SR6600路由器公网作MPLS L3VPN Over GRE Over IPsec备份和NAT多实例功能的配置

管祥杰 2008-10-06 发表

SR6600路由器公网作MPLS L3VPN Over GRE Over IPsec备份和NAT多实例上Internet功能的配置

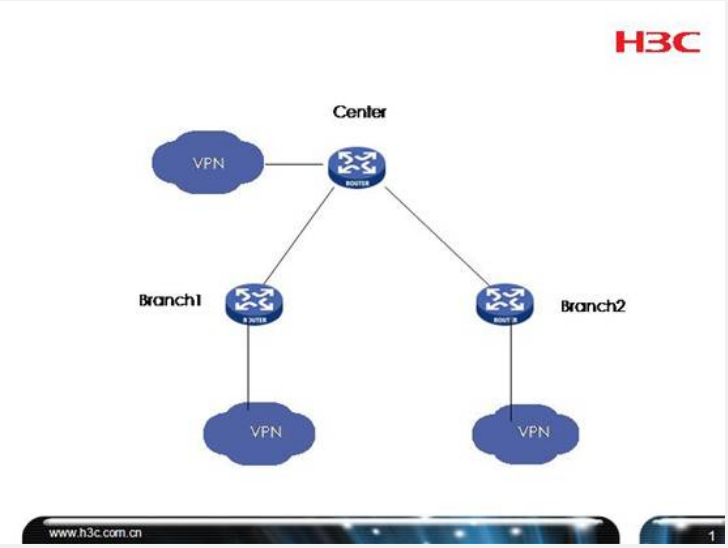
关键字：SR66; MPLS; L3VPN; BGP; OSPF; GRE; IPSec; NAT多实例

一、组网需求:

三台SR66分别是一个总部和2个分支路由器，全部是MPLS L3VPN中的PE设备，3台路由器间使用MPLS网络作为VPN的主用网络，要求主用MPLS网络断开情况下Internet上组建MPLS L3VPN Over GRE Over IPSec作为VPN的备份，另外要求总部和分支的VPN都可以自由访问Internet，不需要总部和分支之间相互转发。

设备清单：SR6600路由器3台

二、组网图:



三、配置步骤:

Center
//配置本地的IKE名字 **ike local-name 1.1.1.1** # //配置OSPF和BGP的Router ID **router id 1.1.1.1** # //配置VPN实例vpna **ip vpn-instance vpna** **route-distinguisher 1:1** **vpn-target 1:1 export-extcommunity** **vpn-target 1:1 import-extcommunity** # //配置mpls lsr-id **mpls lsr-id 1.1.1.1** # //使能MPLS **mpls** # //使能MPLS LDP **mpls ldp** # //配置分支1的IKE Peer，野蛮模式和NAT穿越 **ike peer 2.2.2.2** **exchange-mode aggressive**

```
 exchange-mode aggressive
 pre-shared-key h3c
 remote-name 2.2.2.2
 nat traversal
#
//配置分支2的IKE Peer，野蛮模式和NAT穿越
ike peer 3.3.3.3
 exchange-mode aggressive
 pre-shared-key h3c
 remote-name 3.3.3.3
 nat traversal
#
//配置IPSec提议
ipsec proposal def
#
//IPSec策略branch配置，序号1到分支1，序号2到分支2
ipsec policy branch 1 isakmp
 security acl 3333
 ike-peer 2.2.2.2
 proposal def
#
ipsec policy branch 2 isakmp
 security acl 3334
 ike-peer 3.3.3.3
 proposal def
#
//ACL 3000用于NAT多实例
acl number 3000
 rule 0 permit ip vpn-instance vpna
//ACL 3333用于匹配总部到分支1的GRE
acl number 3333
 rule 0 permit gre source 100.1.1.1 0 destination 100.2.2.2 0
//ACL 3334用于匹配总部到分支2的GRE
acl number 3334
 rule 0 permit gre source 100.1.1.1 0 destination 100.3.3.3 0
#
//用于建立BGP邻居的环回接口
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
//用于建立GRE的环回接口
interface LoopBack100
 ip address 100.1.1.1 255.255.255.255
#
//连接Internet的接口
interface GigabitEthernet0/1
 port link-mode route
 //NAT多实例配置
 nat outbound 3000
 ip address 200.1.1.1 255.255.255.0
 //绑定IPSec策略
 ipsec policy branch
#
//连接MPLS网络的接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.2.3.1 255.255.255.0
 mpls
 mpls ldp
#
//连接vpna的接口
interface GigabitEthernet1/0
 port link-mode route
 ip binding vpn-instance vpna
 ip address 11.2.2.2 255.255.255.0
#
//到分支1的GRE隧道
interface Tunnel0
 description to2.2.2.2
 ip address 1.2.0.1 255.255.255.252
 source LoopBack100
 destination 100.2.2.2
 //使能GRE接口的MPLS和LDP
 mpls
 mpls ldp
#
//到分支2的GRE隧道
interface Tunnel1
 description to3.3.3.3
 ip address 1.3.0.1 255.255.255.252
 source LoopBack100
 destination 100.3.3.3
 //使能GRE接口的MPLS和LDP
 mpls
 mpls ldp
#
//BGP部分配置
bgp 100
 undo synchronization
```

```
 group 100 internal
 peer 100 connect-interface LoopBack0
 peer 2.2.2.2 group 100
 undo peer 2.2.2.2 connect-interface
 peer 3.3.3.3 group 100
 undo peer 3.3.3.3 connect-interface
 #
 ipv4-family vpnv4
  peer 100 enable
  peer 2.2.2.2 enable
  peer 2.2.2.2 group 100
  peer 3.3.3.3 enable
  peer 3.3.3.3 group 100
 #
 ipv4-family vpn-instance vpna
  import-route direct
#
//OSPF部分配置，只将MPLS相关的接口（Loopback0、G0/0和Tunnel）加入到OSPF
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 1.2.3.0 0.0.0.255
  network 1.2.0.0 0.0.0.3
  network 1.3.0.0 0.0.0.3
#
 //保证IPSec的路由，即访问Internet的路由
 ip route-static 0.0.0.0 0.0.0.0 200.1.1.254
 //配置保证vpna可以访问Internet的静态路由，必须要指定Internet出接口
 ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 GigabitEthernet0/1 200.1.1.254
#
```

Branch1

```
#
 //本地IKE名字
 ike local-name 2.2.2.2
#
 //OSPF和BGP的router id
 router id 2.2.2.2
#
//VPN实例vpna
ip vpn-instance vpna
 route-distinguisher 2:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
#
mpls
#
mpls ldp
#
//连接到总部的IKE Peer
ike peer 1.1.1.1
 exchange-mode aggressive
 pre-shared-key h3c
 remote-name 1.1.1.1
 remote-address 200.1.1.1
 nat traversal
#
ipsec proposal def
#
//连接到总部的IPSec策略配置
ipsec policy center 1 isakmp
 security acl 3333
 ike-peer 1.1.1.1
 proposal def
#
//ACL 3000用于NAT多实例
acl number 3000
 rule 0 permit ip vpn-instance vpna
//ACL 3333用于匹配到总部的GRE
acl number 3333
 rule 0 permit gre source 100.2.2.2 0 destination 100.1.1.1 0
#
//用于建立BGP连接和Router ID的环回接口
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
//用于建立GRE连接的环回接口
interface LoopBack100
 ip address 100.2.2.2 255.255.255.255
#
//连接Internet的接口
interface GigabitEthernet0/1
 port link-mode route
 //NAT多实例配置
 nat outbound 3000
 ip address 200.1.1.2 255.255.255.0
 //IPSec策略配置
 ipsec policy center
```

```
#
//连接MPLS网络接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.2.3.2 255.255.255.0
 mpls
 mpls ldp
#
//连接VPNA的接口
interface GigabitEthernet1/0
 port link-mode route
 ip binding vpn-instance vpna
 ip address 12.2.2.2 255.255.255.0
#
//到总部的GRE隧道接口
interface Tunnel0
 ip address 1.2.0.2 255.255.255.252
 source LoopBack100
 destination 100.1.1.1
 //使能MPLS和LDP
 mpls
 mpls ldp

#
//BGP部分配置
bgp 100
 undo synchronization
 group 100 internal
 peer 100 connect-interface LoopBack0
 peer 1.1.1.1 group 100
 peer 3.3.3.3 group 100
 #
 ipv4-family vpnv4
  peer 100 enable
  peer 1.1.1.1 enable
  peer 1.1.1.1 group 100
  peer 3.3.3.3 enable
  peer 3.3.3.3 group 100
 #
 ipv4-family vpn-instance vpna
  import-route direct
#
//OSPF部分配置，注意只将MPLS相关接口加入区域0
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 1.2.3.0 0.0.0.255
  network 1.2.0.0 0.0.0.3
#
 //访问Internet的默认路由
 ip route-static 0.0.0.0 0.0.0.0 200.1.1.254
 //配置保证vpna可以访问Internet的静态路由，必须要指定Internet出接口
 ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 GigabitEthernet0/1 200.1.1.254
#
```

Branch2

```
#
 //本地IKE名字
 ike local-name 3.3.3.3
#
 //OSPF和BGP的router id
 router id 3.3.3.3
#
//VPN实例vpna
ip vpn-instance vpna
 route-distinguisher 3:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
mpls lsr-id 3.3.3.3
#
mpls
#
mpls ldp
#
//连接到总部的IKE Peer
ike peer 1.1.1.1
 exchange-mode aggressive
 pre-shared-key h3c
 remote-name 1.1.1.1
 remote-address 200.1.1.1
 nat traversal
#
ipsec proposal def
#
//连接到总部的IPSec策略配置
ipsec policy center 1 isakmp
 security acl 3333
 ike-peer 1.1.1.1
```

```
 proposal def
#
//ACL 3000用于NAT多实例
acl number 3000
 rule 0 permit ip vpn-instance vpna
//ACL 3333用于匹配到总部的GRE
acl number 3333
 rule 0 permit gre source 100.3.3.3 0 destination 100.1.1.1 0
#
//用于建立BGP连接和Router ID的环回接口
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
//用于建立GRE连接的环回接口
interface LoopBack100
 ip address 100.3.3.3 255.255.255.255
#
//连接Internet的接口
interface GigabitEthernet0/1
 port link-mode route
 //NAT多实例配置
 nat outbound 3000
 ip address 200.1.1.3 255.255.255.0
 //IPSec策略配置
 ipsec policy center
#
//连接MPLS网络接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.2.3.3 255.255.255.0
 mpls
 mpls ldp
#
//连接VPNA的接口
interface GigabitEthernet1/0
 port link-mode route
 ip binding vpn-instance vpna
 ip address 13.2.2.2 255.255.255.0
#
//到总部的GRE隧道接口
interface Tunnel0
 ip address 1.3.0.2 255.255.255.252
 source LoopBack100
 destination 100.1.1.1
 //使能MPLS和LDP
 mpls
 mpls ldp
#
//BGP部分配置
bgp 100
 undo synchronization
 group 100 internal
 peer 100 connect-interface LoopBack0
 peer 1.1.1.1 group 100
 peer 2.2.2.2 group 100
 #
 ipv4-family vpnv4
  peer 100 enable
  peer 1.1.1.1 enable
  peer 1.1.1.1 group 100
  peer 2.2.2.2 enable
  peer 2.2.2.2 group 100
 #
 ipv4-family vpn-instance vpna
  import-route direct
#
//OSPF部分配置，注意只将MPLS相关接口加入区域0
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 1.2.3.0 0.0.0.255
  network 1.3.0.0 0.0.0.3
#
 //访问Internet的默认路由
 ip route-static 0.0.0.0 0.0.0.0 200.1.1.254
 //配置保证vpna可以访问Internet的静态路由，必须要指定Internet出接口
 ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 GigabitEthernet0/1 200.1.1.254
#
```

四、配置关键点:

1) 先配置好MPLS L3VPN部分，可以参照相应内容KMS;

2) 再配置好公网的GRE Over IPSec;

3) 在配置好的GRE上面运行MPLS和LDP;

4) 将GRE隧道也加入到MPLS网络的OSPF进程;

> 5) 最后配置NAT多实例，注意ACL 3000和VPN静态路由的配置，**静态路由务必指定连接Internet出接口。**