F10X0/F50X0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（主模式命令行配置）

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F1080、F1070、F5040、F5020等F10X0、F50X0系列的防火墙。

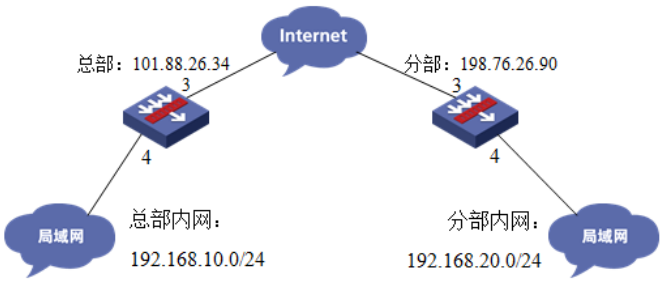
注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

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。

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。

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 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

3.8 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

3.9 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

3.10 总部侧配置安全策略，放通Untrust到Local，以及Local到Utrust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

3.11 分部侧IPSEC配置方法

#与总部侧配置基本相同，IPSEC感兴趣流需要取反配置。

3.12 保存配置

[H3C]save force

3.13 隧道验证

#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>display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------------
    1               198.76.26.90          RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

#通过display ipsec sa可以看到IPSEC SA基本状态。

```
<H3C>display ipsec sa
------------------------------
Interface: GigabitEthernet1/0/3
------------------------------

  ----------------------------
  IPsec policy: GE1/0/3
  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
```

配置关键点