ACG1000系列与V7平台防火墙对接IPSEC VPN配置举例（适用于两端固定地址组网）

IPSec VPN　叶佳豪　2019-08-16 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

本案例适用于软件平台为ACG1000系列应用控制网关：ACG10X0、ACG1000-AKXXX等。

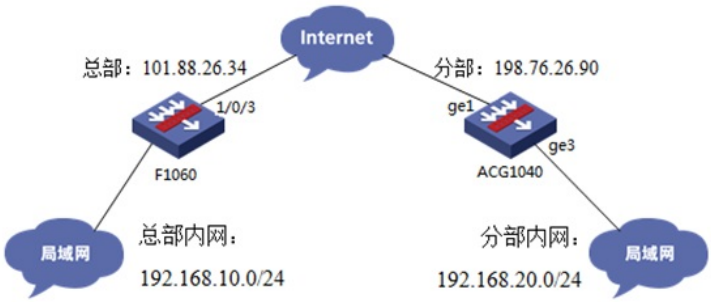
注：本案例是在ACG1040的Version 1.10, Release 6609P06版本上进行配置和验证的。

1.2 配置需求及实现的效果

因公司业务拓展需要将处于两地的公司网络通过IPSEC VPN连通，使总部和分部网络可以相互访问。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（F1060）	1/0/3	101.88.26.34/30	101.88.26.33	1/0/4	192.168.10.0/24
分部（ACG1040）	ge1	198.76.26.90/30	198.76.26.89	ge3	192.168.20.0/24

2 组网图

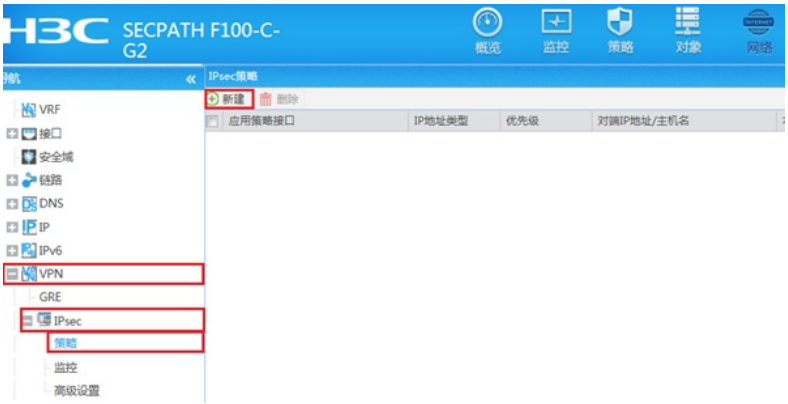


配置步骤

3 配置步骤

3.1 两端配置上网配置

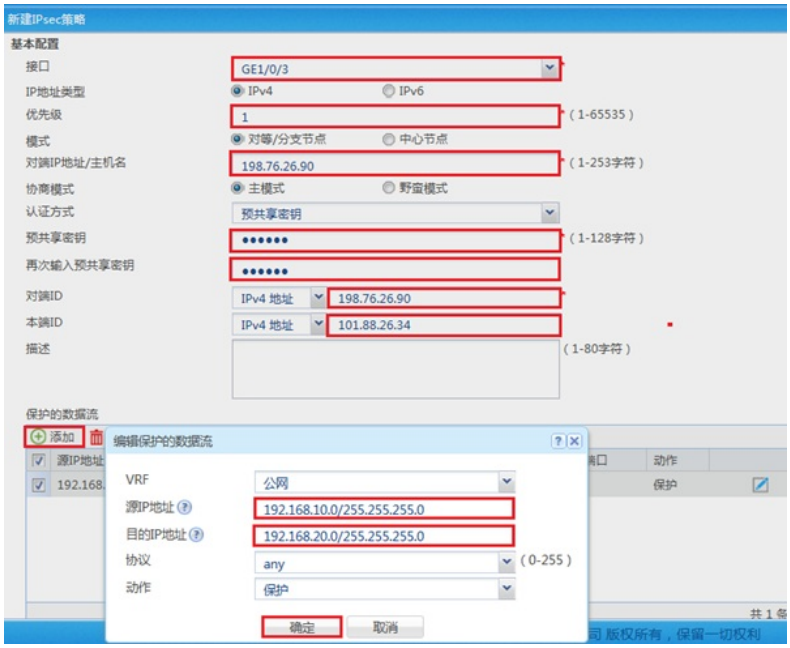
本文档重点给出两台设备IPSEC VPN配置步骤，上网配置略。



3.2 总部侧防火墙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。

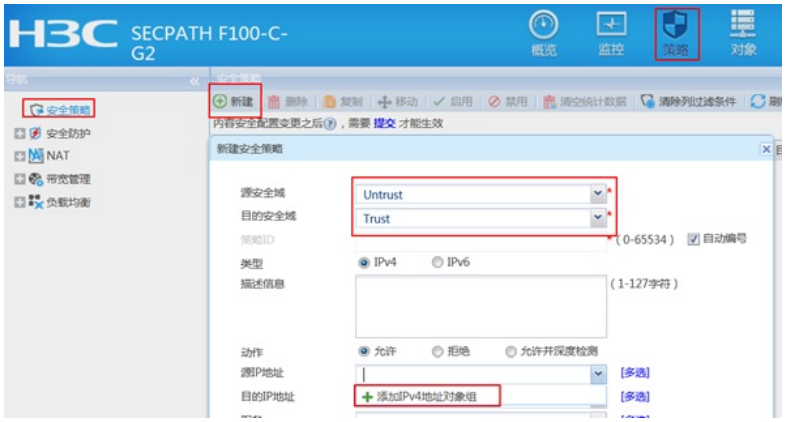


默认防火墙的IPSEC提议为ESP/SHA1/AES-128，IKE安全提议为：

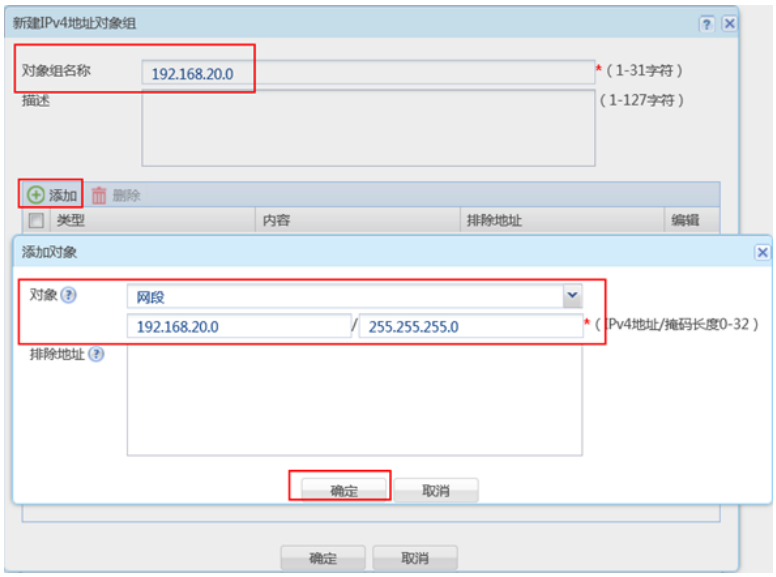
优先级	认证方式	认证算法	加密算法	DH	IKE SA 生存周期
Default	预共享密钥	SHA1	DES-CBC	DH group 1	86400

3.3 总部侧配置安全策略，放通IPSEC感兴趣流的数据策略

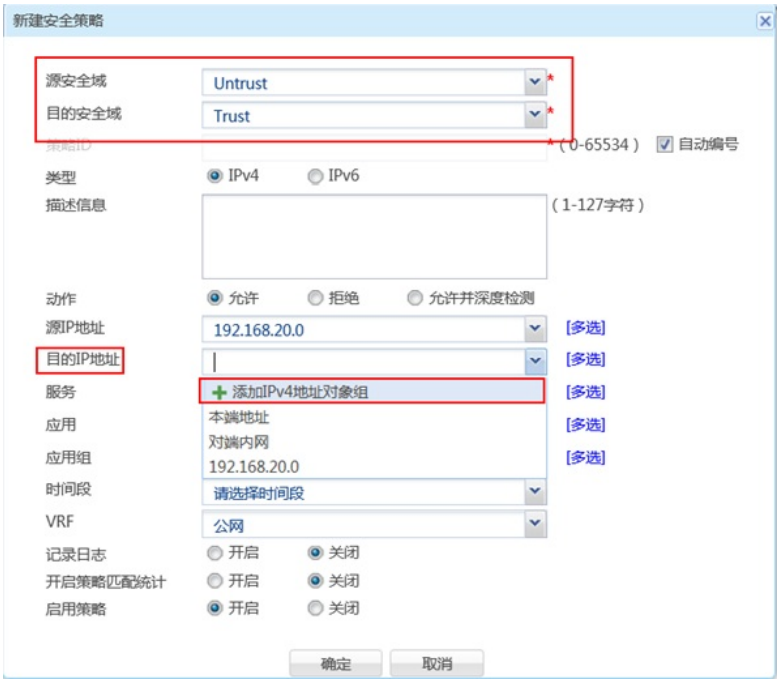
#在“策略”>“安全策略”>点击“新建”，“源IP地址”中点击“添加IPV4地址对象组”



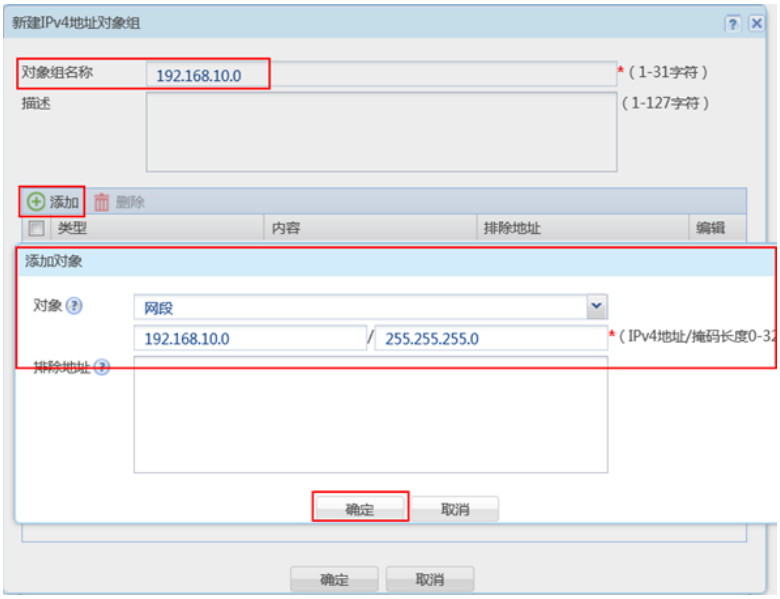
#配置对象组名称为“192.168.20.0”，点击“添加”，对象地址为192.168.20.0网段，为分支内网段地址



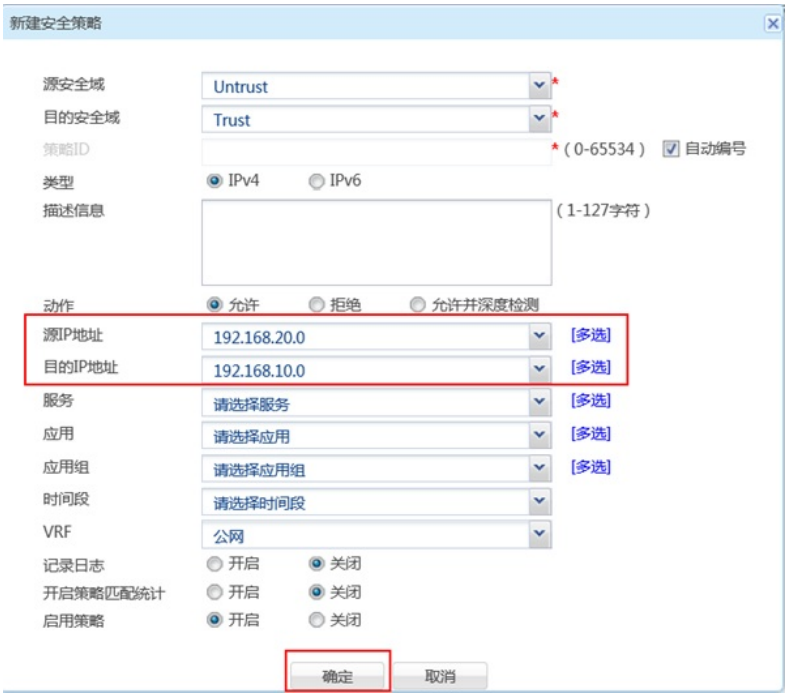
#在“策略”>“安全策略”>点击“新建”，“目的IP地址”中点击“添加IPV4地址对象组”



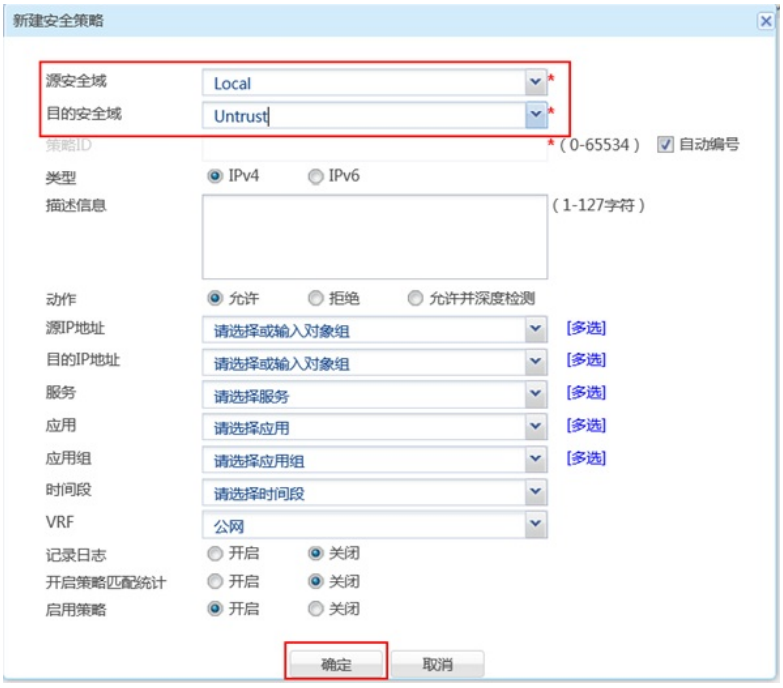
#配置对象组名称为“192.168.10.0”，点击“添加”，对象地址为192.168.10.0网段，为总部内网网段地址



#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



3.4 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

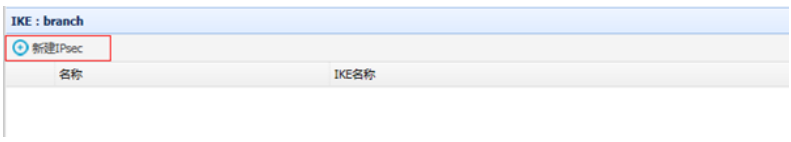


3.5 分部侧IPSEC VPN策略配置

#在 “VPN”>“IPsec第三方对接”中新建IKE对等体。

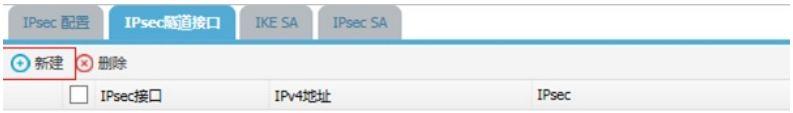
#基本设置中网关名称设置为“branch”，对端网关地址为101.88.26.34，模式设置为主模式，预共享秘钥与防火墙设置一致，IKE协商交互方案加密算法为DES，认证算法为SHA。

#新建IPsec安全提议。



#设置通道名称为“branch”，IKE对等体调用“branch”，ESP加密和认证算法设置为AES128_SHA1，设置完成后点击提交。

#新建IPSEC 隧道接口。



#地址选项中添加本地子网到对端子网的规则。

3.6 配置保存

#在设备管理界面右上角点击配置保存，保存当前配置。

3.7 结果测试

#总部侧分支侧电脑可以正常通信。

```
<H3C>ping -a 192.168.10.1 192.168.20.2
Ping 192.168.20.2 (192.168.20.2) from 192.168.10.1: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.20.2: icmp_seq=0 ttl=127 time=1.550 ms
56 bytes from 192.168.20.2: icmp_seq=1 ttl=127 time=1.157 ms
56 bytes from 192.168.20.2: icmp_seq=2 ttl=127 time=0.876 ms
56 bytes from 192.168.20.2: icmp_seq=3 ttl=127 time=0.894 ms
56 bytes from 192.168.20.2: icmp_seq=4 ttl=127 time=0.966 ms
```

#在总部侧查看IKE与IPSEC SA。

```
<H3C>display ike sa
  Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------------
```

107 198.76.26.90 RD IPsec

Flags:

RD--READY RL--REPLACED FD-FADING RK-REKEY

<H3C>dius

<H3C>dis

<H3C>display ipse

<H3C>display ipsec sa

Interface: GigabitEthernet1/0/3

IPsec policy: branch

Sequence number: 1

Mode: ISAKMP

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1428

Tunnel:

local address: 101.88.26.34

remote address: 198.76.26.90

Flow:

sour addr: 192.168.10.0/255.255.255.0 port: 0 protocol: ip

dest addr: 192.168.20.0/255.255.255.0 port: 0 protocol: ip

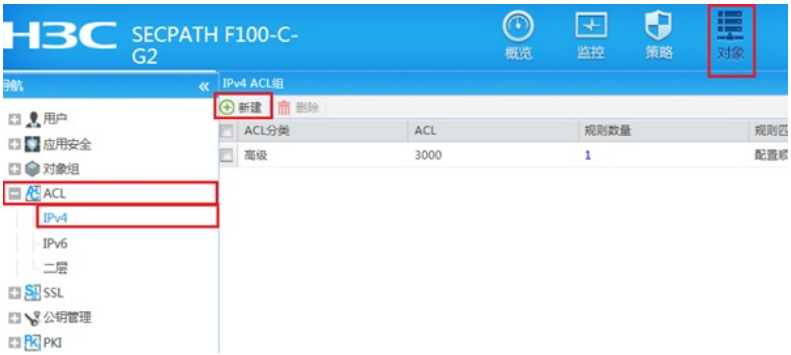
#分部侧设备查看IPSEC连接状态：

3.8 注意事项

3.8.1 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。



#在“类型”中选择高级ACL，ACL编号输入3999。

#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。

#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。

#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。


H3C SECPATH F100-C-G2
概览
监控
策略
导航
安全策略
安全防护
NAT
NAT快速配置
NAT动态转换
策略配置
NAT地址组
NAT内部服务器
NAT静态转换
NAT444动态转换
NAT444静态转换
NAT高级设置
NAT出方向动态转换
新建
复制
开启
关闭
删除
按页面显示导出
接口
接口描述
ACL
地址组
新建NAT出方向动态转换
接口
GE1/0/3
ACL
3999
转换后源地址
NAT地址组
接口IP地址
VRF
公网
转换模式
PAT
不转换端口
PAT方式分配端口时尽量不转换端口
启用规则
启用此条规则

配置关键点