# (和 F5000-X系列两台防火墙采用公网固定地址方式搭建IPSEC VPN配置案例( 主模式WEB配置)

IPSec VPN zhiliao\_FO3qD 2018-11-25 发表

# 组网及说明

# 1 配置需求及说明

## 1.1 适用的产品系列

本案例适用于如F5080、F5060、F5030、F5000-M等F5000、F5000-X系列的防火墙。

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

总部和分部各有一台防火墙部署在互联网出口,因业务需要两端内网需要通过VPN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	1/0/3	198.76.26.90/30	198.76.26.89	1/0/4	192.168.20.0/24

2 组网图



# 配置步骤

#### 3 配置步骤

### 3.1 两端防火墙上网配置

防火墙上网配置请参考"2.3.2 防火墙外网使用固定IP地址上网配置方法"进行配置,本文只针对IPSEC VPN配置进行介绍。

#### 3.2 总部侧IPSEC VPN策略配置

#在"网络">"VPN">"策略"中点击新建。

H <b>BC</b> SE	CPATH	F100-C-		() 概览	<b>十</b> 监控	策略	对象	
釉	*	IPsec策略						
NO VRE		●新建 前 删除						
		🖻 应用策略接口	IP地址类型	1 17	的规	对蒴IP地址	/主机名	3
「安全城								
CT 🕹 (498)								
II R IPv6								
VPN								
GRE								
IPsec								
策略								
监控								
高级设置								

#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。

新建IPsec策略					
基本配置					
接口	GE1/0/3	~			
IP地址类型	IPv4				
优先级	1	. (	1-65535)		
模式	<ul> <li>对等/分支节点</li> <li>中心节点</li> </ul>				
对踌IP地址/主机名	198.76.26.90	- (	1-253字符)	0	
协商模式	<ul> <li>主模式</li> <li>野蛮模式</li> </ul>				
认证方式	预共享密钥	*			
预共享密钥	*****		1-128字符)	ř.	
再次输入预共享密钥					
对銕ID	IPv4 地址 ¥ 198.76.26.90				
本鶐ID	IPv4 地址 ¥ 101.88.26.34				
描述		(1	-80字符)		
保护的数据流					
④ 添加 面 编辑保护的数据流		? ×			
☑ 源IP地址	[		海口	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	保护	~			
					共1係
	确定取消		司版权利	所有,保留一切	刀权利

## 3.3 总部侧配置安全策略, 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"

HBC SECP	ATH F100-C-		
<ul> <li>○ 安全領標</li> <li>○ 安全領標</li> <li>○ 安全防护</li> <li>○ MAT</li> </ul>	○ 新建 内容安全配置支更之后( 新建安全策略	<ul> <li>2011 ◆ 移动 ✓ 点用 ⊘ 禁用</li> <li>2),需要 提交才能生效</li> </ul>	1 10 10 10 10 10 10 10 10 10 10 10 10 10
口 帮 带完管理 口 联 负载均衡	源安全域 目的安全域 第1851D	Untrust Trust	● (0-65534) 図自动病号
	英型 描述信息	● IPv4 ◎ IPv6	(1-127字符)
	設作 源即地址 目的IP地址	<ul> <li>% 允许</li> <li>⑦ 拒绝</li> <li>⑦ 允许</li> <li>● 拒绝</li> <li>⑦ 允</li> <li>● 添加IPv4地址对象组</li> </ul>	许并深度检测 (多选) (多选) (多选)

#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	相					? 🗙
对象组名称 描述	192.168.20.0				* (1-3137 (1-12737	<del>(</del> )
🕀 添加 💼 🗄	删除					
□ 类型		内容		排除地址		编辑
添加对象						0
对象 (?) 排除地址 (?)	网段 192.168.20.0	/ 25	5.255.255.0	~	* ( Pv4 <u>#bt</u> /	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			~	
目的安全域	Trust			~	
東船D				-	(0-65534) 📝 自动编号
类型	IPv4	© IPv6			
描述信息					(1-127字符)
动作	<ul> <li>允许</li> </ul>	◎ 拒绝	◎ 允许并深度	是检测	
源IP地址	192.168.2	0.0		~	[多选]
目的IP地址				~	[多选]
服务	+ 添加IP	/4地址对象组			[多选]
应用	本端地址				[多选]
应用组	对端内网				[梁湖]
	192.168.2	0.0			(39/20)
时间段	请选择时间	同段		*	
VRF	公网			~	
记录日志	◎ 开启	<ul> <li>关闭</li> </ul>			
开启策略匹配统计	◎ 开启	<ul> <li>关闭</li> </ul>			
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					? ×
对象组名称 描述	192.168.10.0	]			▲(1-31字符) (1-127字符)
<ul> <li>◆ 添加</li> <li>前 删除</li> <li>● 类型</li> </ul>	t	内容		排除地址	编辑
添加对象					
对象 🕐	网段 192.168.10.0	/	255,255,255.0	*	* (IPv4地址/擁码长度0-3;
并除地址③	102120012010	r l	2001200120010		
		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

源安全域	Untrust			~	•	
目的安全域	Trust			~ '	•	
策略ID					(0-65534	) 🔽 自动编号
类型	IPv4	© IPv6				
描述信息					(1-127字符	F)
动作	• 允许	◎ 拒绝	◎ 允许并深剧	註检测		
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	导		~	[多选]	
应用	请选择应用	ŧ		~	[多选]	
应用组	请选择应用	用组		~	[多选]	
时间段	请选择时间	可段		~		
VRF	公网			~		
记录日志	◎ 开启	<ul> <li>关闭</li> </ul>				
开启策略匹配统计	◎ 开启	<ul> <li>关闭</li> </ul>				
启用策略	<ul> <li>开启</li> </ul>	◎ 关闭				

3.4 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	编辑
类型	● IPv4 ◎ IPv6		
描述信息		(1-127字符)	
动作	<ul> <li>允许</li> <li>⑦ 拒绝</li> </ul>	◎ 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	<ul> <li>开启</li> <li>美闭</li> </ul>		
开启策略匹配统计	开启 ● 并启 ● 关闭		
户田垒政	◎ 开启 ◎ 关闭		

源安全域	Local		~	
目的安全域	Untrust		~ '	5 C
策略ID			1	(0-65534) 🔽 自动编号
类型		/6		
描述信息				(1-127字符)
动作	<ul> <li>允许</li> <li>① 拒</li> </ul>	色 💿 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	L	~	[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	◎ 开启	闭		
开启策略匹配统计	⑦ 开启 ④ 关	闭		
启用策略	● 开启 ◎ 关	闭		

## 3.5 分部侧IPSEC VPN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分部内网网段192.168.20.0/24,目的IP地址为总部内网网段192.168.10.0/24。

修改IPsec策略								
基本配置								
接口		GE1/0/3				•		
IP地址类型		IPv4		IPv6		-		
优先级		1				(1-65535	)	
模式		对等/分支节	ά.	◎ 中心节点				
对端IP地址/主机名		101.88.26.34				(1-253字符	<del>〕</del> )	
协商模式		主模式		◎ 野蛮模式				
认证方式		预共享密钥				*		
预共享密钥						(1-128字符	)	
再次输入预共享密钥	Ē					<b>i</b> .		
对第ID		IPv4 地址	101.88.	26.34/255.255.	255.255	<b>F</b>		
本銕ID		IPv4 地址	198.76.	26.90		1		
描述	Ē					(1-80字符)		
-								
保护的数据流						( <b>a</b> )		
SETDHE	编辑保护的数据流					? X	=h/k	
192 168 10.0/	VRF	455	1		*		(足)()	
¥ 152.100.20.0/	源IPtttth @	102	168 20 0/2	55 255 255 0			UKGP	2
	Bohrpettel ()	192	100.20.0/2	55.255.255.0		1		
	THE STATE AND ALL OF	192	.168.10.0/2	55.255.255.0	Long Long	(0.055.)		
	19AX	any			*	(0-255)		
	动作	保护	1		*			
			海中	RUSH				井1条
			TOAL	-surg		18	(所有,保留一	切权利

3.6 分部侧安全策略和总部的配置方法类似,只需将IPSEC的感兴趣流的源和目的IP反过来写即可。

痲	12安全策略							×
	150-0-1-0							
	源安主戏	Untrust			× ^			
	目的安全域	Trust			~ *			
	策略ID				* ( 0-	65534)	🔽 自动编号	
	类型	IPv4	© IPv6					
	描述信息				(1-1	27字符)		
	动作	① 允许	◎ 拒绝	◎ 允许并深度检测	Ŋ			
	源IP地址	192.168.10	.0		× (3)	选]		
	目的IP地址	192.168.20	.0		× 3	选]		
	服务	请选择服务			× (\$	选]		
	应用	请选择应用			× (3)	选]		
	应用组	请选择应用约	a.		× (\$	选]		
	时间段	请选择时间	段		~			
	VRF	公网			~			
	记录日志	◎ 开启	<ul> <li>关闭</li> </ul>					
	开启策略匹配统计	◎ 开启	<ul> <li>关闭</li> </ul>					
	启用策略	◎ 开启	◎ 关闭					
		E						
			确定	取消				

### 3.7 测试VPN是否连通

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:在总支侧电脑ping分部侧电脑, IPSEC初始建立时会丢1-2个包, 建立后通信正常。

```
C:\Users\Administrator>ping 192.168.20.88
正在 Ping 192.168.20.88 具有 32 字节的数据:
请求超时。
来自 192.168.20.88 的回复: 字节=32 时间<1ms IIL=255
来自 192.168.20.88 的回复: 字节=32 时间<1ms IIL=255
192.168.20.88 的回复: 字节=32 时间<1ms IIL=255
192.168.20.88 的 Ping 统计信息:
数据包: 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 = 0ms, 最长 = 0ms, 平均 = 0ms
```

## 3.8 查看IPSEC监控信息

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。



## 3.9 保存配置

在设备右上角选择"保存"选项,点击"是"完成配置。

			admin <mark>▼ [→</mark>
	确认提示		▲ 「「「」」「「」」「「」」「「」」「「」」「」」「「」」「」」「「」」「」」「
状	?	确定要保存设备的当前配置吗?	编辑
		是否	

### 4 注意事项

## 4.1 外网接口配置动态地址转换导致VPN无法建立问题

在配置IPSEC VPN时需要注意外网口配置地址转换时一定要排除掉VPN的感兴趣流,因为NAT转换在接口出方向优先于IPSEC策略,如果不修改会导致数据先经过NAT地址转换后无法匹配兴趣流。 在"对象">"ACL">"IPv4"中点击新建按钮。

HBC SE	ECPATH F100-C- 2	(	<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	調整対象
孙	《 IPv4 ACL组			
口 9 用户	新建 前 删除			
	ACL分类	ACL	規則数量	规则四
四 俞 对象组	画 高级	3000	1	配置顺
ACL				
IPv4				
- IPv6				
二层				
🗈 🚉 SSL				
🖬 😪 公钥管理				
EI PKI				

#在"类型"中选择高级ACL, ACL编号输入3999。

IPv4 ACL组		
🛨 新建   💼 删除		
新建IPv4ACL		×
类型	◎ 基本ACL ● 高级ACL	
ACL 💽	3999	* ( 3000-3999或1-63个字
		符)
规则匹配顺序	◎ 按照配置顺序     ◎ 自动排序	
规则编号步长	5	(1-20)
描述		(1-127字符)
	☑ 继续添加规则	(?)
	确定取消	

#以总部防火墙为例,动作选择拒绝,IP协议类型选择拒绝,匹配条件匹配总部侧内网到分部侧内网的 网段(在分部侧防火墙匹配条件取反)后点击确定添加下一条策略。

新建IPv4高级ACL的规	则			K
ACL编号	3999		(3000-3999或 1-63个字符)	~
规则编号	🔽 自动编号		* (0-65534)	
描述			(1-127字符)	
动作	◎ 允许	<ul> <li>拒绝</li> </ul>		
IP协议类型	ip 🗸 (0-256,256f			
匹配条件 🕐	表任意ip) 可匹配源P地址/通配符掩码			
	192.168.10.0	/ 0.0.0.255	*	
	☑ 匹配目的IP地址/i			
	192.168.20.0	/ 0.0.0.255	*	
■ 匹配TCP/UDP报文的目的端口号				,
	回匹配TCP报文的连 确定	接建立标识 <b>取消</b>		

#不需要改变此页面配置,可以直接点击确定按钮。当有多个网段访问VPN的需求时,需要先添加拒绝的策略,再添加全部允许的策略。

新建IPv4高级ACL的规	则		$\mathbf{X}$			
ACL编号 3999		(3000-3999或 1-63个字符)	^			
规则编号	☑ 自动编号	* (0-65534)				
描述		(1-127字符)				
动作	<ul> <li>● 允许</li> <li>● 拒绝</li> </ul>					
IP协议类型	请选择	* ( 0-256,256代				
		表任意ip)				
山配条件 (?)						
	回匹配TCP/UDP报文的源端口号					
CINTCP/UDP报文的目的端口号						
回 匹配TCP报文的迫接建立标识						
III 匹配TCP报文标识						
C 匹配ICMP报文的消息类型和消息码						
	确定取消					

#在"策略">"NAT">"NAT动态转换">"策略配置"中点击新建按钮。接口选择外网接口,ACL选择之前创 建的3999,转换后地址选择接口IP地址。

注意:如果配置策略中已经存在动态转换策略,请在此策略的基础上添加或者更换ACL选项。该操作可能导致断网请谨慎操作。

HBC SECPATH G2	I F100-C-		③概策	正
予航 《	NAT出方向动态转换			
<ul> <li>         ・ 安全策略         ・         ・         ・</li></ul>	<ul> <li>新建 复制</li> <li>接口</li> <li>新建NAT出方向动:</li> <li>接口</li> <li>ACL</li> <li>转换后源地址</li> <li>VRF</li> <li>转换模式</li> <li>不转换端口</li> <li>应用规则</li> </ul>	<ul> <li>开启 (金) 失闭 (前) 番</li> <li>接口描述</li> <li>広時換</li> <li>GE1/0/3</li> <li>3999</li> <li>NAT地址组</li> <li>公网</li> <li>(※) PAT</li> <li>PAT方式分配</li> <li>(※) 启用此条规则</li> </ul>	協会 は な (本)	示导出 地址组 × * * * * *



配置关键点