ACG1000系列与ER路由器对接IPSEC VPN配置举例(适用于两端固定地址 组网)

IPSec VPN **叶佳豪** 2019-09-19 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

本案例适用于软件平台为ACG1000系列应用控制网关: ACG10X0、ACG1000-AKXXX等。 注: 本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。

1.2 配置需求及实现的效果

因公司业务拓展需要将处于两地的公司网络通过IPSEC VPN连通,使总部和分部网络可以相互访问。I P地址及接口规划如下表所示:

公司名称	外网接 口	公网地址/掩码	公网网关	内网接口	内网地址/掩码
总部 (ER8300G2- X)	WAN1	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部 (ACG1040)	ge1	198.76.26.90/30	198.76.26.89	ge3	192.168.20.0/24

2 组网图



配置步骤

3 配置步骤

3.1 两端配置上网配置

本文档重点给出两台设备IPSEC VPN配置步骤,上网配置略。

3.2 总部侧ER8300G2-X IPSEC VPN策略配置

#在"VPN">"IPSEC VPN">"虚接口"中点击新增按钮,在新增虚接口中,虚接口名称设置为"ipsec0",绑 定的接口为WAN1。

≫ 系統导航	安全联盟 虚協口 IKE安全提议 IKE对等体 IPSec安全提议 IPSec安全第	8
≫ 系统监控		
≫ 接口管理	虚接口	
➢ AP管理	虚接口的配置修改后,需要重新启用(先禁用再启用)引用该虚接口的IPSEC安全策略或重新	東龍
> 上网管理	全流 新規 用除	1
≫ Z WiFi		
≫ 安全专区	加加電気使用クロシ	^
W VPN		
 IPSEC VPN 	送按山西标: 1psec0 ♥	
L2TP VPN	郭定接□: 1,2,11 ♥	
≥ QosiikIII	描述:	
≫ 高级设置	増加 取消	
> 设备管理		

#下一步"VPN">"IPSEC VPN">"IKE安全提议"中点击新增按钮,安全提议名称设置为"center",IKE验证 算法、IKE加密算法、IKE DH组参数一般使用系统默认即可。



#下一步"VPN">"IPSEC VPN">"IKE对等体"中点击新增按钮。

▶ 系统导航	安全联盟	虚接口	IKE安全提议	IKE对等体	IPSec安全提议	IPSec安全策略
≫ 系统监控						
≫ 接口管理	对	等体				
➢ AP管理	对等位	本的配置修改	次后,需要重新启用	月(先禁用再启用)	引用该对等体的IPSE	C安全策略或重新使前
≫ 上阿管理	49	新潮	単(論		关键 令·	名称 🗸
> Zwifi					A#7-1	
≫ 安全专区	操作	序号	名称	虚接口	对端地址	模式
W VPN						第1页/共1页共0
> IPSEC VPN						
L2TP VPN						

#在弹出的设置菜单中,对等体名称设置为"center"、虚接口选择为"ipsec0"、对端地址 为"198.76.26.90"、协商模式选择为"主模式"、安全提议选择上一步中创建的"center"、预共享秘钥设置 为"123456",设置完成后点击确定完成IKE对等体设置。

新增IKE对等体	*
对等体名称:	center (范围:1~16个字符)
虚接口:	ipsec0 🗸
对端地址:	198.76.26.90 (IP 或域名)
协商模式:	● 主模式 ○ 野蛮模式
安全提议一:	center ¥
安全提议二:	请选择 🗸
安全提议三:	请选择 🖌
安全提议四:	请选择 🗸
预共享密钥(PSK):	123456 × (范围:1~128个字符)
生命周期:	28800 秒(范围:60~604800秒,缺管值:28800)
DPD :	○开启 ◉ 关闭
DPD周期:	10 秒(范围:1~60秒,缺省值:10)
DPD招时时间:	30 秒(范用:1~300秒,缺省值:30)

#下一步"VPN">"IPSEC VPN">"IPSEC安全提议"中点击新增按钮,安全提议名称设置为"center",ESP 验证算法、ESP加密算法参数一般使用系统默认即可。

≥ 系统导航	安全联盟	虚接口	IKE安全提议	IKE对等体	IPSec安全提议	IPSec安全策略
≥ 系统监控		_				
≥ 接口管理	安	全提议				
➢ AP管理	安全排	影议的配置例	的后,需要重新度	自用(先禁用再启	用)引用该安全提议的	DIPSEC安全策略或
> 上网管理	42	新道	影除		关键之	名称 >
> Z WiFi	26.00	romet A	835		A82-7-	
> 安全专区	3076	INUTE	医联			
W VPN		-				
> IPSEC VPN		安全提		enter	×	(范围:1~31个字符)
L2TP VPN		安主切		AH • ESP	O AH+ESP	
≥ Qositit		ESP程 ECD+2				
≥ 高级设置		ESPJU		000 V		
≫ 设备管理				増加 取消		

#下一步"VPN">"IPSEC VPN">"IPSEC安全策略"中点击新增按钮。

≫ 系统导航	安全联盟	虚撤口	IKE安全提议	IKE对等体	IPSec安全提议	IPSec安全策略
≫ 系统监控						
≫ 接口管理	IP	Sec设置				
➢ AP管理					□ 启用IP	Sec功能
≫ 上网管理					应用	
≥ Z WiPi						
≥ 安全专区	安	全策略				
W VPN	虚接[と提议、IKE対等体 ビー次 新的配置機	和IPSEC安全推	認知 態改 1 の の の の の の の の の の の の の	后,只需要重新启用(先
▶ IPSEC VPN	211004	car o'c c-yji			, IPRATOLOGIZERA	
L2TP VPN	全地	新增	删除		关键字:	名称~
≥ Qosi≹II	操作	序号	名称	状态	本端子网网段	对端子网网段
≥ 高级设置						续 1 元/++ 1 元 +

#在弹出的设置菜单中,安全策略名称设置为"center"、本地子网IP/掩码为"192.168.10.0/24"、对端子 网IP/掩码为"192.168.20.0/24"、对等体和安全策略选择之前创建的"center",设置完成后点击新增。

新增IPSEC安全策略	
安全策略名称:	center (范围:1~16个字符)
是否启用:	启用 🗸
本地子网IP/掩码:	192. 168. 10. 0 / 255. 255. 255. 0
对端子网IP/掩码:	192. 168. 20. 0 / 255. 255. 255. 0
协商类型:	 ● IKE协商 ○ 手动模式
对等体:	center 🗸
安全提议一:	center 🗸
安全提议二:	请选择 🗸
安全提议三:	请选择 🗸
安全提议四:	请选择 🖌
PFS :	禁止・
生命周期:	28800 秒 (范围:120~604800, 缺省值:28800)
触发模式:	流重触发 🖌
	増加 取消

#完成策略配置后开启IPSEC策略后点击应用按钮。

#下一步在"高级配置">"路由配置">"静态路由"中点击新增按钮,目的地址填写对端ACG内网网段地址

`	出接口设置为ipsec0,	选择元成后点击增加元成配置。	

≥ 系统导航	静态路由 策略路由	
≥ 系统监控		
≥ 接口管理	静态路由表	
≫ AP管理	全选 新增 别除 查看路由信息表	关键
> 上网管理	新增静态路由列表	
> ZWIFI		
沙 安全专区	目的地址: 192.168.20.0	
> VPN	子网掩码: 255.255.255.0	
≥ Qos设置	下一跳地址:	
☆ 高级设置	出接口: ipsec0 ✔	
地址转换	描述:	(可选,范围:1~15个
> 路由设置		
应用服务	増加	取消

3.3 分部侧IPSEC VPN策略配置

#在"VPN" >"IPsec-VPN">"IPsec第三方对接" >"IPsec配置"中新建IKE对等体。

VPN > IPsec-VPN > IPsec第三方对接								
	▲ IPsec 配置 IPsec 随道接口 IKE SA IPsec SA							
- VPN	● 新建IKE							
- IPsec第三方对接	名称 详细信息							
一IPsec快速配置								

#基本设置中网关名称设置为"branch"、对端网关地址为101.88.26.34、模式设置为主模式、预共享秘

钥与ER8300设置一致为"123456"、IKE协商交互方案加密算法为3DES,认证算法为MD5,点击添加 到列表、DH组选择"2"后点击提交完成配置。

基本设置	1 <u>1111111</u>				
网关名称	branch		(1-31 字符)		
	○本地源接口	〇本地源IP地址	◎无		
对端网关	静态IP地址	~			
IP地址	101.88.26.34				
模式	○野蛮模式	●主模式(ID保持	≐)		
认证方式	预共享密钥	~			
预共享密钥	•••••	\sim	(6-39 字符)		
高级选项 🎖					
IKE协商交互方案					
	加密算法 3DES	✔ 认证	MD5	✔ 🕣 添加到列表	
	加密算	÷	认证	操作	
	1 3DES		MD5	删除	
	DH组 〇	1	2	05	
	密钥周期	86400	(120-86400 彩		
	NAT穿越连接频率	10	(10-900 秒)		
	本地ID	●无	FQDN	U-FQDN	○ IP地址
	对講ID	◉无		O U-FQDN	○IP地址

#新建IPsec安全提议。

20 🗸 🕅	第1 共1页	• H 0	
IKE : branch			
🕑 新建IPsec			
名称			IKE名称

#设置通道名称为"branch",IKE对等体调用"branch",ESP加密和认证算法设置为3DES_MD5H后点击 添加到列表,设置完成后点击提交按钮。

诵道名称	branch		(1-31 字符)	
IKE	branch	~		
ここの ジャンティー ディー			U	
IPSEC协商交互力条	ESP 3DES_	MD5 V AH NU	ILL 🗸 🕑)添加到列表
	FSP		AH	18/2
				2#(1 F
	1 3DE	S_MD5	NULL	1来TF 删除
完美向前保密(PFS)	● 无	01	NULL O 2	SHF 删除 ○ 5
完美向前保密(PFS) 模式 密钥周期	 ① 元 ④ 随道模式 ④ 秒 	'S_MD5 ○1 ○千字节	NULL Og O 内者都有	SHF 删除 ○ 5
完美向前保密(PFS) 模式 密钥周期 秒	 ① 元 ③ 近 道 模式 ③ 秒 28800 	is_MD5 〇 1 〇 千字节	NULL O 2 〇 两者都有	SHF 删除 ○ 5 (120-86400 秒)
完美向前保密(PFS) 模式 密钥周期 秒 连接方式	 ① 元 ① 近 ① 近 ② 形 ② 秒 ② 8800 ③ 自动连接 	is_MD5 ○ 1 ○ 千字节 ○ 流星敏发送	○ 2 ○ 元 ○ 四 ○ 四 ○ 四 古 部 有 ○ 二 ○ 四 吉 部 有	SHTF 開除 (120-86400秒) 障自动连接

#在"VPN" >"IPsec-VPN">"IPsec第三方对接" >"IPsec隧道接口"中点击新建。

VPN > IPsec-VPN > IPsec第	三方对接	
──■上网行为管理 ─■安全防护	▲ IPsec 配置 IPsec版道按口 IKE SA IPsec SA	
- VPN	 ● 新建 ● 删除 	
- IPsec第三方对接	□ IPsec接口 IPv4地址	IPsec
- IPsec快速配置		

#IPsec选择之前创建的"branch",地址选项中添加本地子网到对端子网的规则后点击添加到列表,注意:Tunnel口的IPV4地址不需要填写。

IPv4地址	tunner	0 (0-1023)	(例如:192.168.	1.1/24)	
IPsec	brance	1	~		
地址项目	192.16	8.20.0/24 - 192	.168.10.0/24 例如:	192.168.1.1/24-192.1	168.2.1/24) 💽 激励
		源地址	目的地址	操作	
	1	192.168.20.0/24	192.168.10.0/24	删除	

#在 "网络配置" > "路由"> "静态路由"中填写去往对端内网的路由,出接口为tunnel0接口。

静态路由	
目的地址	192.168.10.0
子网掩码	255.255.255.0
下一跳/出接口	○下─跳 ●出接口
出接口	tunnel0 (tunnel、pppoe接口,黑洞路由)
权重	1 (1-255)
距离	1 (1-255)
地址探测	- ~
	提交取消

3.4 配置保存

#在设备管理界面右上角点击配置保存,保存当前配置。

and the second		
	配置保存	退出

3.5 结果测试

#分支侧电脑可以与总部侧电脑正常通信,下图为Ping测试结果。

C:\Users\lfw1769>ping 192.168.10.2	
正在 Ping 192.168.10.2 具有 32 字节的数据: 来自 192.168.10.2 的回复: 字节=32 时间=1ms 来自 192.168.10.2 的回复: 字节=32 时间<1ms 来自 192.168.10.2 的回复: 字节=32 时间<1ms 来自 192.168.10.2 的回复: 字节=32 时间<1ms 来自 192.168.10.2 的回复: 字节=32 时间=1ms	TTL=126 TTL=126 TTL=126 TTL=126
192.168.10.2 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 往返行程的估计时间<以毫秒为单位>: 最短 = 0ms, 最长 = 1ms, 平均 = 0ms	0 <0% 丢失>,

查看总部侧IPSEC安全联盟情况:

全联盟	虚搁口	IKE安全	注提议 I	KE 对等体	IPSec安全	提议 IPS	iec安全策略		
安	全联盟SA								
通	过安全联盟:	A , IPSec	能够对不同	的数据流提	供不同级别的好	全保护,在这	由可以查询到相	且应隧道当前状态,	了解隧道建立的各个根
数									
数 818	*								
300 8(8	名称	方向	隧道	两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
数 用(8	。 名称 center	方向 in	経道が 198.76. =>101.88	两端 .26.90 8.26.34	AH SPI	AH 算法	ESP SPI 0x5b5d2f1d	ESP 算法 3DES_MD5	数据流 192.168.20.0/24 =>192.168.10.0/24

#分部侧设备查看IPSEC连接状态:

IKE连接情况:

J	IPsec 配置	1PseckElling[]	IKE SA	IPsec SA			
ſ	8	称		对講用关	本地网关	状态	过期时间/s
	1 🗌 br	anch		101.88.26.34	198.76.26.90	连接	85788

IPSEC连接情况:

IPSEC详细信息		
		^
ID	1185	
名称	branch	
本地网关	198.76.26.90	
对端网关	101.88.26.34	
状态	连接	
源网络	192.168.20.0/24	
目的网络	192.168.10.0/24	
ESP SAs		
ESP SA life(seconds)	28138/28800	
ESP SA life(kilobytes)	0/0/0	
ESP inbound SPI	127315210	
ESP outbound SPI	1532833565	
ESP encapsulation	tunnel	
ESP ENC ALGO	3des	
ESP AUTH ALGO	md5	
AH SAs		
AH SA life(seconds)		~

3.6 常见问题

3.6.1 当使用ER2100设备配置IPSEC VPN时没有配置静态路由的位置怎么处理?

ER2100定位为分支设备,因此设备不支持填写静态路由。使用此设备进行IPSEC VPN配置时无需添加 到ipsec接口的静态路由就可以和对端建立IPSEC隧道。

3.6.2 IPSEC隧道中的Tunnel接口地址是做什么使用的?

Tunnel接口地址是为GRE OVER IPSEC VPN隧道配置GRE两端地址准备的,只做IPSEC VPN此地址不需要添加。

3.6.3 ER路由器与ACG设备是否可以通过野蛮模式建立IPSEC VPN?

实际测试不支持。

配置关键点