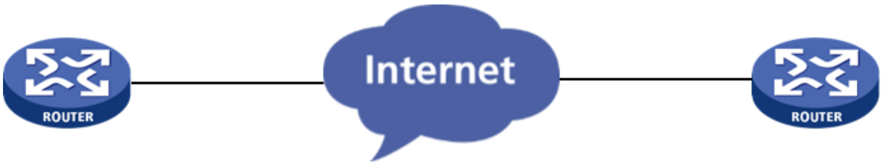
MSR V7不固定地址结合DDNS建立IPsec隧道典型配置案例

IPSec VPN　PPPoE　**孙轶宁**　2018-08-20 发表

组网及说明

总部和分部设备都是MSR3620，均采用PPPoE方式动态获取地址，需要使用DDNS技术使分部与总部设备之间建立IPSec VPN。



配置步骤

1. 总部配置

```
 dialer-group 1 rule ip permit
#
 dns server 114.114.114.114        // DNS服务器配置，必选
#
ddns policy GigabitEthernet0/0       // DDNS配置
 url oray://xxx.oray.net
 username xxx
 password cipher $c$3$FfX6Z0QOVZmxJNi9wBg3TXqVJo2BwHGRgJvieDwFAEM=
 interval 0 0 1
#
interface Dialer0
 ppp pap local-user xxx password cipher $c$3$7Gw/H5un4WfVczBy9PhVSnwUhwtzt0y5IS0M
 dialer bundle enable
 dialer-group 1
 ip address ppp-negotiate
 nat outbound 3200
 ddns apply policy GigabitEthernet0/0 fqdn www.xxx.com  // 接口应用DDNS
 ipsec apply policy 123   // 绑定IPsec策略到Dialer接口上
#
interface GigabitEthernet0/0
 pppoe-client dial-bundle-number 0
#
 ip route-static 0.0.0.0 0 Dialer0   // 配置默认路由
#
acl advanced 3200                        // NAT ACL
 rule 5 deny ip source 192.168.16.0 0.0.15.255 destination 192.168.0.0 0.0.15.255  // 拒绝IPsec数据流
 rule 1000 permit ip
#
ipsec transform-set 123                                    // 配置IPsec安全提议
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template 123 65535                            // 配置IPsec策略模板
 transform-set 123
 ike-profile 123
#
ipsec policy 123 65535 isakmp template 123      // 将模板应用到策略上
#
ike profile 123          // 配置IKE Profile
 keychain 123
 exchange-mode aggressive
 match remote identity fqdn 123
 proposal 65535
#
ike proposal 65535                  // 配置IKE安全提议
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain 123       // 配置IPsec预共享密钥
 pre-shared-key hostname 123 key cipher $c$3$kR2YXCsG8am/6KexFkGTgg2Y+dRksRw3wA==
```

2. 分部配置

```
 dialer-group 1 rule ip permit
#
 dns server 114.114.114.114        // DNS服务器配置，必选
#
interface Dialer0
 ppp pap local-user xxx password cipher $c$3$J+kPr7vTBqgi+CcN3SEgqs6iP5Ytiag8NKTB
 dialer bundle enable
 dialer-group 1
 ip address ppp-negotiate
 nat outbound 3100
 ipsec apply policy 123   // 绑定IPsec策略到Dialer接口上
#
interface GigabitEthernet0/0
 pppoe-client dial-bundle-number 0
#
 ip route-static 0.0.0.0 0 Dialer0    // 配置默认路由
#
acl advanced 3000                    // IPsec ACL
 rule 5 permit ip source 192.168.0.0 0.0.15.255 destination 192.168.16.0 0.0.15.255
#
acl advanced 3100                    // NAT ACL
 rule 5 deny ip source 192.168.0.0 0.0.15.255 destination 192.168.16.0 0.0.15.255   // 拒绝IPsec数据流
 rule 1000 permit ip
#
ipsec transform-set 123                        // 配置IPsec安全提议
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy 123 65535 isakmp                // 配置IPsec策略
 transform-set 123
 security acl 3000
 remote-address www.xxx.com      // 对端地址指定为DDNS地址
 ike-profile 123
#
 ike identity fqdn 123                                 // 配置IKE FQDN
#
ike profile 123                                  // 配置IKE Profile
 keychain 123
 exchange-mode aggressive
 match remote identity address 0.0.0.0 0.0.0.0    // 因为远端地址不固定，因此匹配所有地址
 proposal 65535
#
ike proposal 65535                                    // 配置IKE安全提议
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain 123                              // 配置IPsec预共享密钥，注意这边的pre-shared-key地址必须包含IPsec安全策略里的remote-address，否则会提示找不到pre-share-key
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$bPT/nV7B9eYpBabcqorgjs8502r8yPqTCg==
```

配置关键点

1. 注意在非模板方式端的pre-shared-key地址必须包含IPsec安全策略里的remote-address，**不能是对端的FQDN**，否则会提示找不到pre-share-key，报错如下：

```
*Aug 18 19:47:54:397 2018 xxx IKE/7/EVENT: vrf = 0, local = x.x.x.x, remote = x.x.x.x/500 Pre-shared key matching address x.x.x.x not found
```

2. 注意两台路由器都需要配置DNS。

3. 注意IPsec策略是应用在Dialer口上，而不是物理口。