F10X0/F50X0系列两台防火墙一端固定IP，一端PPPOE拨号搭建IPSEC VPN配置案例（野蛮模式命令行）

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。

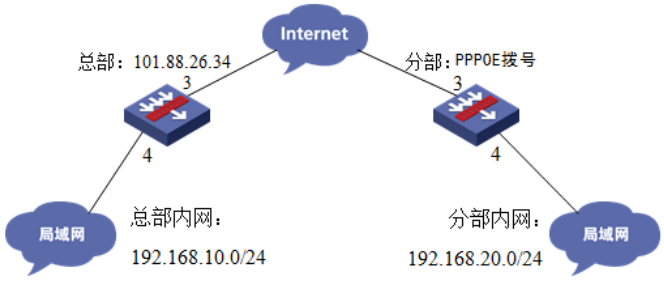
注：本案例分支是F100-C-G2的Version 7.1.064, Release 9510P08版本，总部是F1000-C-G2的Version 7.1.064, Release 9323P1801上进行配置和验证的。

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	PPPOE拨号	自动获取网关	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”及“2.3.1 防火墙外网使用拨号上网配置方法”进行配置，本文只针对IPSEC VPN配置进行介绍。

3.2 总部侧排除IPSEC兴趣流不做NAT

#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 GE1/0/3_IPv4_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0.0.0.0/0，密码设置为123456。

[H3C]ike keychain 1
[H3C-ike-keychain-1]pre-shared-key address 0.0.0.0 0.0.0.0 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，协商模式调整为野蛮模式。本端身份识别为center，分部身份识别为branch。
[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1] exchange-mode aggressive
[H3C-ike-profile-1] local-identity fqdn center
[H3C-ike-profile-1]match remote identity address 0.0.0.0 0.0.0.0
[H3C-ike-profile-1]match remote identity fqdn branch
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]quit

3.7 总部侧创建IPSEC安全策略模板

[H3C]ipsec policy-template GE1/0/3 1
[H3C-ipsec-policy- template-GE1/0/3-1]transform-set GE1/0/3_IPv4_1
[H3C-ipsec-policy- template-GE1/0/3-1]local-address 101.88.26.34
[H3C-ipsec-policy- template-GE1/0/3-1]ike-profile 1
[H3C-ipsec-policy- template-GE1/0/3-1]quit

3.8 总部侧创建IPSEC安全策略

#创建IKE安全策略GE1/0/3将安全策略模板和安全策略绑定。
[H3C]ipsec policy GE1/0/3 1 isakmp template GE1/0/3

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 保存配置

[H3C]save force

3.11 分部侧创建IPSEC兴趣流匹配到总部的数据

#创建IPSEC的感兴趣流，用于匹配IPSEC数据。
<H3C>system
[H3C]acl advanced 3999
[H3C-acl-ipv4-adv-3999]rule permit ip source 192.168.20.0 0.0.0.255 destination 192.168.10.0 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 192.168.20.0 0.0.0.255 destination 192.168.10.0
0.0.0.255
[H3C-acl-ipv4-adv-3888]rule permit ip source any
[H3C-acl-ipv4-adv-3888]quit

3.12 分部侧创建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 GE1/0/3_IPv4_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

3.13 分部侧创建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

3.14 分部侧创建IKE安全密钥

#创建IKE密钥，地址填写总部侧设备的公网IP，密码设置为123456。
[H3C]ike keychain 1

[H3C-ike-keychain-1] pre-shared-key address 101.88.26.34 255.255.255.255 key simple 123456
[H3C-ike-keychain-1]quit

3.15 分部侧创建IKE安全框架

#创建IKE安全框架，匹配keychain 1安全密匙，协商模式调整为野蛮模式。本端身份识别为branch，分部身份识别为center，并制定对端地址为总部侧公网地址。

[H3C]ike profile 1
[H3C-ike-profile-1]keychain 1
[H3C-ike-profile-1]exchange-mode aggressive
[H3C-ike-profile-1] local-identity fqdn branch
[H3C-ike-profile-1] match remote identity fqdn center
[H3C-ike-profile-1] match remote identity address 101.88.26.34 255.255.255.255
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]quit

3.16 分部侧创建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 GE1/0/3_IPv4_1
[H3C-ipsec-policy-isakmp-GE1/0/3-1]security acl 3999
[H3C-ipsec-policy-isakmp-GE1/0/3-1] remote-address 101.88.26.34
[H3C-ipsec-policy-isakmp-GE1/0/3-1]ike-profile 1
[H3C-ipsec-policy-isakmp-GE1/0/3-1]quit

3.17 分部侧外网接口调用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

3.18 保存配置

[H3C]save force

3.19 隧道验证

#分部通过命令行查看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
-------------------------------------------------------------------
    69              101.88.26.34          RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

分支通过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: 218.76.28.33
        remote address: 101.88.26.34
    Flow:
        sour addr: 192.168.20.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.10.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 584061864 (0x22d013a8)
      Connection ID: 519691042817
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3493
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 1859593926 (0x6ed726c6)
      Connection ID: 889058230272
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3493
      Max sent sequence-number: 4
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

#总部通过命令行查看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
-----------------------------------------------------------------------
    19              218.76.28.33          RD           IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

#分支通过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: Template
  -------------------------------
    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: 218.76.28.33
    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: 1859593926 (0x6ed726c6)
      Connection ID: 30064771075
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3463
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 584061864 (0x22d013a8)
      Connection ID: 30064771074
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3463
      Max sent sequence-number: 4
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

配置关键点