Typical configuration example of MSR V7 non-fixed address combined with DDNS to establish IPsec tunnel

Routers 蒋笑添 2020-04-14 Published

Network Topology

[Network Topology & Requirements]

Both the headquarters and branch equipment are MSR3620, and both use PPPoE to dynamically obtain addresses. It is necessary to use DDNS technology to establish an IPSec VPN between the branch and headquarters equipment.

Configuration Steps

1. Headquarters configuration

```
#
 dialer-group 1 rule ip permit
#
 dns server 114.114.114.114 // DNS server configuration, required
#
ddns policy GigabitEthernet0 / 0 // DDNS configuration
 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 // interface application DDNS
 ipsec apply policy 123 // Bind the IPsec policy to the Dialer interface
#
interface GigabitEthernet0 / 0
 pppoe-client dial-bundle-number 0
#
 ip route-static 0.0.0.0 0 Dialer0 // Configure the default route
#
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 // reject IPsec dat
a flow
 rule 1000 permit ip
#
ipsec transform-set 123 // Configure IPsec security proposal
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template 123 65535 // Configure IPsec policy template
 transform-set 123
 ike-profile 123
#
ipsec policy 123 65535 isakmp template 123 // Apply the template to the policy
#
ike profile 123 // Configure IKE Profile
 keychain 123
```

```
 exchange-mode aggressive
 match remote identity fqdn 123
 proposal 65535
#
ike proposal 65535 // Configure IKE proposal
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain 123 // Configure IPsec pre-shared key
 pre-shared-key hostname 123 key cipher $c$3$kR2YXCsG8am/6KexFkGTgg2Y+dRksRw3wA==
```

2. Branch configuration

```
#
 dialer-group 1 rule ip permit
#
 dns server 114.114.114.114 // DNS server configuration, required
#
interface Dialer0
 ppp pap local-user xxx password cipher $c$3$JkPr7vTBqgi+CcN3SEgqs6iP5Ytiag8NKTB
 dialer bundle enable
 dialer-group 1
 ip address ppp-negotiate
 nat outbound 3100
 ipsec apply policy 123 // Bind the IPsec policy to the Dialer interface
#
interface GigabitEthernet0 / 0
 pppoe-client dial-bundle-number 0
#
 ip route-static 0.0.0.0 0 Dialer0 // Configure the default route
#
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 // reject IPsec dat
a flow
 rule 1000 permit ip
#
ipsec transform-set 123 // Configure IPsec security proposal
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy 123 65535 isakmp // Configure IPsec policy
 transform-set 123
 security acl 3000
 remote-address www.xxx.com // The peer address is designated as the DDNS address
 ike-profile 123
#
 ike identity fqdn 123 // Configure IKE FQDN
#
ike profile 123 // Configure IKE Profile
 keychain 123
 exchange-mode aggressive
 match remote identity address 0.0.0.0 0.0.0.0 // Because the remote address is not fixed, match all a
ddresses
 proposal 65535
#
ike proposal 65535 // Configure IKE proposal
 encryption-algorithm 3des-cbc
 authentication-algorithm md5
#
ike keychain 123  // Configure the IPsec pre-shared key. Note that the pre-shared-key address her
```

e must include the remote-address in the IPsec security policy, otherwise it will prompt that th e pre-share-key cannot be found.

pre-shared-key address 0.0.0.0 0.0.0.0 key cipher c3$bPT/nV7B9eYpBabcqorgjs8502r8yPqTCg ==

Key Configuration

1. Note that the pre-shared-key address on the non-template side must contain the remote-address in the IPsec security policy, and **cannot be the FQDN of the peer**, otherwise it will prompt that the pre-share-key cannot be found, and the error is as follows:

* 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. Note that both routers need to be configured with DNS.

3. Note that the IPsec policy is applied to the Dialer port, not the physical port.