IPSec VPN 李章华 2019-09-22 发表

组网及说明

1 配置需求或说明

1.1适用产品系列

本案例适用于ERG2 产品系列路由器: ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等, Co mware V7平台的MSR830-WiNet系列路由器,如MSR830-10BEI-WiNet、MSR830-6EI-WiNet、MS R830-5BEI-WiNet、MSR830-6BHI-WiNet、MSR830-10BHI-WiNet等。MSR版本: 0605P20

1.2配置需求及实现的效果

在总部和分部之间分别建立安全隧道,对客户总部PC所在的子网(192.168.2.0)与客户分支机构PC 所在的子网(192.168.1.0)之间的数据流进行安全保护。安全协议采用ESP协议,加密算法采用3DE S,认证算法采用MD5。

2 组网图



配置步骤

3 配置步骤

3.1配置ER G2路由器

#选择"VPN→IPSEC VPN→虚接口"。单击<新增>按钮,在弹出的对话框中选择一个虚接口通道,并将 其与对应的出接口进行绑定,单击<增加>按钮完成操作



#选择"VPN→IPSEC VPN→IKE安全提议"。单击<新增>按钮,在弹出的对话框中输入安全提议名称, 并设置验证算法和加密算法分别为MD5、3DES,单击<增加>按钮完成操作



#选择"VPN→IPSEC VPN→IKE对等体"。单击<新增>按钮,在弹出的对话框中输入对等体名称,选择 主模式,选择对应的虚接口。在对端地址填写对端的IP或者域名,并选择已创建的安全提议信息,预 共享密钥和MSR侧保持一致,单击<增加>按钮完成操作



#选择"VPN→IPSEC VPN→IPSec安全提议"。单击<新增>按钮,在弹出的对话框中输入安全提议名称,选择安全协议类型为ESP,并设置验证算法和加密算法分别为MD5、3DES,单击<增加>按钮完成操作

▶ 系统导航	安全联盟 虛接口	IKE安全提议	IKE对等体	IPSec安全提议	IPSec安全策略	
≫ 系统监控						
> 推口管理	安全提议					
» AP管理	安全提议的配置修	次后,需要重新自	用(先幫用再启用])引用该安全提议的IF	PSEC安全策略或重制	f使能IPSEC功能,新的配置才能
≫ 上阿管理	23 97	MAR		关键字:	名称 •	· · · · · · · · · · · · · · · · · · ·
≽ ztifi	新作 成品	北部		224W	ALITS	ESDIT
>> 安全考区		编辑IPSE	安全提议列表		ALL	
W V78		_				
► IPSEC V78		安	全提议名称:	er		(問用:1~31个家符)
LETT VEB		安	全协议类型:	O AH @ ESP	AH+ESP	
> Q+s设置		ES	P验证算法:	MD5 -		
≫ 高级设置		ES	p加密算法:	3DES -		
> 设备管理		_		602b TE:		
> 特性专区				ALA		
2. III (CIYAO						

#选择"VPN→IPSEC VPN→IPSec安全策略"。选中"启用IPSec功能"复选框,单击<应用>按钮生效。单击<新增>按钮,在弹出的对话框中输入安全策略名称,在"本地子网IP/掩码"和"对端子网IP/掩码"文本框中分别输入两端对应子网信息,并选择协商类型,对等体,安全提议,单击<增加>按钮完成操作

▶ 系统导航	安全联盟 虛独口 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	IPSec设置
» AP管理	☑ 倉用IPSec功能
> 上同管理	虚用
> ZTifi	按截TBCRC中心学会对来
> 安全专区	安全筆唱 编典17365.发生中电力表
W 178	虚报口、IXE安全提议 新使能IPSEC功能一2
> IPSEC VPM	安全策略名称: 01-851 (3国:1~16个东谷)
L2TP VPS	是否启用: 启用 ▼
> Q+s设置	福作 序号 本地子网IP/搜码: 192.168.1.0 / 255.255.255.0
≫ 高级设置	1 対議子网IP/権码: 192.168.2.0 / 255.255.255.0
> 设备管理	协商类型: ● IKE协商 ○ 手动模式
> 特性考区	对等体: ez ➡
》用户YAQ	安全提议一: er ▼
	安全提议二: 请选择 ▼
	安全提议三: 请选择 ▼
	安全提议曰: 请选择 ▼
(二) 退出	PFS: 単止 -
	生命周期: 28800 秒(范围:120~604800, 敲省值:28800)
	触发模式: 长连模式 ▼
	· 能改 - 和:A

#为经过IPSec VPN隧道处理的报文设置路由,才能使隧道两端互通(一般情况下,只需要为隧道报文 配置静态路由即可)。选择"高级设置→路由设置→静态路由",单击<新增>按钮,在弹出的对话框中 ,设置目的地址、子网掩码等参数,单击<增加>按钮完成操作

≫ 系统导航	静态路由 策略	路由			
≥ 系统监控					
≫ 接口管理	静态路由非	4			
≽ AP管理	全选新增		a.息表	关键字: 描述	•
➢ 上阿管理	握作 序号	目的地址	子网撞码	下一跳地址	出接口
≥ Ztifi	0 1	编辑静态路由列非			× 100
> 安全专区					W25 [10
> VPH		目的地址:	192, 168, 2, 0		6052 T 10
> Q+s设置		子阿攘码:	255.255.255.0		
2 高级设置		下一跳地址:			
-tehilat ta		出接口:	ipsec0 -		
> 路由设置		描述:		(可き,范围:1~	15个字符)
应用服务					
> 设备管理			1662 4		
≥ 特性专区		-			
5 Bichario					

3.2配置MSR路由器

#选择"虚拟专网→IPSEC VPN→Ipsec策略"。单击<添加>按钮,在弹出的对话框中填写ipsec策略名称, 单WAN默认选择WAN口,多WAN要手动选择对应WAN口,组网方式选择点到点,对端地址填写对端的IP,预共享密钥和ER侧填写一致,ACL数字写3000以上的,点击ACL后的"+"进入ACL配置页面。



#进入ACL配置页面选择受保护的协议为IP,填写两端ipsec网段信息,注意后面填写为反掩码,点击<添加>按钮添加,可以添加多条规则,完成后点击<显示高级配置>按钮进入高级配置。

受保护协议	ip		٠	1		
本端受保护网段/反掩码	\$ 192.168.2.0	1	0.0.0.255	本端受保护端口		
讨骗受保护网段/反撤6	9 192.168.1.0	17	0.0.0.255	对端受保护端口		

#高级配置IKE配置协商模式选择主模式,本端身份类型和对端身份类型选择IP,填写两端WAN口地址, 算法组合与ER侧一致,验证算法、加密算法和PFS分别为MD5、3DES、DH2,单击<lpsec配置>按钮 进行下一步操作

W NAUE				
5 9.80E	PH-SR			
FINE				
ER LINGAME	Received and a second			879 (91)
RMR2	0 0397	高级配置 108度 5	PaedCIII	
	0 mar	1008/6	王概式	•
C muen	他能型示單1页,具1页。他能页具1例影響,已後中0.	*3896952	1988 • 10.1.1.2	(#99:1.1.1.1)
		70496952 •	1PH842 * 10.5.5.5	(495:1111)
		20年4677285月(DPD)	○ 开启半 矢闭	
		算が目白	R83.*	
		4.23DA -	MDS	
		3083E3 ·	1065-CBC	•
		PFS .	CH group 2	•
		SAE/790/R	86400	89 (60-604800, 1018-10 3686400)
		1078442		

#lpsec配置算法组合和ER侧保持一致,安全协议、认证算法和加密算法分别为:ESP、MD5、3DES, ,封装模式为隧道模式,单击<返回基本配置>按钮进入基本配置后点击<确定>完成配置。





4 验证配置

#查看VPN状态

两端均设置完成后,保护流ping后建立隧道。您可以通过选择ER路由器的"VPN→IPSEC VPN→安全 联盟"页面,MSR的"虚拟专网→IPSEC VPN→监控信息",并单击<刷新>按钮来查看相应的隧道是否 已成功建立。

ER隧道建立图

系统导航	安全联盟	虚推口	IKES	化全提说 IK	E对等体	IPSec表	全提议	PSec安全策略		
系统震控										
後口管理	安	全联盟SA								
い管理		过安全联盟5	A. IPSe	ec能够对不同的	政議流提 #	「不同级别的	安全保护。右	这里可以查询到相	应隧道当前状态。	了新碰撞建立的各个参
上同管理		•								
云Ti7i		4.15	dealer	FE 25 at 1					FOR 1818	44 MIL
安全专区		-	73195	M APPE	•	AH SPI	AH B.Z	ESP SPI	ESP #35	at in a
171		er-msr	out	10.1.1.1 =>10	0.1.1.2			0x9cd312d2	3DES_MD5	192.168.1.0/24 =>192.168.2.0/24
> IPSEC VFS L2TP VFS		er-msr	in	10.1.1.2 =>10	0.1.1.1			0x28569474	3DES_MD5	192.168.2.0/24 =>192.168.1.0/24
Q++10Z							莱	1页/共1页共2	朱记录 每页 10	0 9914 41 1 6010
高级设置										
0508										

MSR隧道建立图

	нзс	IPsec VPN							
*		Presting	12978B						
0									-
		E 90849	sta:	×	0.59				
•		🗉 mer	Active	REPRESENT	0.0303	沈景中日	571	m/Astron	出入于节期
G	BIG NR IPsec VPN	1941至于第1页,4	113. maile19669.cz	10.1.1.1	10世 ESP-3DES-CBC 以近 ESP-MD5 SA3E神时间(X8/sec) 1843200/3600	J教DP 192.168.2.0/24 田台DP 192.168.1.0.。 Photocol ESP Snc port 0	In 181117514 [ESP] Out 676762739 [ESP]	0/0	0,10
					SABE(#R1R1R1X8/sec) 1843200/3585	Des port 0			

配置关键点