IPSec VPN **史晓虎** 2020-09-18 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MER3220、MER5200、MER8300路由器。

1.2 配置需求及实现的效果

Router A使用ERG2路由器, Router B均使用MER路由器,在两者之间建立一个安全隧道,对客户分支 机构A所在的子网 (192.168.1.0/24) 与客户分支机构B所在的子网 (192.168.0.0/24) 之间的数据流进 行安全保护,实现两端子网终端通过IPsec VPN 隧道进行互访。并且MSRV5路由器是不固定的IP地址

2 组网图



配置步骤

3 配置步骤

3.1 基本上网配置

路由器基本上网配置省略,可参考"路由器上网配置方法"案例。

3.2 配置IPSEC VPN

3.2.1 配置 MSRV5--Router A

#单击【VPN】--【IPsec VPN】--【新建】

VPN > IPsec VPN							
В нзс							
一设备概览	IPsec连接 III	控信息					
- 12 快速向导	连接名称	启用	按口	连接类型	对读影地由于	本端地址	
- 韓口配置							
- 🗈 NAT配置					25	3 2	
- ☜ 安全配置							
音 带宽控制							
- ◎ 高级配置							
- VPN							
- IPsec VPN							
E L2TP							
GRE							

#接口名称选择【G0/0】, 组网模式选择【站点到站点】, 对端网关地址填【2.2.2.2】, 本端网关地址 填【1.1.1.2】, 预共享秘钥填写【1】, 网关ID对端ID类型和本端ID类型选择【IP地址】

新建IPsec连接			
IPsec连接名称	tomer * 字符 (1 - 32)	
□ 网关信息			
接口			
HMINEL	● 站局到站局 ○ PC到站局		
对端网关地址/主机名	2.2.2.2	* 字符 (1 - 255)	
本端网关地址			
认证方式			
 预共享密钥 			
密钥	•	* 字符 (1 - 128)	
确认密钥	•	* 字符 (1 - 128)	
○证书	\checkmark		
网关ID			
对端ID类型	● IP地址 ○ FQDN	对端网关ID	字符 (1-255)
本端ID类型	● IP地址 ○ FQDN ○ User FQDN	本端网关ID	字符(1-255)

#筛选方式选择【流量特征】,源地址填写【192.168.1.0/0.0.0.255】,目的地址填写【192.168.0.0/0. 0.0.255】,点击【高级】,第一阶段交换模式选择【野蛮模式】,认证算法选择【MD5】,加密算法 选择【3DES】,第二阶段协议选择【ESP】,ESP认证算法选择【MD5】,ESP加密算法选择【3DE

S】,点击【确定】

////Lann	
筛选方式	流量特征 🗸
源地址/通配符	192.168.1.0 0.0.0.255 *
目的地址/通配符	192.168.0.0 (0.0.255 *
反向路由注入	
▼高级 第一阶段	
交换模式	○ 主模式 ● 野蛮模式
认证算法	MD5 V
加密算法	3DES 🗸
DH	Diffie-Hellman Group1 🗸
SA的生存周期	86400 秒 (60 - 604800, 缺省值=86400)
协议	ESP v
ESP认证算法	MD5 V
ESP加密算法	3DES V
封装模式	● 隧道模式 ○ 传输模式
PFS	None
SA的生存周期	
基于时间的生存周期	3600 秒 (180 - 604800, 缺省值 = 3600)
基于流量的生存周期	1843200 千字节 (2560 - 4294967295, 缺省值 = 1843200)
DPD	○ 开启 ● 关闭
星号 (*) 为必须填写项	确定 取消

3.2.2 配置MER--Router B

#单击【虚拟专网】--【IPsec VPN】--【IPsec策略】,点击【添加】

	inse	IPsec VPN					
ch							
₽.		IPsec策略 监控信息					
?							-
۲							<u>iii</u>
-		输入关键字自动查询	高级查询			61 8	F 174.40 BRR
۲		□ 22	49 Ministration	te 🗆	太陽神市	安约德州市	100. Per
۲			2010/01/2	1982	17 BRADALL	A 3 BIEPEDALL	JRC H
¢	虚拟专网	当前显示第0页,共0页。当8	前页共0条数据,已选中0。每页	显示: 10 🖌			<< < > >>
	IPsec VPN						
Q							
eeo							
S S							

#选择【中心节点】,选择公网接口【WAN0】,填写预共享密钥【1】,点击【显示高级配置】

添加IPsec 策略			×
添加IPsec 策略			
名称 *	tomsr	(1-63字符)	
接口 *	WAN0(GE0)	~	
组网方式	🔾 分支节点 👔 💿 中心节点 👔		
认证方式			
预共享密钥 *	•	(1-128字符)	
显示高级配置			
	确定	取消	

#配置IKE,协商模式选择【野蛮模式】,本端身份类型选择【IP地址】配置【2.2.2.2】,算法组合选 择【自定义】,认证算法选择【MD5】,加密算法选择【3DES】,PFS选择【DH1】

高级配置 IKE配置	IPsec配置
协商模式	野蛮模式
本端身份类型	IP地址 ▼ 2.2.2.2 (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 V
加密算法 \star	3DES-CBC
PFS *	DH group 1 🗸
SA生存时间	86400 秒 (60-604800, 缺省值为86400)
返回其本配票	

#配置IPsec,安全协议选择【ESP】,认证算法选择【MD5】,加密算法选择【3DES-CBC】,并保 证两端算法一致。然后点击【返回基本配置】,再点击【确定】

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 ● 隧道模式		
PFS			
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

#MER和MSRV5点击页面右上角保存按钮

		_	MER8300				📕 中文 🎽 功能向导 📙 保存 admin 🥋
	H3C	-	系统信息				
	系统信息		2017/200 1445/00				
			36394112 AURONA	12/1/2/19			
	MiniAP管理	>	CPU使用素	内存使用素			
		>			22 1Khns (1)	0	121
		>	ф.	Ť	22.4Kbps ①	1707*	ж н о
۲		>	· · · · · · · · · · · · · · · · · · ·	低 高 🛄	接口速率	用户状态	系统日志
		>					
		>	CPU使用率			系统时间 22:36:52	运行时间 2019-12-22 0天 02:47:20
		× .	3% 0%				
		>	当前使用率 平均使用	₽ 		产品型号 MED9300	: 序列号:
						Boot RC 1.31 软件版本 7.1.064 R	2023月3日2日前19060044、)M版本: 硬件版本: 2.0 :: elease 0809P07 ,
		avcal III PHAT	<	🙁 e 📼 📼 🖿			> > ten du E⊐ O ≭ I■ 22:37 □

3.4 验证配置结果

#在MSRV5下面的终端ping对端MER的内网的地址触发隧道

C:\Users\ping 192.168.0.1
正在 Ping 192.168.0.1 具有 32 字节的数据: 来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=254 来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=254 来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=254 来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=254
192.168.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 1ms, 最长 = 1ms, 平均 = 1ms

#在MSRV5上查看隧道情况

IPsecia	É 接 监控信息				
	连接名	接口	对端地址	本端地址	连接状态
	tomer	GigabitEthernet0/0	2.2.2.2		Connected

#在MER上查看隧道信息

输入关键字目动造词	高级直询				刷新
□ 策略名称 状态	接口	本端地址	对端地址	安全提议	操作

配置关键点