F1000-AK系列和ERG2路由器IPsec VPN主模式配置（WEB）

IPSec VPN　IPSec VPN　zhiliao_8mkdB　2018-11-24 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

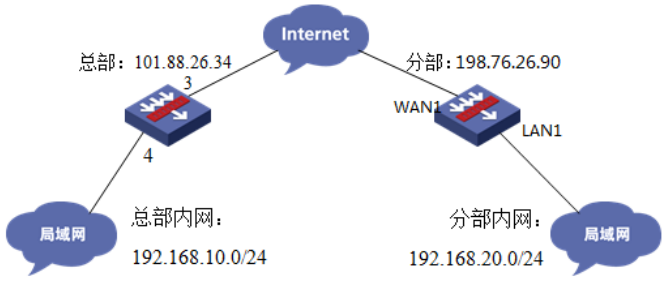
本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙和ERG2产品系列路由器对接

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

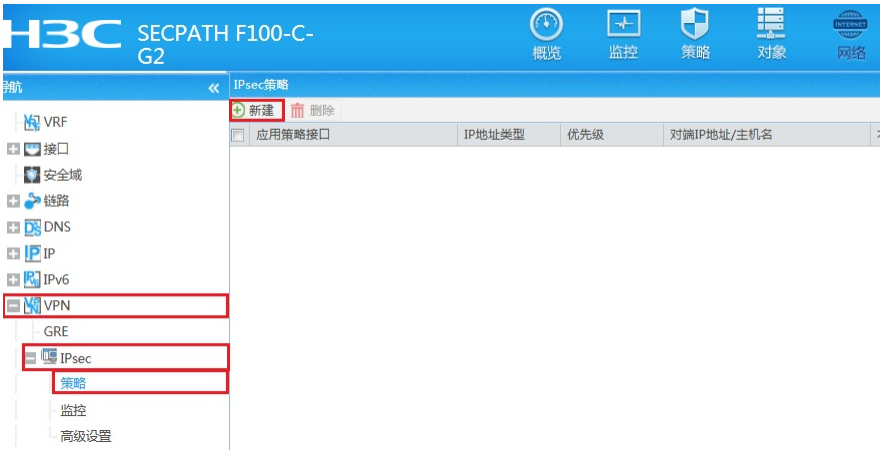


配置步骤

3 总部侧IPSEC VPN配置

3.1 IPsec策略配置

#在“网络”>“VPN”>“策略”中点击新建。

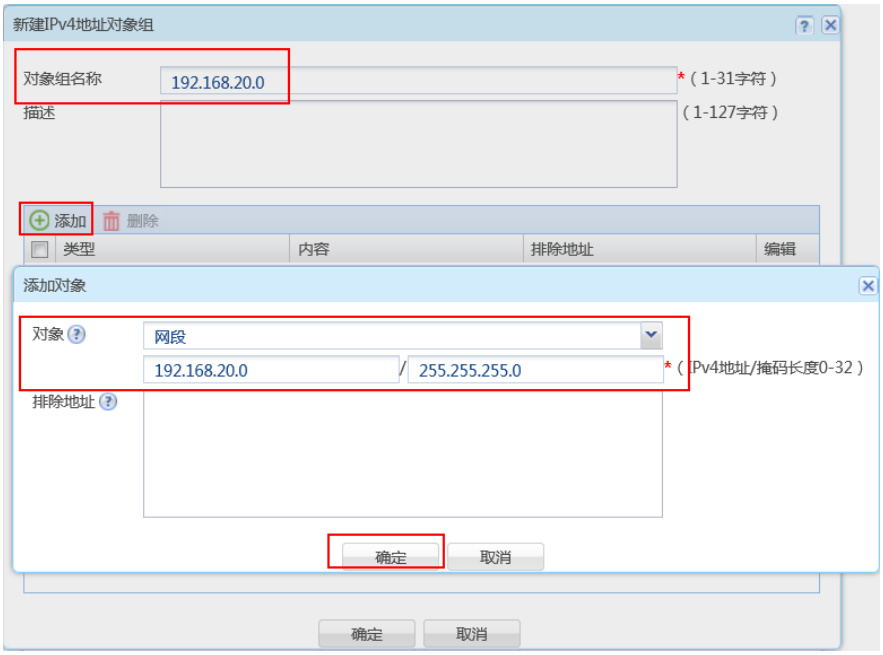


#在“基本配置”中“接口”选择接入外网的1/0/3接口，“优先级”设置为1（优先级代表了策略匹配顺序，当存在多条VPN隧道时需要对各VPN隧道优先级进行设置），“认证方式”选择域共享密钥，建立VPN两端隧道的域共享密钥必须一致。对端ID设置对IP地址即分公司公网地址，本端ID默认为本端公网接口IP地址。在保护的数据流中添加源为总部内网网段192.168.10.0/24，目的IP地址为分部内网网段192.168.20.0/24。高级设置中配置ike参数和ipsec参数，该参数需要保证总部和分支必须一致。

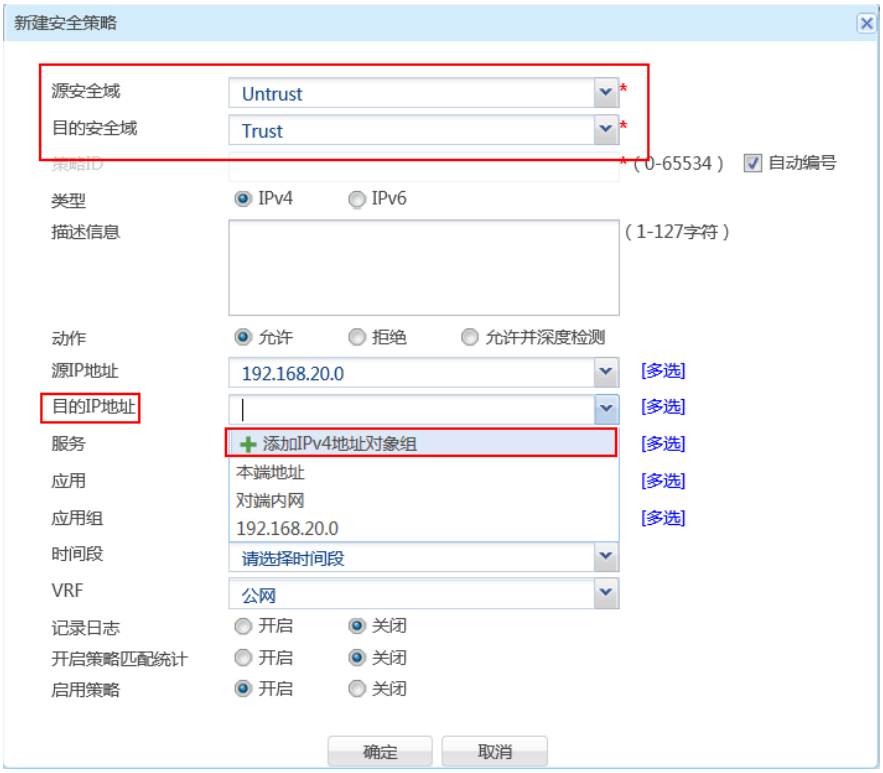
3.2 配置安全策略，放通IPSEC感兴趣流的数据策略

#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”

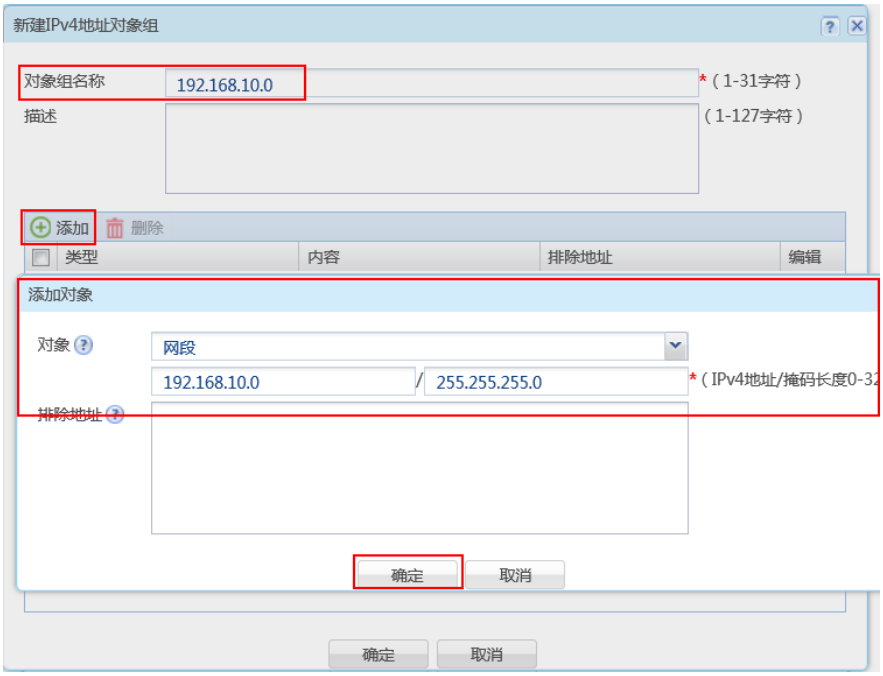
#配置对象组名称为“192.168.20.0”，点击“添加”，对象地址为192.168.20.0网段，为分支内网段地址



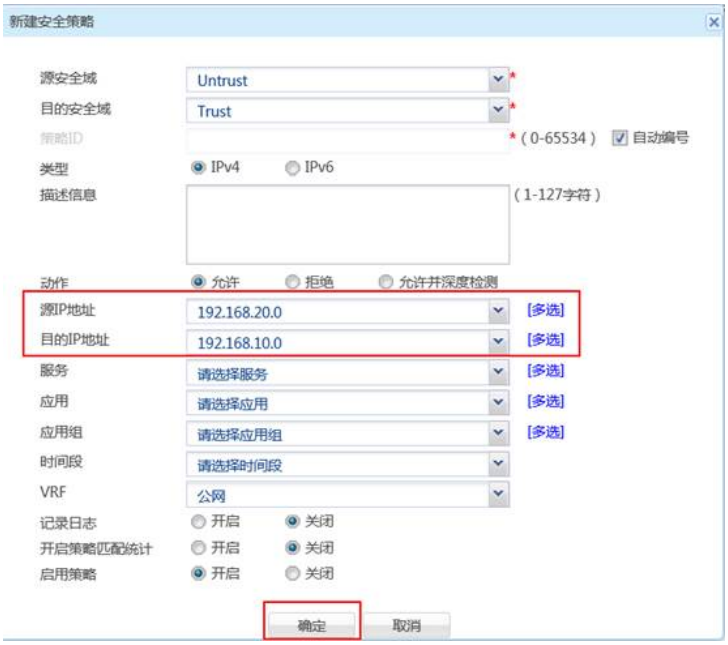
#在“策略”>“安全策略”>点击“新建”，“目的IP地址”中点击“添加IPV4地址对象组”



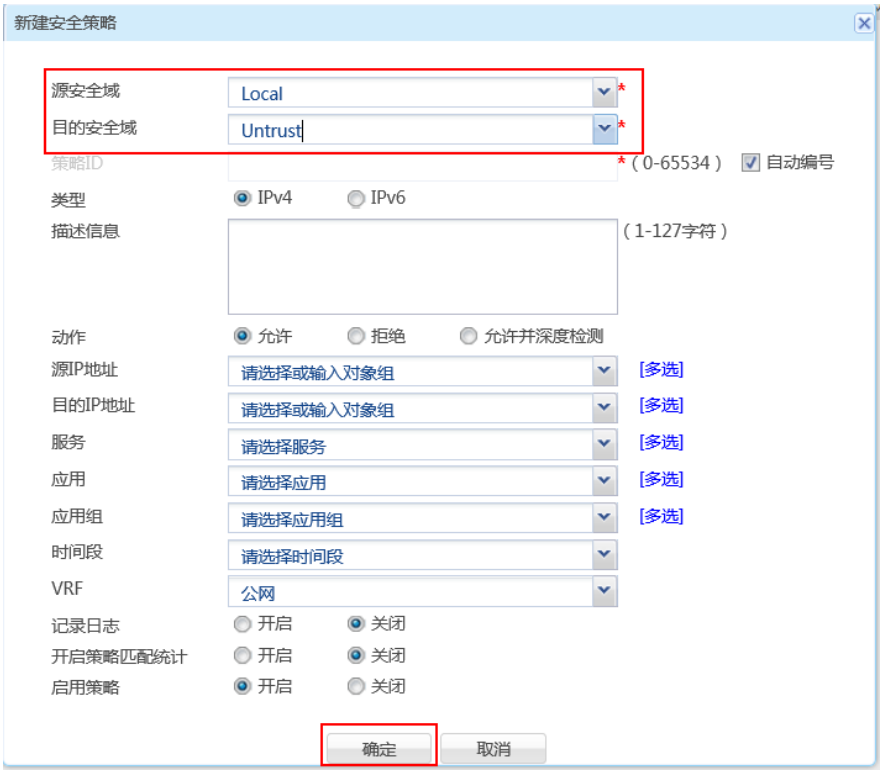
#配置对象组名称为“192.168.10.0”，点击“添加”，对象地址为192.168.10.0网段，为总部内网网段地址



#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



3.3 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

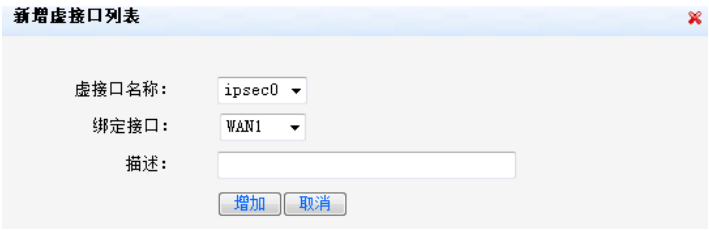


3.4 保存配置

4 分支侧IPsec配置

4.1 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：



4.2 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。

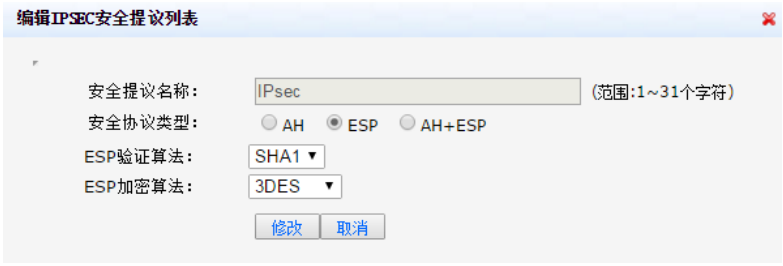
4.3 配置IKE对等体

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101.88.26.34、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。

4.4 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：



4.5 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：

4.5 配置去往对端子网的静态路由

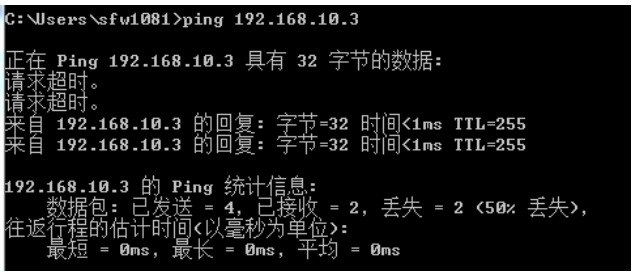
单击【高级设置】--【路由设置】--【静态路由】，目的地址配置成对端子网，即192.168.10.0，子网掩码为255.255.255.0，出接口为ipsec0虚接口。

6 测试VPN是否连通

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。



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

配置关键点