F10X0/F50X0系列防火墙和ERG2采用公网固定地址方式搭建IPSEC VPN配置案例（主模式命令行配置、NAQ保活VPN隧道）

IPSec VPN　程咪　2019-09-23 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F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

ERG2系列路由器：ER5200G2、ER8300G2、ER3200G2等

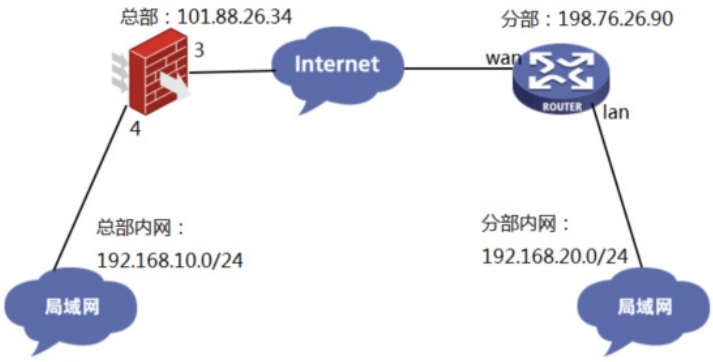
注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

1.2 配置需求及实现的效果

分部是台ER5200G2路由器，总部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	1/0/3	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 防火墙和ERG2路由器上网配置

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。

ERG2路由器上网配置请参考“2.2.2 路由器使用静态地址方式上网配置方法”进行配置，本文只针对IPSEC VPN配置进行介绍。

3.2 总部侧创建IPSEC兴趣流匹配到分部的数据

#创建IPSEC的感兴趣流，用于匹配IPSEC数据。

<H3C>system-view

[H3C]acl advanced 3999

[H3C-acl-ipv4-adv-3999]rule permit ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255

[H3C-acl-ipv4-adv-3999]quit

#创建acl 3888调用在外网接口用于排除IPSEC兴趣流不做NAT。

[H3C]acl advanced 3888

[H3C-acl-ipv4-adv-3888]rule deny ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255

[H3C-acl-ipv4-adv-3888]rule permit ip source any

[H3C-acl-ipv4-adv-3888]quit

3.3 总部侧创建IPSEC安全提议

#加密类型设置为aes-cbc-128，认证类型设置为sha1。

[H3C]ipsec transform-set 1

[H3C-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128

[H3C-ipsec-transform-set-1]esp authentication-algorithm sha1

[H3C-ipsec-transform-set-1]quit

3.4 总部侧创建IKE安全提议

#IKE安全提议默认的认证类型为sha1，加密类型为DES-CBC，DH组为DH1，所以不需要配置也存在这些参数。

[H3C]ike proposal 1

[H3C-ike-proposal-1]quit

3.5 总部侧创建IKE安全密钥

#创建IKE密钥，地址填写分部侧设备的公网IP，密码设置为123456。

[H3C]ike keychain 1

[H3C-ike-keychain-1]pre-shared-key address 198.76.26.90 key simple 123456

[H3C-ike-keychain-1]quit

3.6 总部侧创建IKE安全框架

#创建IKE安全框架，将本端地址、对端地址、keychain、proposal关联起来。

[H3C]ike profile 1

[H3C-ike-profile-1]keychain 1

[H3C-ike-profile-1]local-identity address 101.88.26.34

[H3C-ike-profile-1]match remote identity address 198.76.26.90

[H3C-ike-profile-1]proposal 1

[H3C-ike-profile-1]quit

3.7 配置全局IKE DPD功能

#创建ike dpd，IKE SA协商成功之后10秒本端会发送DPD探测报文，并等待接收DPD回应报文。若本端在10秒内没有收到DPD回应报文，则会第二次发送DPD探测报文。在此过程中总共会发送三次DPD探测报文，若第三次DPD探测报文发出后10秒仍没收到DPD回应报文，则会删除发送DPD探测报文的IKE SA及其对应的所有IPsec SA。若在此过程中收到了DPD回应报文，则会等待10秒再次发送DPD探测报文

[H3C]ike dpd interval 10 retry 10 periodic

3.8 总部侧创建IPSEC安全策略

#创建IKE安全策略GE1/0/3将transform-set、acl、ike-profile、本端地址、对端地址关联起来。

[H3C]ipsec policy GE1/0/3 1 isakmp

[H3C-ipsec-policy-isakmp-GE1/0/3-1]transform-set 1

[H3C-ipsec-policy-isakmp-GE1/0/3-1]security acl 3999

[H3C-ipsec-policy-isakmp-GE1/0/3-1]local-address 101.88.26.34

[H3C-ipsec-policy-isakmp-GE1/0/3-1]remote-address 198.76.26.90

[H3C-ipsec-policy-isakmp-GE1/0/3-1]ike-profile 1

[H3C-ipsec-policy-isakmp-GE1/0/3-1]quit

3.9 总部侧外网接口调用IPSEC策略和NAT动态转换策略

[H3C]interface GigabitEthernet 1/0/3

[H3C-GigabitEthernet1/0/3]ipsec apply policy GE1/0/3

[H3C-GigabitEthernet1/0/3]nat outbound 3888

[H3C-GigabitEthernet1/0/3]quit

3.10 总部侧配置安全策略放通IPSEC数据

#创建对象组，组名称为192.168.10.0

[H3C]object-group ip address 192.168.10.0

[H3C-obj-grp-ip-192.168.10.0]0 network subnet 192.168.10.0 255.255.255.0

[H3C-obj-grp-ip-192.168.10.0]quit

#创建对象组，名称为192.168.20.0

[H3C]object-group ip address 192.168.20.0

[H3C-obj-grp-ip-192.168.20.0]0 network subnet 192.168.20.0 255.255.255.0

[H3C-obj-grp-ip-192.168.20.0]quit

#创建对象策略，策略名称为Untrust-Trust

[H3C]object-policy ip Untrust-Trust

[H3C-object-policy-ip- Untrust-Trust] rule 0 pass source-ip 192.168.20.0 destination-ip 192.168.10.0

[H3C-object-policy-ip- Untrust-Trust]quit

#创建Untrust到Tust域的域间策略调用Untrust-Trust策略

[H3C]zone-pair security source Untrust destination Trust

[H3C-zone-pair-security-Untrust-Trust]object-policy apply ip Untrust-Trust

[H3C-zone-pair-security-Untrust-Trust]quit

3.11 总部侧配置安全策略，放通Untrust到Local，以及Local到Untrust的策略，用于建立IPSEC 隧道

#创建对象策略，策略名称为Untrust-Local

[H3C]object-policy ip Untrust-Local

[H3C-object-policy-ip-Untrust-Local] rule 0 pass

[H3C-object-policy-ip-Untrust-Local]quit

#创建Untrust到Local域的域间策略调用Untrust- Local策略

[H3C]zone-pair security source Untrust destination Local

[H3C-zone-pair-security-Untrust-Local]object-policy apply ip Untrust-Local

[H3C-zone-pair-security-Untrust-Local]quit

#创建对象策略，策略名称为Local-Untrust

[H3C]object-policy ip Local-Untrust

[H3C-object-policy-ip-Local-Untrust]rule 0 pass
[H3C-object-policy-ip-Local-Untrust]quit
#创建Local到Untrust域的域间策略调用Local-Untrust策略
[H3C]zone-pair security source Local destination Untrust
[H3C-zone-pair-security-Local-Untrust]object-policy apply ip Local-Untrust
[H3C-zone-pair-security-Local-Untrust]quit

3.12 配置NQA，用于保活IPSEC VPN隧道。

创建ICMP-echo类型的NQA测试组（管理员为admin，操作标签为test1），并配置探测报文的目的地址为分部ERG2内网的ip：192.168.20.1，源ip是总部内网的ip：192.168.10.1。
<H3C> system-view
[H3C] nqa entry admin test1
[H3C-nqa-admin-test1] type icmp-echo
[H3C-nqa-admin-test1-icmp-echo] destination ip 192.168.20.1
[H3C-nqa-admin-test1-icmp-echo] source ip 192.168.10.1
配置下一跳地址为101.88.26.33，以便测试报文使用ipsec vpn隧道发给分部设备。
[H3C-nqa-admin-test1-icmp-echo] next-hop ip 101.88.26.33
配置可选参数：一次NQA测试中探测的次数为10，探测的超时时间为500毫秒，测试组连续两次测试开始时间的时间间隔为5000毫秒。
[H3C-nqa-admin-test1-icmp-echo] probe count 10
[H3C-nqa-admin-test1-icmp-echo] probe timeout 500
[H3C-nqa-admin-test1-icmp-echo] frequency 5000
启动ICMP-echo测试操作，并一直进行测试。
[H3C] nqa schedule admin test1 start-time now lifetime forever

3.13 分部创建IPSEC虚接口

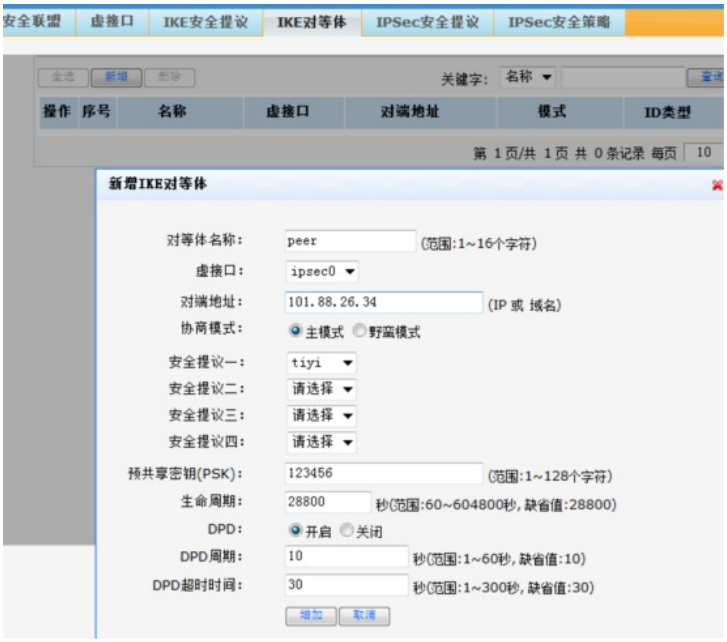
#在“VPN”>“IPSEC VPN”>“虚接口”中点击新建，绑定到外网接口WAN1

3.14 分部创建IKE安全提议

#在“VPN”>“IPSEC VPN”>“IKE安全提议”中点击新建
IKE安全提议的认证类型为SHA1，加密类型为DES，DH组为DH1。

3.15 分部创建IKE对等体

#在“VPN”>“IPSEC VPN”>“IKE对等体”中点击新建
对端地址选择总部公网IP，选择配置好的IKE安全提议，使用主模式，输入IKE 预共享密钥，开启DPD，和总部进行匹配。



3.16 分部创建IPSEC安全提议

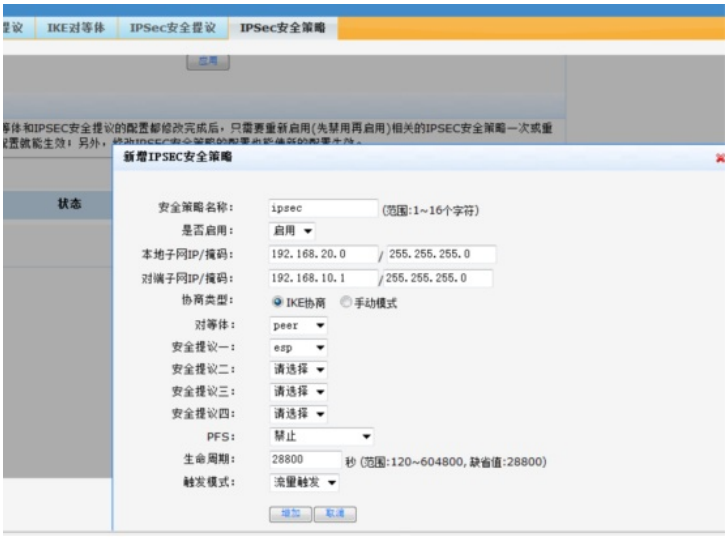
#在“VPN”>“IPSEC VPN”>“IPSEC安全提议”中点击新建

#加密类型设置为aes128，认证类型设置为sha1。

3.17 分部创建IPSEC 安全策略

#在“VPN”>“IPSEC VPN”>“IPSEC 安全策略”中点击新建

本端子网IP为本端需要走VPN的内网地址，对端子网为总部需要走VPN的地址，调用之前创建的IKE对等体和IPSEC的安全提议。



3.18 启用IPSEC安全策略功能

3.19 分部创建去往总部的静态路由

#在“高级设置”>“路由设置”>“静态路由”中点击新建

新增一条静态路由。目的地址为对端的VPN网段。出接口选择IPSEC虚接口。

3.20 隧道验证

V7防火墙侧：

通过命令行查看display ike sa可以看到隧道状态为RD状态表示ike建立完成。

```
[H3C]dis ike sa
    Connection-ID   Remote                Flag         DOI
-------------------------------------------------------------------------
    29              198.76.26.90          RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

#V7防火墙通过display ipsec sa可以看到IPSEC SA基本状态。

```
[H3C]dis ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/3
-------------------------------

  -----------------------------
  IPsec policy: GE1/0/3
  Sequence number: 1
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    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
```

```
[Inbound ESP SAs]
  SPI: 4032357769 (0xf058e589)
  Connection ID: 158913789952
  Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3545
  Max received sequence-number: 8
  Anti-replay check enable: Y
  Anti-replay window size: 64
  UDP encapsulation used for NAT traversal: N
  Status: Active

[Outbound ESP SAs]
  SPI: 1786751150 (0x6a7fa8ae)
  Connection ID: 64424509441
  Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3545
  Max sent sequence-number: 8
  UDP encapsulation used for NAT traversal: N
  Status: Active
```

ERG2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