防火墙内网接口属于VRF实例外网接口属于缺省VRF实例下IPSEC VPN建立方法

目录

1 配置需求及说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0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。

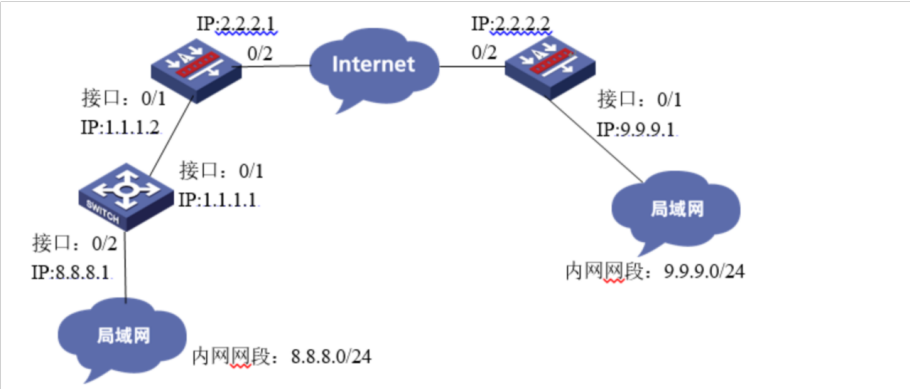
1.2 配置需求及实现的效果

总部和分部各有一台防火墙部署在互联网出口，之前部署的IPSEC VPN业务正常使用。但是现在分支侧为满足业务隔离需求将部分网段数据使用VPN实例进行隔离，因为分支只有一个外网出口在保证之前VPN业务不中断的情况下为新增网段配置IPSEC VPN与总部互通。

IP地址及接口规划如下表所示：

名称	外部接口	地址/掩码	网关	内部接口	内网地址/掩码
总部防火墙	0/2	2.2.2.2/30	2.2.2.1	0/1	9.9.9.1/24
分部防火墙	0/2	2.2.2.1/30	2.2.2.2	0/1	1.1.1.2/30
分部交换机	0/1	1.1.1.1/30	1.1.1.2	0/2	8.8.8.1/24

2 组网图



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 总部侧接口配置

#防火墙0/2接口配置地址2.2.2.2/30、0/1接口配置地址9.9.9.1/24

```
<H3C>system-view
[H3C]interface GigabitEthernet 0/2
[H3C-GigabitEthernet0/2]ip address 2.2.2.2
255.255.255.252
[H3C-GigabitEthernet0/2]iquit
[H3C]interface GigabitEthernet 0/1
[H3C-GigabitEthernet0/1]ip address 9.9.9.1
255.255.255.0
[H3C-GigabitEthernet0/1]iquit
```

3.3 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 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit ip source
9.9.9.0 0.0.0.255 destination 8.8.8.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]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 0 deny ip source
9.9.9.0 0.0.0.255 destination 8.8.8.0 0.0.0.255
[H3C-acl-ipv4-adv-3888]rule permit ip source any
[H3C-acl-ipv4-adv-3888]quit
```

3.4 总部侧创建IPSEC安全提议

#加密类型设置为3des-cbc，认证类型设置为md5。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
```

3.5 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
```

3.6 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 2.2.2.1 key simple 123456
[H3C-ike-keychain-1]quit
```

3.7 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 2.2.2.2
[H3C-ike-profile-1]match remote identity address 2.2.2.1
```

```
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]quit
```

3.8 总部侧创建IPSEC安全策略

#创建IPSEC安全策略1将transform-set、acl、ike-profile、本端地址、对端地址关联起来。

```
[H3C]ipsec policy 1 1 isakmp
[H3C-ipsec-policy-isakmp-GE1/0/3-1]transform-set 1
[H3C-ipsec-policy-isakmp-1-1]security acl 3000
[H3C-ipsec-policy-isakmp-1-1]local-address 2.2.2.2
[H3C-ipsec-policy-isakmp-1-1]remote-address
2.2.2.1
[H3C-ipsec-policy-isakmp-1-1]ike-profile 1
[H3C-ipsec-policy-isakmp-1-1]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 0/2
[H3C-GigabitEthernet0/2]ipsec apply policy 1
[H3C-GigabitEthernet0/2]nat outbound 3888
[H3C-GigabitEthernet0/2]quit
```

3.10 总部侧路由配置

```
[H3C] ip route-static 0.0.0.0 0 2.2.2.1
```

3.11 分部侧创建VRF实例

```
<H3C>system-view
[H3C]ip vpn-instance 1
[H3C-vpn-instance-1]quit
```

3.12 分部侧将连接内网交换机的0/1接口绑定VPN实例

#将分部设备内网接口绑定VPN实例并配置地址

```
[H3C]interface GigabitEthernet0/1
[H3C-GigabitEthernet0/1]ip binding vpn-instance 1
[H3C-GigabitEthernet0/1]ip address 1.1.1.2
255.255.255.0
[H3C-GigabitEthernet0/1]quit
```

#设备0/2为公网接口不绑定VPN实例只配置地址

```
[H3C]interface GigabitEthernet0/2
[H3C-GigabitEthernet0/2]ip address 2.2.2.1
255.255.255.252
[H3C-GigabitEthernet0/2]quit
```

3.13 分部侧创建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 3000
[H3C-acl-ipv4-adv-3000] rule 0 permit ip vpn-
instance 1 source 8.8.8.0 0.0.0.255 destination
9.9.9.0 0.0.0.255
[H3C-acl-ipv4-adv-3000]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 0 deny ip vpn-instance 1 source 8.8.8.0 0.0.0.255 destination 9.9.9.0 0.0.0.255
[H3C-acl-ipv4-adv-3888]rule permit ip source any
[H3C-acl-ipv4-adv-3888]quit
```

3.14 分部侧创建IPSEC安全提议

#加密类型设置为3des-cbc，认证类型设置为md5。

```
[H3C]ipsec transform-set 1
[H3C-ipsec-transform-set-1]esp encryption-algorithm 3des-cbc
[H3C-ipsec-transform-set-1]esp authentication-algorithm md5
[H3C-ipsec-transform-set-1]quit
```

3.15 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
```

3.16 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 2.2.2.2 key simple 123456
[H3C-ike-keychain-1]quit
```

3.17 分部侧创建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 2.2.2.1
[H3C-ike-profile-1]match remote identity address
2.2.2.2
[H3C-ike-profile-1]proposal 1
[H3C-ike-profile-1]inside-vpn vpn-instance 1
[H3C-ike-profile-1]quit
```

3.18 分部侧创建IPSEC安全策略

#创建IPSEC安全策略1将transform-set、acl、ike-profile、本端地址、对端地址关联起来。

```
[H3C]ipsec policy 1 1 isakmp
[H3C-ipsec-policy-isakmp-GE1/0/3-1]transform-set 1
[H3C-ipsec-policy-isakmp-1-1]security acl 3000
[H3C-ipsec-policy-isakmp-1-1]local-address 2.2.2.1
[H3C-ipsec-policy-isakmp-1-1]remote-address
2.2.2.2
[H3C-ipsec-policy-isakmp-1-1]ike-profile 1
[H3C-ipsec-policy-isakmp-1-1]quit
```

3.19 总部侧外网接口调用IPSEC策略和NAT动态转换策略

```
[H3C]interface GigabitEthernet 0/2
[H3C-GigabitEthernet0/2]ipsec apply policy 1
[H3C-GigabitEthernet0/2]nat outbound 3888
```

```
[H3C-GigabitEthernet0/2]quit
```

3.20 分支侧路由配置

```
[H3C] ip route-static 0.0.0.0 0 2.2.2.2
[H3C] ip route-static vpn-instance 1 8.8.8.0 24
1.1.1.1
[H3C] ip route-static vpn-instance 1 9.9.9.0 24
2.2.2.2 public
```

3.21 交换机配置

#交换机则不存在VPN实例，因此简单配置IP地址及路由即可；

```
[H3C]interface GigabitEthernet0/1
[H3C-GigabitEthernet0/1]ip address 1.1.1.1
255.255.255.252
[H3C-GigabitEthernet0/1]quit
[H3C]interface GigabitEthernet0/2
[H3C-GigabitEthernet0/2]ip address 8.8.8.1
255.255.255.0
[H3C-GigabitEthernet0/2]quit
```

#路由配置

```
ip route-static 0.0.0.0 0 1.1.1.2
```

3.22 保存配置

```
[H3C]save force
```

3.23 隧道验证

#从分支侧终端（8.8.8.8）ping总部终端（9.9.9.9）可以正常ping通；

```
<H3C>ping 9.9.9.9
Ping 9.9.9.9 (9.9.9.9) from 8.8.8.8: 56 data bytes, press CTRL_C to break
56 bytes from 9.9.9.9: icmp_seq=0 ttl=254 time=2.000 ms
56 bytes from 9.9.9.9: icmp_seq=1 ttl=254 time=1.000 ms
56 bytes from 9.9.9.9: icmp_seq=2 ttl=254 time=1.000 ms
56 bytes from 9.9.9.9: icmp_seq=3 ttl=254 time=3.000 ms
56 bytes from 9.9.9.9: icmp_seq=4 ttl=254 time=1.000 ms

--- Ping statistics for 9.9.9.9 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.600/3.000/0.800 ms
<H3C> % Feb 13 14:56:39:918 2020 H3C PING/6/PING_STATISTICS: Ping statistics for 9.9.9.9: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip
```

```
min/avg/max/std-dev = 1.000/1.600/3.000/0.800 ms.
```

#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
-------------------------------------------------
----------------
         48                   2.2.2.2
RD           IPsec
```

#通过display ipsec sa可以看到IPSEC SA基本状态。

```
<H3C>display ipsec sa
-------------------------------
Interface: Vlan-interface100
-------------------------------


  -----------------------------
  IPsec policy: 1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 1
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
```

```
    Inside VPN: 1
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: 2.2.2.1
        remote address: 2.2.2.2
    Flow:
        sour addr: 8.8.8.8/255.255.255.0  port: 0
protocol: ip
        dest addr: 9.9.9.9/255.255.255.0  port: 0
protocol: ip

    [Inbound ESP SAs]
      SPI: 3115739214 (0xb9b6684e)
      Connection ID: 4294967298
       Transform set:  ESP-ENCRYPT-3DES-CBC  ESP-
AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
       SA  remaining  duration  (kilobytes/sec):
1843199/2339
      Max received sequence-number: 5
      Anti-replay check enable: Y
```

```
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 141198058 (0x086a82ea)
    Connection ID: 4294967299
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-
AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec):
1843199/2339
    Max sent sequence-number: 5
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

3.24 配置注意点

3.24.1 IKE Keychain后不需要添加VPN实例

在配置ike keychain时后面不需要添加VPN实例，如果将ike keychain添加VPN实例IKE协商将在实例内传输无法到达对端，导致VPN建立失败。

3.24.2 关于路由问题

现场设备共添加3条静态路由，以下为四条路由的解释：

1、此静态路由保证了从缺省实例转发的数据能到外网网关；

```
[H3C] ip route-static 0.0.0.0 0 2.2.2.2
```

2、此条路由保证从VPN实例1中目的地址为9.9.9.0的数据可以通过缺

省路由表进行转发，其中路由器中的“public”为必配参数。

```
[H3C] ip route-static vpn-instance 1 9.9.9.0 24
2.2.2.2 public
```

3、因为用户网关在交换机因此需要有一条VPN实例路由将数据转发至交换机。

```
[H3C] ip route-static vpn-instance 1 8.8.8.0 24
1.1.1.1
```