IPSec VPN **史晓虎** 2020-01-17 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, ME R系列路由器, 如: MER3220、MER5200、MER8300。

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PC1所在的子网(192.168.10.0)与客户分支机构 PC2所在的子网(192.168.2.0)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3 DES,认证算法采用MD5,ERG2作为总部,MER作为分部。

2 组网图



配置步骤

3 配置步骤

3.1配置ERG2路由器

#选择【VPN】--【IPSEC VPN】--【虚接口】。单击【新增】按钮,将其与对应的出接口进行绑定, 单击【增加】。

编辑虚接口列表		×
-		
虚接□名称:	ipsec1 T	
绑定接口:	WAN1 •	
描述:		
	修改 取消	

#选择【VPN】--【IPSEC VPN】--【IKE安全提议】。单击【新增】按钮,设置验证算法和加密算法 分别为MD5、3DES,DH组选择DH2,单击【增加】。

➣ 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	安全提订	ŵ.				
» AP管理	安全提议的	配置修改后,需要重新启	用(先禁用再启用)引用该安全提议的IF	SEC安全策略或重新	使能IPSEC功能,新的配置
» 上网管理		新増 冊除		关键字:	名称 🗸	 查询 显示 (
» Z ¥i¥i	提作 底是			计证算法	加密管法	
※ 安全专区	2K IF 37 - 5	。 編帯TFF安全提	论제本			S
W_VPH	/ 1	ABILLYTE	w /342			DH2 mo
> IPSEC VPN		安全提	议 2 称 : 7	r	(禁国)1 16((合))	[10 行(4 4)
L2TP VPN		IKEN	证算法: 7	ND5 👻	(四国:1~10(子付)	
₩ Qos设置		ікера	密算法:	BDES 👻		
》 高级设置		IKE	:DH组: I	DH2 modp1024 ▼		
》 设备管理				修改 [取消]		
≫ 特性专区						
》用户FAQ						

#选择【VPN】--【IPSEC VPN】--【IKE对等体】。单击【新增】按钮,选择野蛮模式,选择对应的 虚接口,对端地址填写0.0.0.0。在"ID类型"选择NAME,本端ID为ER,对端ID为MSR,预共享秘钥填 写123456,保证两端秘钥一致,单击【增加】。

编辑IKE对等体	
对等体名称:	ike2 (范围:1~16个字符)
虚接口:	ipsec1 🔻
对端地址:	0.0.0.0 (IP 或 域名)
协商模式:	○ 主模式 💿 野蛮模式
ID类型:	○ IP类型 [●] NAME类型
本端ID:	ER (范围:1~32个字符)
	MER (范围:1~32个字符)
安全提议一:	IKE 🔻
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,缺省值:28800)
DPD :	○ 开启 ⑧ 关闭

#选择【VPN】--【IPSEC VPN】--【IPSEC安全提议】。单击【新增】,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】。

» 系统导航	安全联盟 虚接口	IKE安全提议 IK	E对等体 IPSec安全提该	IPSec安全策略	
» 系统监控					
》 接口管理	安全提议				
≫ AP管理	安全提议的配置修订	改后,需要重新启用(先	禁用再启用)引用该安全提议的	DIPSEC安全策略或重新	使能IPSEC功能,新的配置才能的
》 上网管理	全选 新增	粉像余	关键:	字: 名称 ▼	查询 显示全部
» ZTifi	操作 应是		安全集议	▲山質注	Een質注
》 安全专区		编辑IPSEC安全	提议列表	AII异丛	
W VPN					
> IPSEC VPN		安全提订	X名称: er		(范围:1~31个字符)
L2TP VPN		安全协议	>次类型: ○ AH ● ESF	O AH+ESP	
》 Qos设置		ESP验证	E算法: MD5 ▼	1	
>> 高级设置		ESP加密	E算法: 3DES ▼		
> 设备管理			修改 取消		
》 特性专区				_	
》用户FAQ					

#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,本端子网192.168.10.0/24,对端子网192.168.2.0/24,并选择协商类 型,对等体,安全提议,单击【增加】。

编辑IPSEC安全策略列表		×
r		
安全策略名称:	ipsec2 (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:	192.168.2.0 / 255.255.255.0	
协商类型:	◎ IKE协商 ◎ 手动模式	
对等体:	ike2 🔻	
安全提议—:	IPSEC •	
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 :	DH1 modp768 🔹	
生命周期:	28800 秒 (范围:120~604800, 缺省值:28800)	
触发模式:	流量触发 ▼	

#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】,目的地址填 写 192.168.2.0,出接口选择ipsec1。

编辑静态路由列表		×
<i>n</i>		
目的地址:	192.168.2.0	
子网掩码:	255.255.255.0	
下—跳地址:		
出接口:	ipsec1 🔻	
描述・		(可选,范围:1~15个字
, <u>11121</u> .	符)	

3.2配置MER路由器

#选择【虚拟专网】--【IPsec VPN】--【IPsec策略】单击【添加】按钮。

	пэс		IPsec VPN	
ch.			10	
Щ.			Ib.sec.akut W.K.Mata	
?				10
0				
- 77			输入关键字自动查询 网络	15t0 BIR
۲			□ 冬秋 妇母方式 違□ 太陽物址 砂漠物址	
۲				
¢	虚拟专网		当前显示第0页,共0页。当前页共0账数据,已透中0. 每页显示: 10 💌	<< < > >>
	IPsec VPN			
Q				
eg.				
		_		

#选择分支节点,对端地址填写5.5.5.5,预共享秘钥为123456,保证两端秘钥一致,配置保护流,本端地址为192.168.2.0/24,对端地址为192.168.10.0/24,并点击高级设置进行下一步设置。

修改IPsec 策略		×
LAND AND		444
修改IPSeC 策略		
名称 *	MER (1-63字符)	
接口 *	WAN0(GE0)	
组网方式	◎ 分支节点 👔 🗇 中心节点 👔	
	∑対端网关地址 ★ 5.5.5.5 (例如:1.1.1.1)	
认证方式	预共享密钥	
预共享密钥	••••• (1-128字符)	
保护流配置		
编号 受保护协议	本端受保护网段/掩码 本端受保护端口 对端受保护网段/掩码 对端受保护端口	_
IP	192.168.2.0/24 192.168.10.0/24	
显示高级配置	-	
	确定 取消	

#IKE配置,协商模式选择野蛮模式,本端身份类型选择FQDN,填写MER,对端身份类型选择IP地址,填写5.5.5.5,认证算法,加密算法,PFS分部为MD5,3DES-CBC,DH2,保证与ERG2侧一致。

高级配置 IKE配置	IPsec配置		
协商模式	野蛮模式	T	
本端身份类型	FQDN V MER	(1-255字符)	
对端身份类型 \star	IP地址 ▼ 5.5.5.5	(例如:1.1.1.1)	
对等体存活检测(DPD)	○ 开启 ● 关闭		
算法组合	自定义 ▼		
认证算法 <mark>*</mark>	MD5	T	
加密算法 🗙	3DES-CBC	¥	
PFS *	DH group 2	¥	
SA生存时间	86400	秒(60-604800,缺省值为86400)	

#IPsec配置,安全协议选择ESP,认证算法MD5,加密算法3DES-CBC,PFS为Group1,算法保证与ERG2保持一致。

			
高级配置 IKE配置	IPsec配置		
算法组合	自定义 ▼		
安全协议 \star	ESP		
ESP认证算法 *	MD5		
ESP加密算法 *	3DES-CBC		
封装模式 *	◎ 传输模式 ම 隧道模式		
PFS	Group_1		
基于时间的SA生存时间	3600	秒(180-604800, 缺省值为3600)	
基于流量的生存时间	1843200	千字节(2560-4294967295, 缺省值为1843200)	
返回基本配置			

3.3保存配置



3.4验证配置

#ERG2侧, 点击【VPN】--【IPSEC VPN】--【安全联盟】, 查看ipsec隧道信息。

安全联盟	虚接口	IKE安全排	2议	IKE对等体 I	PSec安全提议	IPSec安全策	略		
中本時期の									
通过安全期	关盟SA,I	PSec能够对不	同的對	加据流提供不同级别	的安全保护。在这	里可以查询到相	回应隧道当前状态	,了解隧道建立	的各个参数。
刷新									
		名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	数据流
		ipsec2	in	4.4.4.4 =>5.5.5.	.5		0xb5c15050	3DES_MD5	192.168.2.0/24 =>192.168.10.0/24
		ipsec2	out	5.5.5.5 =>4.4.4.	.4		0xdbca08f2	3DES_MD5	192.168.10.0/24 =>192.168.2.0/24
第1页/共1页共2 级记录 每页 10 行 ^{14 44} 1 Go ^{>> >>}									

#MER侧,点击【虚拟专网】--【IPsec VPN】--【监控信息】,查看ipsec隧道信息。

IP	IPsec VPN								
	IPsec策略 监控信息								
							: -		
輸	入关键字自动查	间	高级查询				<u>刷新</u> 删除		
	策略名称	状态	接口	本端地址	对講地址	安全提议	調整		
	MER	Active	WAN0(GE0)	4.4.4.4	5.5.5.5	ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5	ê		

配置关键点