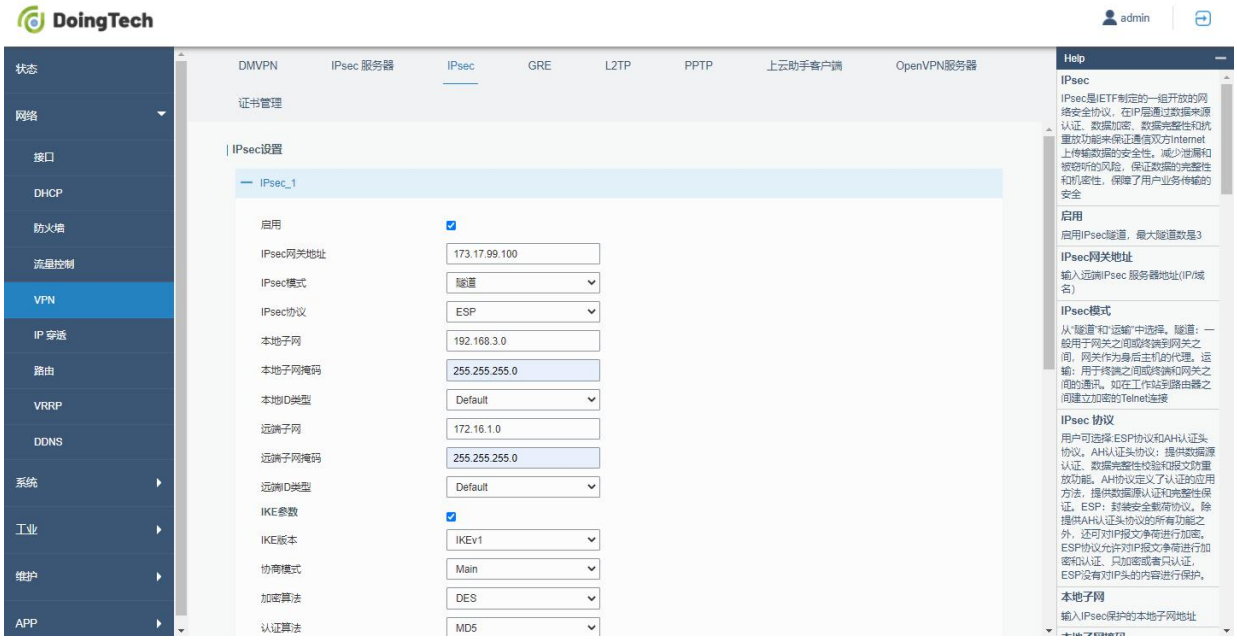
3、进入网络→接口→连链路备份界面启用对应 SIM 卡并上调链路优先级，保存配置

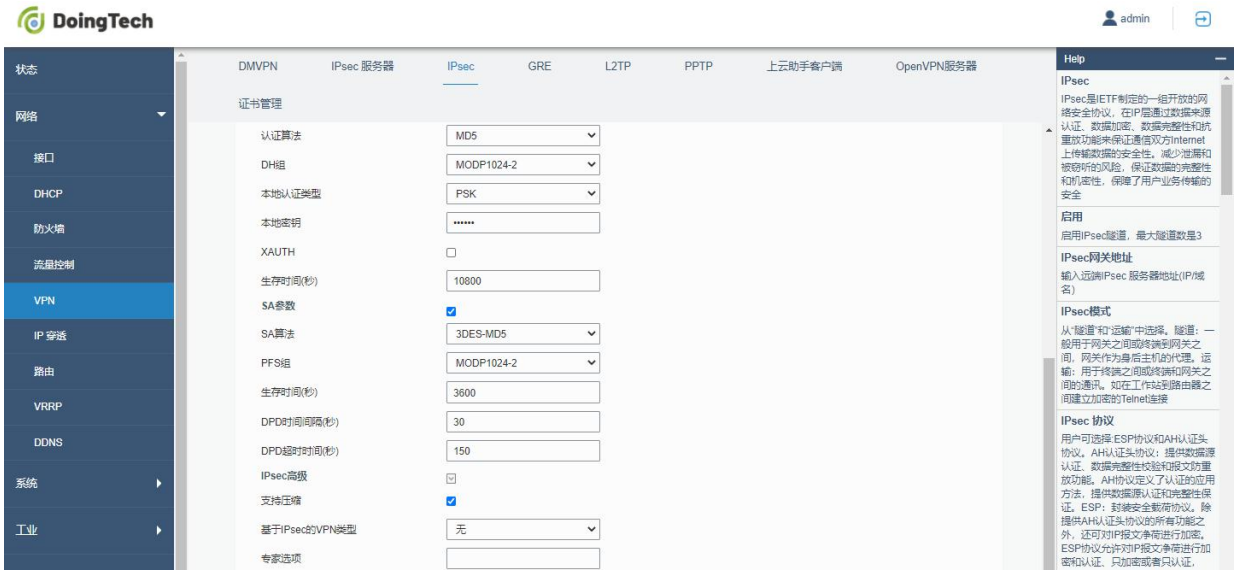
4、对应 SIM 卡拨号成功，当前链路变为绿色

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）





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

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: dymap
        sa timing: remaining key lifetime (sec): 3312
        IV size: 8 bytes
        replay detection support: Y
Crypto map tag: dymap, seq num: 1, local addr: 173.17.99.100
    access-list nonat permit ip 172.16.1.0 255.255.255.0 192.168.3.0 255.255.255.0
    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: dymap
        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: dymap
        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

第二台远端 ORB305

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。