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。



HANNE HARD BAR OF	■ ○ 両板 監控	自 ■ ^{第略 对象}	▲ ■ 网络 系统		当前用户:admin 提交 保存 帮助 关于 修改告码 注册
 ● 接口 (* LTE 4G □,接口对 	DHCP服务列表 小 新建 業 地球		1		🗞 គេនា
◆ 安主活法 ◆ 安主活法 ◆ 安主活法 ◆ 安主活法 ◆ 四 NAS ◆ 日本 ◆ 日本	· ^{接口各你} 3 新建DHCP服务	类型	· 新田 ? ×		
	接口名称 类型 服务类型 可分配IP地址范围 子网输码 默认网关(*) DNS服务 首选DNS服务器		GE0/0/2 ● IP-4 IP- ● 服务器 中: 10.3.0.2 255 255.0 10.3.0.1 ● 使用系统的DNS设置 1.2.2.2	▼* * * * * * * * * * * * * *	4 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:





5、配置防火墙安全策略与源 NAT 以允许内网访问外网:

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 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 Dhcp Enabled. Yes Autoconfiguration Enabled : Yes Default Gateway 10.3.0.1 DNS Servers 1.2.2.2 Lease Obtained. : 2014年10月16日 15:00:00



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



HLIAWEI			9 5%			Ë	前用户: admi	1 提交 保	存 離助	关于 修改函	嗣 注销
(* LTE 40 (* LTE 40	 接口列表 ◆新建 X 删除 	0		🛯 副新	接口名称	~	请输入接口》	耕		Q. 260 🏂	清除查询
 ● 安全区域 □ □ □ □ DNS 	接口名称	安全区域	中地址	让接类型	VLAN	模式	物理	状态 IPv4	IPv6	启用	编辑
DHCP服务器	GE0.0/0(GE0.MGMT)						*			7	
口 🖾 路由	6E1.0/0							٠		3	
IPSec	6E1.0/1				_					17	- 12
Sector Pact	GE1.0/2							*		1	2
D 😂 ORE	GE1/0/3						+	+	+		- 🕼
D ESSL VPN	GE1.0/4							*	+	- 5	
🖸 TSMEES)	GE1.0/5 4					¥hr	٠			4	B
修改GigabitEthernet		57网按口参数	修改GigabitEthernet	III 直内网	的按口参照	£X					? ×
接口名称	ØlgabilEthernet1/0/1	1	接口名称	GigabitEthemetr/0/3							
别名			别名								
虚拟系统③	public 🔽 *		虚拟系统③	public 🔽 *							
安全区域	untrust		安全区域	trust							
模式	 函由 ○ 交換 ○ 	旁路检测 〇 接口对	模式		○ 旁路检测	○ 接口对					
IPv4 IPv6			IPv4 IPv6								
连接类型	● 静态F ○ DHCP ○	PPPOE	连接类型	● 静态ℙ ○ DHCP	O PPPCE						
中地址	1.1.3.1/255.255.255.0	一行一条记录 输入格式为"1.11. 或者"1.1.112"。	F地址	10.1.1.1/255.255.255.0		一行一条记录 输入格式为11 或者11.1.1.12	1.1.1/265.265 4°°	255.0"			
默认网关			默认网关			1					
■法DNB服务器 ③ 各用DNB服务器 ③			ii选DNS服券器 の								
🗌 多出口选项	2		- 多出口选项								

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





				当前用户:admin 握实 保存 鞣制) 关于 橡胶密码 注稿
■ 穆口 (*) LTE 46] 復口討 ④ 安全区域 □ □ DNS □ □ DNCP開系器 ■ ● 路由	22 2 3 3 4 次 先 8 8 ドー(第1)(代先約) ドー(第1)(代先約) 60 60	1 1 265- <1-255>	立用		
	静态路由列表				
企作之路由	◆新建 器删除				1000 1000 1000 1000 1000 1000 1000 100
· 運 RIP · 運 oppr	發虚誤篇由器 目的地址/續到	目的虚拟新由器	下一跳 优先级 出接口	螺定即-Link名称 绑定时D名称	編集
BGP	3				
■ 动吃醋由温控表 >> 90 m +					2
新建静态路由		? ×	新建静态路由		? ×
协议类型	IPv4 O IPv6		协议类型	 IPv4 IPv6 	
源虚拟路由器	public	~	源虚拟路由器	public 🗸	
目的地址/掩码	10.1.2.0/255.255.255.0	*	目的地址/箱码	10.1.3.0/255.255.255.0	(1)
目的虚拟路由器	public	~	目的虚拟路由器	public	
出接口	NONE	~	出接口	NONE 🗸	
下一跳	1.1.3.2		下一跳	1.1.3.2	
优先级	60	<1-255>	优先级	60	:1-255>
可靠性检测	 不检测 绑定BFD 	〇 绑定IP-Link	可靠性检测	● 不检测 ○ 绑定BFD ○ 绑定	IP-Link
描述 4 配置到 此处假 下一跳	分支1私网IP地址的路由, 设Firewall_A到Internet的 IP地址为1.1.3.2。	确定取消	描述	支2私网IP地址的路由, Firewall_A到Internet的 地址为1.1.3.2。 确定	取消

7、在网络→IPsec→IPsec→新建配置 IPsec 服务器策略并应用

		当前用户:aomin 提文 保存 棘动 关于 修改密码 注请
 ● 擦口 (*) LTE 46 ○, 接山斑 ● 安全区域 □ □₂ DNS 	IPSec年最列表 1 中 30世< 第日件 思 第日 前些 4年 场景 本 3世 新景 本 3世 新景 百音(1) 百音(1)	8) 25日 (前前注册) 25日 (10) (10) (10) (10) (10) (10) (10) (10)
ロ 画 DHCP服装器 口 画 路由	新建IPSec角瘤 4	
BigPSec SigPSec SigPSec	構成 自制点 自制点 自動点 通貨用力成的方向目前、不成力から自然的有点。	★ ② ③ ③ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○
5	新築品称 pality1 * 支加数目的 OE107 ●* 読品 対数数位 1.3.1 ● 対数数位	(4)T (8).5
	以区方式 ● 料具専定器 RAU協会 用非協会型数学を応知的保定・単式価 医病血型 ● 単豆酸 多正確 運動出始地域 18.11.872 医病口の ● ● 第 第 水和000 ● ● ● 11.31 別余00 ● ● ● ● 別余00 ● ● ● 0	◎
	2 (封监销换展表	(U)

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

O DoingTech

状态		- 链路	备份	蜂窝网络	端[口 广域网	刚 网桥	交换机	环回	
网络	-	链路伊	先级							
接口		Ø	先级	启用规则	当前链路	接口	连接类型		IP	操作
DHCP			1		•	Cellular-SIM2	DHCP	10.8	81.192.57	

- 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						

oingTech

ORB305 与华为防火墙构建 IPsec VPN 配置指导手册

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)	
DoingTech	👤 adr	min 🔁

O DoingTech

	*								Help -
状态	DMVPN	IPsec 服务器	IPsec	GRE	L2TP	PPIP	上云助于客户调	OpenVPN服务器	IPsec
网络 🗸	证书管理								IPsec是IETF制定的一组开放的网络安全协议,在IP层通过数据来源 ▲ 认近我是加密、数据加密、数据完整性和抗
接口	IPsec设置								上传输数据的安全性。减少泄漏和 被窃听的风险,保证数据的完整性
DHCP	- IPsec_1								和机密性,保障了用户业务传输的 安全
防火増	启用								启用 启用IPsec隧道,最大隧道数是3
流星控制	IPsec网关地划	:	1.1.1.1						IPsec网关地址 約 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法 法
VPN	IPsec模式		隧道		~				名)
	IPsec协议		ESP		~				IPsec模式
IP 穿透	本地子网		192.168.2.0						於 碱道和 运剩 中因早,碱道:一 般用于网关之间或终端到网关之
路由	本地子网掩码		255.255.255	.0					间,网关作为身后主机的代理。运 输:用于终端之间或终端和网关之 间的通讯,如在工作站到路由器之
VRRP	本地ID类型		Default		~				间建立加密的Telnet连接
	远端子网		10.1.2.0						BOTTER FORMUTARIES
DDNS	运端子网撞码		255.255.255	.0					协议。AH认证头协议:提供数据源
系统	远端ID类型		Default		~				放功能。AH协议定义了认证的应用 方法、提供数据源认证和完整性保
T	IKE参数								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
	IKE版本		IKEv1		~				外,还可对IP报文净荷进行加密。 ESP地议会运动P报文海筋进行加
∰£P ▶	协商模式		Main		~				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。
	加密算法		3DES		~				本地子网
APP 🕨	いに首注		MD5		~				输入IPsec保护的本地子网地址
	* WOLLPHIA								* 由之际推动风

C DoingTech			💄 admin 🛛 🔁
状态	DMVPN IPsec 服务器	IPsec GRE L2TP PPTP OpenVPN客户端 OpenVPN部务器	Help —
网络 🔻	证书管理		IPSec IPsec是IETF制定的一组开放的网 络安全协议,在IP层通过数据来源 认证、数据加密、数据完整性和抗
接口	DH组	MODP1024-2	上传输数据的安全性。减少泄漏和 按琼斯的风险(保证数据的索整性
DHCP	本地认证类型	PSK •	和机密性、保障了用户业务传输的安全
防火墙	本地密新 XAUTH		启用 启用IPsec隧道,最大隧道数是3
流量控制	生存时间(秒)	10800	IPsec网关地址
VPN	SA參数	٥	輸入週期IPsec服時鐵地址(IP/域 名)
	SA算法	3DES-MD5 V	IPsec模式
IP穿透	PFS组	MODP1024-2 V	从"隧道"和"迈蜀"中远岸。隧道:一 般用于网关之间或终端到网关之 词 网络你知道你主知的说理。还
路由	生存时间(秒)	3600	前,两天下为身后主机员们包里。运 输:用于终端之间或终端和网关之 间的漂流,如在工作社会图图由器之
VRRP	DPD时间间隔(秒)	30	间建立加密的Telnet连接
DDNS	DPD超时时间(秒)	150	IPsec 协议 用户可选择:ESP协议和AH认证头
bbito	IPsec高级		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
系統	支持压缩	8	放功能。AH协议定义了认证的应用 方法,提供数据遵认证和完整性保
<u>⊥</u> # ►	基于IPsec的VPN类型	无 *	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报文争荷进行加密。
	+ IPsec_2		ESP协议允许对IP报文争荷进行加 密和认证、只加密或者只认证。
鯽	+ IPsec_3		ESP没有对IP头的内容进行保护。
400			本地子网 输入IPsec保护的本地子网地址
APP -	保存		*

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



oingTech									💄 admin 🔁
状态		概况	蜂窝	网络	VPN	路由信息	主机列表		Help — 客户端
网络	×	客户端							名称 显示已经启用的VPN客户质的名称
系统	۲		4 ips	3称 sec_1		状态	本地IP 192.168.2.0/24	远端IP 10.1.2.0/24	状态 显示开启的客户跳是否与服务器连 接
									本地IP