

# F1000-AK系列防火墙和ERG2路由器IPsec VPN主模式配置

IPSec VPN 程焱 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F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

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

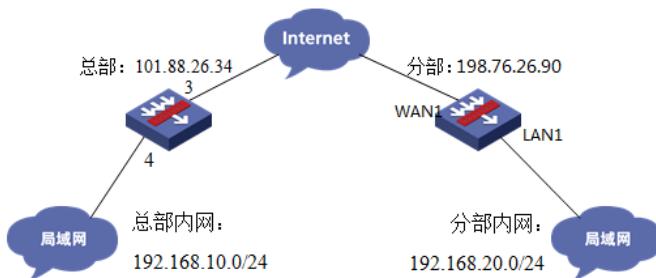
注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

#### 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	WAN1	198.76.26.90/30	198.76.26.89	LAN1	192.168.20.0/24

## 2 组网图



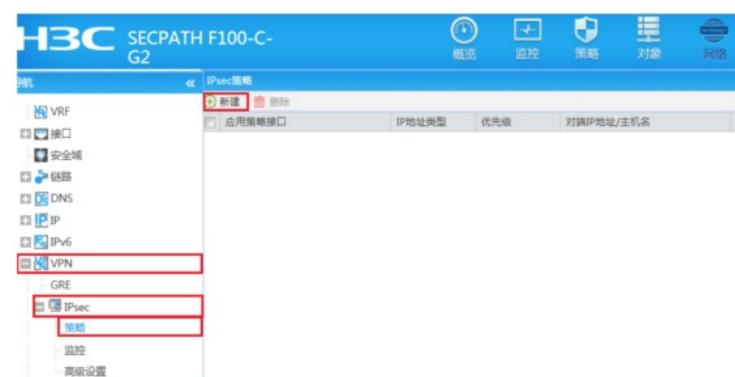
## 配置步骤

### 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。

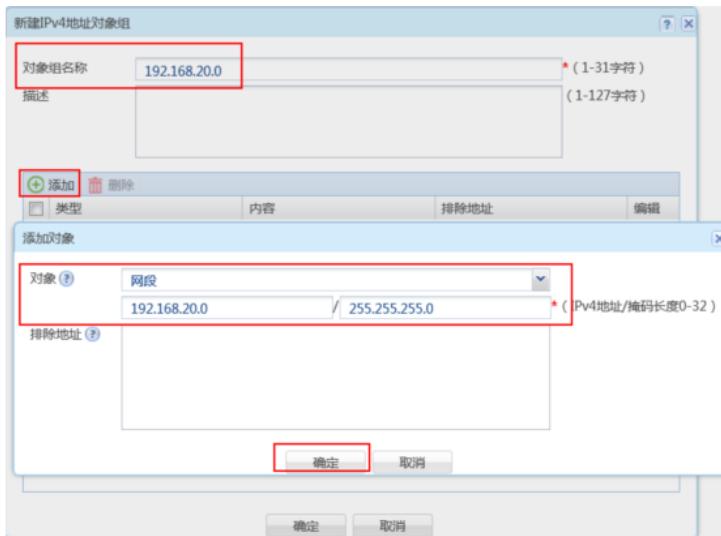


#在“基本配置”中“接口”选择接入外网的1/0/3接口，“优先级”设置为1（优先级代表了策略匹配顺序，当存在多条VPN隧道时需要对各VPN隧道优先级进行设置），“认证方式”选择域共享密钥，建立VPN两端隧道的域共享密钥必须一致。对端ID设置对IP地址即分公司公网地址，本端ID默认为本端公网接口IP地址。在保护的数据流中添加源为总部内网网段192.168.10.0/24，目的IP地址为分部内网网段192.168.20.0/24。高级设置中配置ike参数和ipsec参数，该参数需要保证总部和分支必须一致。

### 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对象组”

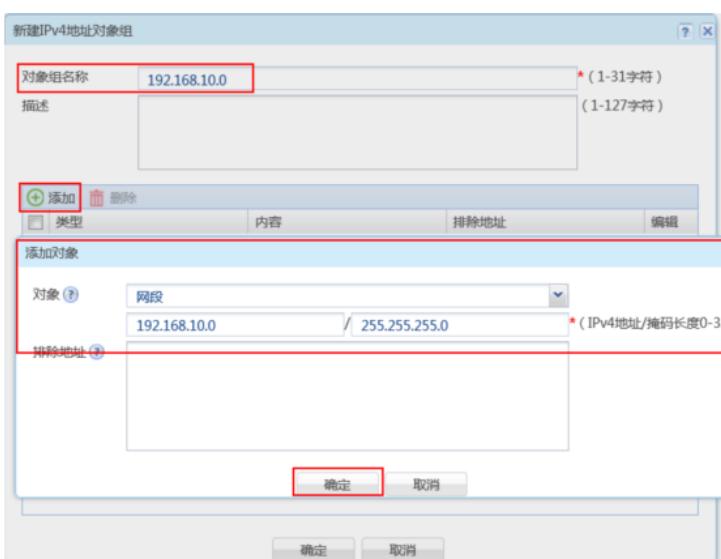
#配置对象组名称为“192.168.20.0”，点击“添加”，对象地址为192.168.20.0网段，为分支内网段地址



#在“策略”>“安全策略”中点击“新建”，“目的IP地址”中点击“添加IPv4地址对象组”



#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



#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

新建安全策略

源安全域	Untrust
目的安全域	Trust
策略ID	(0-65534) <input checked="" type="checkbox"/> 自动编号
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
描述信息	(1-127字符)
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 拒绝 <input type="radio"/> 允许并深度检测
源IP地址	192.168.20.0 [多选]
目的IP地址	192.168.10.0 [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 [多选]
VRF	公网
记录日志	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
开启策略匹配统计	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
启用策略	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭

**确定** **取消**

### 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

新建安全策略

源安全域	Untrust
目的安全域	Local
策略ID	(0-65534) <input checked="" type="checkbox"/> 自动编号
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
描述信息	(1-127字符)
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 拒绝 <input type="radio"/> 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 [多选]
VRF	公网
记录日志	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
开启策略匹配统计	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
启用策略	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭

**确定** **取消**

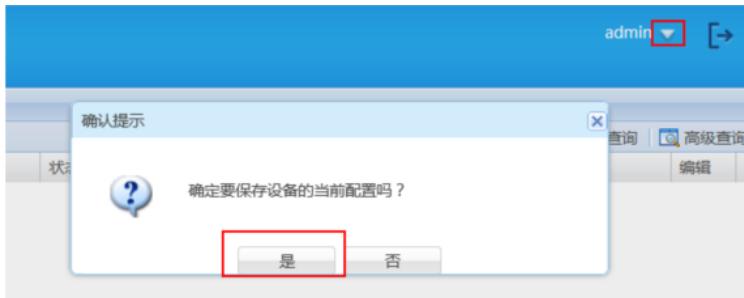
新建安全策略

源安全域	Local
目的安全域	Untrust
策略ID	(0-65534) <input checked="" type="checkbox"/> 自动编号
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
描述信息	(1-127字符)
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 拒绝 <input type="radio"/> 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 [多选]
VRF	公网
记录日志	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
开启策略匹配统计	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭
启用策略	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭

**确定** **取消**

### 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：



#### 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。



#### 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）、配置预共享密钥，此处配置为123456  
、其余选择默认即可。



**编辑IKE对等体**

对等体名称:	IKE	(范围:1~16个字符)
虚接口:	ipseco	
对端地址:	101.88.26.34	(IP 或 域名)
协商模式:	<input checked="" type="radio"/> 主模式 <input type="radio"/> 野蛮模式	
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:	<input checked="" type="radio"/> 开启 <input type="radio"/> 关闭	
DPD周期:	10	秒(范围:1~60秒, 缺省值:10)
DPD超时时间:	30	秒(范围:1~300秒, 缺省值:30)
<input type="button" value="修改"/> <input type="button" value="取消"/>		

### 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：

**IPSec安全提议列表**

安全提议:	IPsec	AH算法	ESP算法
安全协议:	ESP	---	3DES-SHA1

**编辑IPSec安全提议**

安全提议名称:	IPsec	(范围:1~31个字符)
安全协议类型:	<input type="radio"/> AH <input checked="" type="radio"/> ESP <input type="radio"/> AH+ESP	
ESP验证算法:	SHA1	
ESP加密算法:	3DES	
<input type="button" value="修改"/> <input type="button" value="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IPSec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：

安全策略名称： ipsec (范围:1~16个字符)  
 是否启用： 启用  
 本地子网IP/掩码： 192.168.20.0 / 255.255.255.0  
 对端子网IP/掩码： 192.168.10.0 / 255.255.255.0  
 协商类型： IKE协商  
 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 (范围:120~604800, 缺省值:28800)  
 触发模式： 流量触发

### 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。

目的地址： 192.168.10.0  
 子网掩码： 255.255.255.0  
 下一跳地址：  
 出接口： ipsec0  
 描述： (可选, 范围:1~15个字符)

### 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。

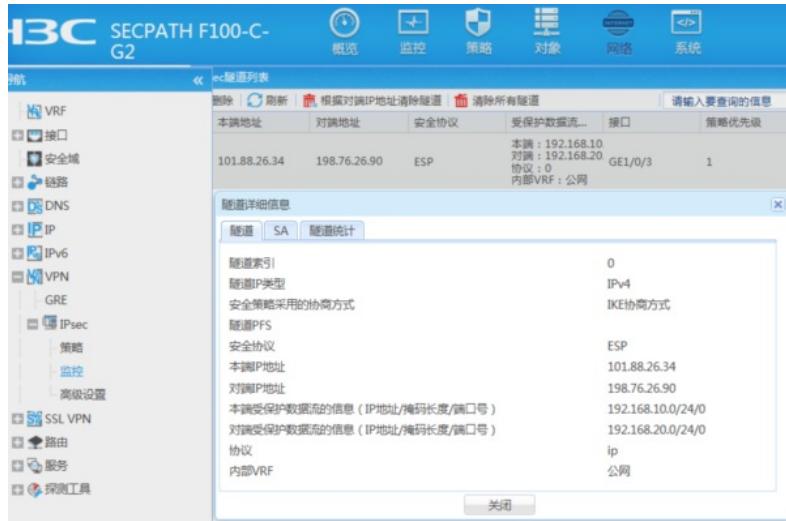
```
C:\Users\sfw1081>ping 192.168.10.3

正在 Ping 192.168.10.3 具有 32 字节的数据:
请求超时。
请求超时。
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
```

#### 3.3.2 查看IPSEC监控信息

防火墙侧：在“网络”>“VPN”>“IPsec”>“监控”中查看对端信息，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

名称	方向	隧道两端	AH SPI	AH 算法	ESP SPI	ESP 算法	掩码
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

配置关键点