IPSec VPN 程咪 2019-09-23 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

本案例适用于如M9006、M9010、M9014等M9K系列的防火墙

ERG2 产品系列路由器: ER8300G2-X、ER6300G2、ER3260G2、ER3200G2等。

注: 本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

总部有一台防火墙分支有一台ERG2路由器都部署在互联网出口,因业务需要两端内网需要通过VP N相互访问。IP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	1/0/3	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部	WAN1	198.76.26.90/30	198.76.26.89	LAN1	192.168.20.0/24

2 组网图



配置步骤

3 配置步骤

3.1 总部侧IPSEC VPN配置

3.1.1 IPsec策略配置

#在"网络">"VPN">"策略"中点击新建。



#在"基本配置"中"接口"选择接入外网的1/0/3接口,"优先级"设置为1(优先级代表了策略匹配顺序,当存在多条VPN隧道时需要对各VPN隧道优先级进行设置),"认证方式"选择域共享密钥,建立VPN两端隧道的域共享密钥必须一致。对端ID设置对IP地址即分公司公网地址,本端ID默认为本端公网接口IP地址。在保护的数据流中添加源为总部内网网段192.168.10.0/24,目的IP地址为分部内网网段192.168.20.0/24。高级设置中配置ike参数和ipsec参数,该参数需要保证总部和分支必须一致。

NCTON ATTAK							
新建IPsec雜輯							
基本配置							
接口		GE1/0/3		~			
IP地址类型		IPv4	© IPv6				
优先级		1		• (3	1-65535)		
模式		◉ 对莓/分支节点	◎ 中心节点				
对錆IP地址/主机	名	198.76.26.90		• C	1-253字符))	
协商模式		 主模式 	◎ 野宣模式				
认证方式		预共享密钥		*			
预共享密钥					1-128字符))	
再次输入预共享:	家明						
XIIMID		IPv4 地址 * 1	198.76.26.90				
本蒴ID		IPv4 地址 ¥ 1	101.88.26.34				
描述				(1	-80字符)		
保护的数据流							
(+) 添加 前	编辑保护的数据流			? ×			
▼ 源IP地址					R[]	动作	
☑ 192.168.	VRF	公网		~		保护	
	源IP地址()	192.168.10.0/	255.255.255.0				
	目的IP地址()	192.168.20.0/	255.255.255.0				
	协议	any		✓ (0-255)			
	动作E	保油		~			
		DH3/-					++ 1
		确定	取消			Cata (9.42-4	元 A
					Po meters	LUCE COLONE	10000
高级配置							
-							
IKE参数							
加密算法		3DES-CBC		~			
认证算法		SHA1		~			
DH		DH group 2		~			
IKE SA 牛存團	RH .	86400		¥2 (6	0-604800	辞省为86400)	
IDroc Ste		00400					
#filestar			() 体统相关				
安全协议		ESP	© AH	C AH-ESP			
ESPILIE		SHA1		~			
FCPhn家镇3+		2055-090		~			
DEC		SUES-COC					
PTS				•			
IPsec SA生存的	町间 🕐			Eb. (1	00 604000		
接 了可问				0(1	80-004800)	
基于流量				干字节	5 (2560-42	94967295)	
IPsec SA 空闲	超时时间(?)			眇(6	0-86400)		
DPD检测 ③		开启					
内同VRF		公网		~			
本端IP地址							
QoS预分类 ()		□ 开启	_				
		神法	取消				

3.1.2 配置安全策略, 放通IPSEC感兴趣流的数据策略

#在"策略">"安全策略">点击"新建","源IP地址"中点击"添加IPV4地址对象组"

H3C	SECPATH F100-C- G2		() 概范 単控	日本 日
日本 「使 安全領路 日 愛 安全防护 日 M NAT	◆ 新建 前 部除 内容安全配置安更之后() 新建 新建 新建	复利 ➡ 移动 ✓ 品用 ⊘ ‡ ,需要 <mark>提交</mark> 才能生效	1999 - Restances 🕅 (R. 1999)	WAPEJISSHA 📿 RA
日 48 用完管理 日 12 负载均衡	源安全域 目的安全域 別NEID	Untrust Trust	× * • (0-65534) 📝 自动编号
	美型 描述信息	● IPv4 ◎ IPv6	(1-127)	Ŧ)
	动作 透明P地址	● 允许 ◎ 拒绝 (○ 允许并深度检测 ✓ [多选]	
	EIE/PASAL	▲ SetThe AntiBetTy Bold	(*2)	

#配置对象组名称为"192.168.20.0",点击"添加",对象地址为192.168.20.0网段,为分支内网段地址

新建IPv4地址对象	组			? ×
对象组名称 描述	192.168.20.0			*(1-31字符) (1-127字符)
 () 添加 () 添加 () 添加 () 参型 	除	内容	排除地址	编辑
添加对象				3
对象 (?) 排除地址 (?)	网段 192.168.20.0	/ 255.255.255.0	¥	(Pv4地址/掩码长度0-32)
		确定 取消		

#在"策略">"安全策略">点击"新建","目的IP地址"中点击"添加IPV4地址对象组"

源安全域	Untrust			~ *		
目的安全城	Trust			~ *		
策略ID	_			- (0	-65534)	☑ 自动编辑
类型	IPv4	◎ IPv6				
描述信息				(1-	127字符)	
动作	• 允许	◎ 拒绝	◎ 允许并深度检测	N		
源IP地址	192.168.2	0.0		*	8选]	
目的IP地址	1			× [3	5选]	
服务	+ 添加IP	/4地址对象组		[3	8选]	
应用	本端地址			[3	5选]	
应用组	对端内网 102.169.20	0.0		(3	3选]	
时间段	192.108.20 请选择时间	0.0 DEQ		*		
VRF	公网			~		
记录日志	◎ 开启	(2) 关闭				
开启策略匹配统计	◎ 开启	 美闭 				
启用策略	 开启 	关闭				

#配置对象组名称为"192.168.10.0",点击"添加",对象地址为192.168.10.0网段,为总部内网网段地址

新建IPv4地址对象组	1			? ×
对象组名称 描述	192.168.10.0]		* (1-31字符) (1-127字符)
 ◆ 添加 ● 添加 ● 类型 	\$	内容	排除地址	编辑
添加对象	2 162		×	
*138K	Mex 192.168.10.0	/ 255.255.255.	0	*(IPv4地址/掩码长度0-3)
AMOUNT				
L		确定取消		
		确定 取消		

#最后确认一下"源IP地址"为对端内网所在对象组,"目的IP地址"为本端内网地址所在对象组,确定即可

按全策略						
源安全域	Untrust			~		
目的安全域	Trust			~		
策略ID					(0-6553	4) 📝 自动编号
类型	IPv4	© IPv6				
描述信息					(1-127字	符)
动作	 允许 	◎ 拒绝	◎ 允许并深度	陸測		
源IP地址	192.168.2	20.0		*	[多选]	
目的IP地址	192.168.1	10.0		~	[多选]	
服务	请选择服务	号		~	[多选]	
应用	请选择应用	ŧ		~	[多选]	
应用组	请选择应用	刊组		~	[多选]	
时间段	请选择时间	间段		~		
VRF	公网			~		
记录日志	◎ 开启	(1) 关闭				
开启策略匹配统计	◎ 开启	美闭				
启用策略	◎ 开启	◎ 关闭				

3.1.3 总部侧配置安全策略, 放通Untrust到Local, 和Local到Utrust的策略, 用于建立IPsec 隧道

源安全域	Untrust	* *	
目的安全域	Local	~ *	
策略ID		*(0-65534) 📝 自动	编号
类型	IPv4		
描述信息		(1-127字符)	
动作	 允许 恒绝 	◎ 允许并深度检测	
源IP地址	请选择或输入对象组	~ [多选]	
目的IP地址	请选择或输入对象组	▼ [多选]	
服务	请选择服务	▼ [多选]	
应用	请选择应用	▼ [多选]	
应用组	请选择应用组	▼ [多选]	
时间段	请选择时间段	~	
VRF	公网	*	
记录日志	 一 开启 ● 关闭 		
开启策略匹配统计	开启 ● 并启 ● 关闭		
启用策略	开启		

源安全域	Local			~	· · · · · · · · · · · · · · · · · · ·
目的安全域	Untrust			~ *	e
策略ID					(0-65534) 📝 自动编号
类型	IPv4	© IPv6			
描述信息					(1-127字符)
动作	● 允许	◎ 拒绝	◎ 允许并深	度检测	
源IP地址	请选择或编	俞入对象组		~	[多选]
目的IP地址	请选择或编	俞入对象组		~	[多选]
服务	请选择服务	5		~	[多选]
应用	请选择应用	Ð		~	[多选]
应用组	请选择应用	围组		~	[多选]
时间段	请选择时间	同段		~	
VRF	公网			~	
记录日志	◎ 开启	◎ 关闭			
开启策略匹配统计	◎ 开启	◎ 关闭			
白田体政	◎ 开启	◎ 关闭			

3.1.4 保存配置

在设备右上角选择"保存"选项,点击"是"完成配置。



3.2 分支侧IPsec配置

3.2.1 配置IPSec 虚接口

单击【VPN】--【VPN设置】--【虚接口】,点击【新增】,绑定对应的WAN口,比如WAN1:

НЗС									
▶ 系接导数	安全联盟	虚推口	IKE安全提议	IKE对等体	IP8ec宴:	全體說	IPSec安全策略		
▶ 系统监控									
≫ 推口管理	安	全現 III SA							
▶ 上同管理	(B)	过安全联盟S	A · IPSec能够对:	不同的救援流提供	共不同级别的5	安全保护・石	主这里可以查询到相	应隧道当前状态,	了解随道建立的各个参
≫ 安全考区	R.	•							
W W28	430	4.84	10	210512		AL. 18.0	t ron ont	Een Wit	# # # A
> IPSEC VPS		-	/3149	AIPTS	AH SPI	API #3	ESP SPI	EPh. W.W	n n x
L2TP VPM						Ж	1页/共1页共0	条记录 每页 10	f7™ ₩ 1 60₩
▶ Q+x设置									
▶ 高级设置									
▶ 设备管理									
> JII PANG									
新增虚接口列表									×
虚接口名 绑定报 指	3称: 8口: 萌述:	iı W	osec0 ▼ AN1 ▼	<u>观消</u>					

3.2.2 配置IKE安全提议

单击【VPN】--【VPN设置】--【IKE安全提议】,点击【新增】,配置IKE安全提议的各个参数:安全提议名称、IKE验证算法、IKE加密算法、IKE DH组,如下图配置。

▶ 系统导航	安全联盟	虚務口	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	全體议						
▶ NL篇编	安全核	影响的配置相	(次后,需要重新启	用(先禁用再启用)引用该安全提议的IP:	SEC安全解臨或重新使能IPS	BEC功能,新的能置才能生效。	
> 上同管理		1. 1.1	2.9		关键字:	名称 •	R# A+±s	
p 200	投作	序号	名称		计连算法	加密算法	DHft	
- MINE	1	1	BE.		SHA1	3DES	DH2 modp1024	
> 12181 V78						第1页/共1页共1条	2景 梅页 10 行(4) 4 1 69 10 10	
编辑IKE安全	提议列	ŧ					×	
安全	全提议名	称:	IKE	2		(范围:1~16个字符)		
IK	E验证算	法:	SH	A1 👻				
IK	E加密算	法:	3D	ES 🔻				
	IKE DH	组:	DH	2 modp1	024 🗸			
			fi		取消			

3.2.3 配置IKE对等体

单击【VPN】--【VPN设置】--【IKE对等体】,点击【新增】,配置IKE对等体: 对等体名称为IKE、绑定虚接口为ipsec0(前面已经创建)、对端地址为总部的公网ip,即101.88.26.3 4、协商模式选择主模式、安全提议选择ike(前面已经创建)、配置预共享秘钥,此处配置为123456 、其余选择默认即可。

					-	1				
>	系统导航	安全联盟	虚景口	IKE安全瞿	記 IKE對等件	IPSec安全提议	IPSec安全策略			
≥	系统监控					-				
Þ	推口管理	R	等体							
÷.	AT管理	对等性	的配置修	改后, 雷要重新,	自用(先禁用再启用))引用该对等体的IPSEC	安全策略成重新使能IP	SEC功能,新的配	置才能生效。	
Þ	上阿管理	2.0	1.1			关键字:	名称 •	24	[二月二日]	
≽			-						-	
>	安全专区	W 11-	16-5	25.88	R. H. L	XI WATE IK	21.99	ID类型	XXBN	DPD
-		0	1	IKE	ipsec0	101.88.26.34	た際主		INE	关闭
Ľ,	TESEC VEN						第1页/共1页共1	朱记录 每页 10	(7·* * 1	60 * *
_	LETP VPS									

ITEX1 争协		
对等体名称:	IKE	(范围:1~16个字符)
虚接口:	ipsec0 💌	
对端地址:	101.88.26.34	(IP 或 域名)
协商模式:	◉ 主模式 ◎ 野蛮模式	2
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 ◙ 关闭	
DPD周期:	10 利	如范围:1~60秒,缺省值:10)
DPD超时时间:	30 利	少(范围:1~300秒,缺省值:30)

3.2.4 配置IPSec安全提议

单击【VPN】--【VPN设置】--【IPSec安全提议】,点击【新增】,配置IPSEC安全提议:安全提议 名称、安全协议类型、ESP验证算法、ESP加密算法配置如下图:

▶ 系统习候	安全联盟 虛務	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	西黎改后,需要重新启F	用(先慧用再启用)引用该安全提议的IP	SEC安全策略或重新使能IPSE	C功能,新的配置才能生效。
▶ 上阿管理	2.5	1. 2.2	关键字	名称 •	24 AF±#
> Z¥i¥i	撥作 序号	名称	安全协议	AHTA	ESP#法
> REVE	1.1	Psec	ESP		3DES-SHA1
s IPSRC VFN L2TF VFN				第 1页/共 1页 共 1条记	た 朝気 10 行 m m 1 Go m m
编辑IPSEC安全提该	议列表				×
,					
安全提议	名称:	IPsec		(范)	围:1~31个字符)
安全协议	类型:	⊖ AH ●	ESP OAH+ESP		
ESP验证	算法:	SHA1 V			
ESP加密	算法:	3DES •			
		修改 I	取消		

3.2.5 配置IPSec安全策略

单击【VPN】--【VPN设置】--【IPSec安全策略】,勾选启【用IPSec功能】,点击【新增】,配置IP Sec安全策略:本地子网IP即为分支路由器内网网段,此处配置为192.168.20.0/24,对端子网IP即为总 部防火墙内网网段,此处配置为192.168.10.0/24,其余参数按照下图所示配置:

▶ 系统导航	安全联盟	虚接口	IKE安全提说	IKE对等体	IPSec安全提议	IPSec安全策略		
> 系统监控								
≫ 推口管理	IP	Sec设置						
⇒ AT管理					図 AREPS	Sec功能		
> LPHEN								
> 安全专家	安	全策略						
V WH	虚接口	1、IKE安全的	推议、IKE对等体和 新DD和要用新生物	IPSEC安全提彩	的配置都修改完成后・	只需要重新启用(先期) 防急等的影響生命。	用再启用)相关的IPSE	C安全策略一次规重新使制
5 IFSE 178	-		(10 m m m m m m m m m m m m m m m m m m			88 -		原用金田
L2TF VFS	18 ft	184	名称	状态	大幅学に	刘靖子同同段	bast	其它
> 2.922			incer	88	192.168.20.0/	192.168.10.0/	arth.#	od With - nor
> 2412	-		with a	and a	255.255.255.0	255.255.255.0	THE LOT PI	A1410.00
> III.PYAQ						第1页/共1页;	+1条记录每页 5	1914 4 1 Go H
安全策略复致	. r	insec		/****	1 C (100000)			
女主東南石州	•	ipsec		(范惠:1	~16个字符)			
是否启用	:	启用	•					
本地子网IP/撞码	:	192.16	8.20.0	/ 255.2	55.255.0			
对端子网IP/撞码	:	192.16	8.10.0	/ 255. 25	55.255.0			
协商类型	:	IKE	协商 ◎手ュ	动模式				
对等体		IKE	•					
安全提议一		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		禁止	•					
生命周期	:	28800	秒低	120~	604800, 缺省伯	直:28800)		
触发模式	:	流量触	发 -					
	(修改	取消					

3.2.6 配置去往对端子网的静态路由

单击【高级设置】--【路由设置】--【静态路由】,目的地址配置成对端子网,即192.168.10.0,子网 掩码为255.255.255.0,出接口为ipsec0虚接口。

▶ 系统导航 静态路由	策略語曲				
▶ 系统监控					
	* 由 基				
⇒ AT管理	4. ## ## ######	85.0	ARF: 新述	•	R4 A F±#
▶ 上阿管理 操作	作序号 目的地址	子同識码	下一跳地址	出售口	Nif
≥ ž¶iři /	1 192.168.10.0	255.255.255.0		ipsec0	
> 安全考区			第1页/月1	页 共 1 条记录 每页 10	
> ***					
》 <u>東田高</u> 葉					
地址新林					
> 新由设置					
编辑静态路由列表					
日的抽屉	102 168 1	0.0			
EU1097T.	192.100.1	0.0			
子网掩码:	255.255.2	55.0			
下一, 那, 地址:					
出接口:	insec0 -				
	10000				
描述:			(可	选,范围:1~	15个字符)
		14 m	-		
		इड म्ह	(用		

3.3 测试VPN是否连通

3.3.1 数据访问触发IPsec建立

在总部或者分部内网中任意找一台电脑访问对端网络资源。 举例:在分支侧电脑ping总部侧电脑, IPSEC初始建立时会丢1-2个包,建立后通信正常。

C:\Users\sfw1081>ping 192.168.10.3
正在 Ping 192.168.10.3 具有 32 字节的数据: 请求鸫时。
頃水廸叭。 来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=255 来自 192.168.10.3 的回复: 字节=32 时间<1ms TTL=255
192.168 10.3 的 Ping 统计信息: 数据句: 已发送 = 4, 已接收 = 2, 丢失 = 2 (50% 丢失),
往返行程的估计时间(以毫秒为单位): 最短 = Oms,最长 = Oms,平均 = Oms

3.3.2 查看IPSEC监控信息

防火墙侧:在"网络">"VPN">"IPsec">"监控"中查看对到信息,如果有隧道信息就说明VPN已经正常建立,如果没有隧道信息就说明VPN未建立成功。



ERG2路由器侧:在【VPN】--【VPN设置】--【IPSec安全策略】--【安全联盟】里查看隧道建立情况

全联盟SA								
通过安全联盟SA, IPSec能	够对不同的数据流程	供不同级别	的安全保护。在这里	可以查询到相应	隧道当前状态。	了解碰撞建立的	各个参数。	
196								
	名称	方向	隧道两端	AH SPI	AH TEA	ESP SPI	ESP 算法	数据流
	ipsec	in	101.88.26.34 =>198.76.26.90			0x6a7fa8ae	3DES_SHA1	192.168.10.0/24 =>192.168.20.0/24
	ipsec	out	198.76.26.90 =>101.88.26.34			0xf058e589	3DES_SHA1	192.168.20.0/24 =>192.168.10.0/24
							W 17	5/#15#35/37#5

配置关键点