华为 AR G3 路由 DDNS+IPSEC VPN 配置实例（两端均为动态 IP）

涉及产品：	华为 AR G3 路由器 V300R001	涉及技术：	DDNS+IPSEC VPN
工程师：	冉正锋	E-MAIL：	rzf@corem.com.cn

一、 需求

如上图所示：

两个局域网采用华为 AR G3 系列路由器通过 ADSL 拨号连接到 Internet，总部服务器端局域网地址为 192.168.9.0/24，分支机构客户端局域网地址为 192.168.10.0/24，需要在两台 AR 上配置 IPSEC 实现互通。

二、 配置思路

1、 服务器端申请花生壳 DDNS，自动更新 DNS 解析。

2、 客户端发起 IPSEC 连接。

三、配置步骤

1、 配置 DDNS，首先在花生壳网站申请 DDNS，申请方法详见官网，记下用户名、密码、域名;Username:test2013,密码 tese_2013(密码不能有@),域名:test2013.oicp.net

2、 在服务器端路由器配置 DDNS：脚本如下：

```
dns resolve
dns server 61.128.128.68
ddns policy oray
 url oray://test2013:test_2013@phddnsdev.oray.net  //注意用户名和密码
```

```
interface Dialer1
 link-protocol ppp
 ppp chap user telecomtestadsl
 ppp chap password cipher %$%$LSky<U'bgAqlFw.i{e_5,"BQ%$%$
 ppp pap local-user telecomtestadsl password cipher %$%$T5Mf/$}DLOCui&Y!$4a3,"BC%$%$
 ppp ipcp dns admit-any
 ppp ipcp dns request
 tcp adjust-mss 1460
 ip address ppp-negotiate
 dialer user ppp
 dialer bundle 1
 dialer-group 1
 ddns apply policy oray    //接口下应用 DDNS 策略
nat outbound 3002
```

3、 查看 DDNS 更新是否成功:

```
<RT-PuLuoSi>dis ddns  policy
Policy name          : oray
Policy interval time : 3600
Policy URL           : oray://test2013:test_2013@phddnsdev.oray.net
Policy bind count    : 1


=====  interface Dialer1 ======
  Statuses           : ESTABLISH(2)    // ESTABLISH 表示更新成功
  Refresh            : enable
```

4、 配置 IPSEC，服务器端采用模板方式。配置如下:

服务器端:

```
acl number 3002
 rule 5 deny ip source 192.168.9.0 0.0.0.255 destination 192.168.10.0 0.0.0.255  //VPN 数据不进行 Nat
转换
 rule 10 permit ip source 192.168.9.0 0.0.0.255
```

```
#
ipsec proposal p1       //ipsec 安全提议，默认即可
ike peer server v2       //IKE 对等体 V2
 pre-shared-key simple huaweivpn    //共享密钥
 dpd type periodic      //定时 DPD
 dpd retransmit-interval 5    //每隔 5 秒一个周期
ipsec policy-template temp 1
 ike-peer server
 proposal p1
#
ipsec policy policy99 10 isakmp template temp
#
interface Dialer1
ipsec policy policy99    //应用 Ipsec 策略
nat outbound 3002
#
```

客户端:

```
acl number 3001
 rule 5 permit ip source 192.168.10.0 0.0.0.255 destination 192.168.9.0 0.0.0.255 //配置 Ipsec 兴趣流
#
acl number 3002
 rule 5 deny ip source 192.168.10.0 0.0.0.255 destination 192.168.9.0 0.0.0.255
 rule 10 permit ip source 192.168.10.0 0.0.0.255
#
ipsec proposal p1
#
ike peer toserver v2
 pre-shared-key simple huaweivpn
 dpd type periodic
 dpd retransmit-interval 5
```

```
 remote-address test2013.oicp.net   //此处为域名
#
ipsec policy policy99 10 isakmp
 security acl 3001
 ike-peer toserver
 proposal p1
#
interface Dialer1
ipsec policy policy99
nat outbound 3002
```

三、 验证结果

1、查看 IPSEC SA

```
<RT-Client>dis ipsec  sa


==============================

Interface: Dialer1

 Path MTU: 1492

==============================


  -----------------------------

  IPSec policy name: "policy99"

  Sequence number  : 10

  Acl Group        : 3001

  Acl rule         : 5

  Mode             : ISAKMP

  -----------------------------

    Connection ID     : 148

    Encapsulation mode: Tunnel
```

```
    Tunnel local      : 113.249.121.1
    Tunnel remote     : 14.104.236.9
    Flow source       : 192.168.10.0/255.255.255.0 0/0
    Flow destination  : 192.168.9.0/255.255.255.0 0/0
    Qos pre-classify  : Disable

    [Outbound ESP SAs]
      SPI: 1973192363 (0x759c86ab)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-MD5
      SA remaining key duration (bytes/sec): 1887427558/2246
      Max sent sequence-number: 99
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 2220370819 (0x84582b83)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-MD5
      SA remaining key duration (bytes/sec): 1887431546/2246
      Max received sequence-number: 80
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N
```

2、 Ping 测试

```
<RT-Client>ping -a 192.168.10.1 192.168.9.1
  PING 192.168.9.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.9.1: bytes=56 Sequence=1 ttl=255 time=15 ms
    Reply from 192.168.9.1: bytes=56 Sequence=2 ttl=255 time=14 ms
    Reply from 192.168.9.1: bytes=56 Sequence=3 ttl=255 time=16 ms
    Reply from 192.168.9.1: bytes=56 Sequence=4 ttl=255 time=17 ms
    Reply from 192.168.9.1: bytes=56 Sequence=5 ttl=255 time=15 ms

  --- 192.168.9.1 ping statistics ---
```

```
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 14/15/17 ms
```

四、 配置注意事项

1、 Nat Outbound 必须将兴趣流 Deny 掉

2、 必须配置 DPD，如果不配置 DPD，造成一端掉线，另一端 SA 没有清除。