MSR 系列路由器公网 Internet 上的 MPLS L3VPN over GRE over IPsec 隧道备份 MPLS L3VPN 网络的配置举例

目 录

1 简介 1
2 配置前提 1
3 配置举例 1
3.1 组网需求 1
3.2 使用版本 2
3.3 配置步骤 2
3.3.1 设备PE配置 2
3.3.2 设备PE 1 配置 5
3.3.3 设备PE 2 配置 8
3.4 验证配置 11
3.5 配置文件 12
4 相关资料 18

1 简介

本文档介绍 Internet 上的 MPLS L3VPN over GRE over IPsec 隧道备份 MPLS L3VPN 网络的的典型案例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 GRE Over IPSec 和 MPLS L3VPN 的特性。

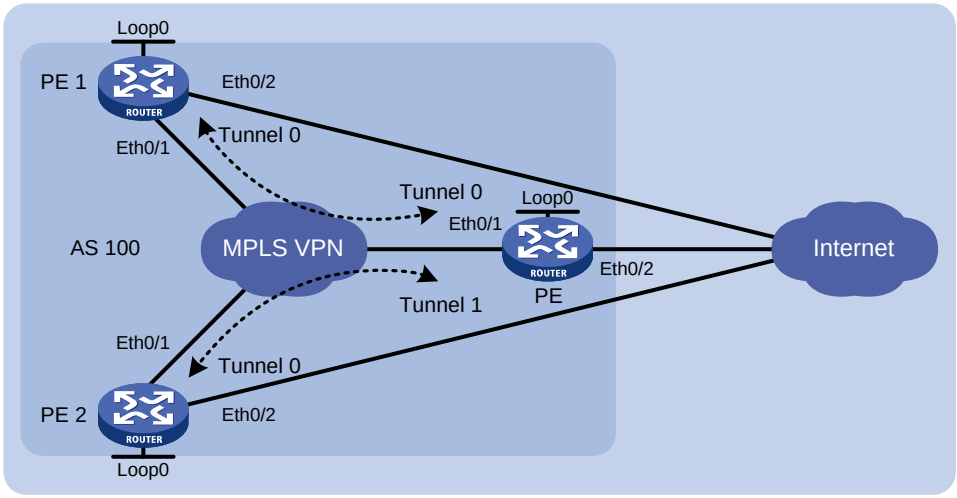
3 配置举例

3.1 组网需求

如 图 1 所示，在MPLS VPN骨干网中，总部PE路由器与分支PE路由器互通，为防止主用MPLS VPN网络断开后PE间无法互联，现要求：

- 在 PE 间建立基于隧道的冗余备份链路，使得 MPLS 网络故障时 PE 间仍能够互访。
- 在 PE 上配置 NAT 多实例，使得 PE 的 VPN 路由都可以访问 Internet。

图1 MSR 系列路由器 MPLS L3VPN Over GRE Over IPSec 备份和 NAT 多实例功能组网图



设备	接口	IP地址	设备	接口	IP地址
PE 1	Loop0	2.2.2.2/32	PE	Loop0	1.1.1.1/32
	Loop100	100.2.2.2/32		Loop100	100.1.1.1/32
	Eth0/1	10.1.1.2/24		Eth0/1	10.1.1.1/24
	Eth0/2	20.1.1.2/24		Eth0/2	20.1.1.1/24
	Tunnel0	1.2.0.2/24		Tunnel0	1.2.0.1/24
PE 2	Loop0	3.3.3.3/32		Tunnel1	1.3.0.1/24
	Loop100	100.3.3.3/32	Internet	-	20.1.1.254/24

	Eth0/1	10.1.1.3/24			
	Eth0/2	20.1.1.3/24			
	Tunnel0	1.3.0.2/24			

3.2 使用版本

本举例是在 Release 2311 版本上进行配置和验证的。

3.3 配置步骤

3.3.1 设备PE配置

配置设备接口地址。

```
<PE> system-view
[PE] interface loopback 0
[PE-LoopBack0] ip address 1.1.1.1 255.255.255.255
[PE-LoopBack0] quit
[PE] interface loopback 100
[PE-LoopBack100] ip address 100.1.1.1 255.255.255.255
[PE-LoopBack100] quit
[PE] interface ethernet 0/1
[PE-Ethernet0/1] port link-mode route
[PE-Ethernet0/1] ip address 10.1.1.1 255.255.255.0
[PE-Ethernet0/1] quit
[PE] interface ethernet 0/2
[PE-Ethernet0/2] port link-mode route
[PE-Ethernet0/2] ip address 20.1.1.1 255.255.255.0
[PE-Ethernet0/2] quit
```

配置 OSPF 协议，使网络互通。

```
[PE] ospf 1
[PE-ospf-1] area 0.0.0.0
[PE-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE-ospf-1-area-0.0.0.0] quit
[PE-ospf-1] quit
```

配置 MPLS LSR-ID，使能 MPLS 和 MPLS LDP 功能。

```
[PE] router id 1.1.1.1
[PE] mpls lsr-id 1.1.1.1
[PE] mpls
[PE-mpls] quit
[PE] mpls ldp
[PE-mpls-ldp] quit
```

在接口 Ethernet0/1 配置 MPLS 和 MPLS LDP 功能。

```
[PE] interface ethernet0/1
[PE-Ethernet0/1] mpls
[PE-Ethernet0/1] mpls ldp
```

```
[PE-Ethernet0/1] quit
```
创建 VPN 实例 vpna，并配置 RD 和 VPN Target 属性。
```
[PE] ip vpn-instance vpna
[PE-vpn-instance-vpna] route-distinguisher 1:1
[PE-vpn-instance-vpna] vpn-target 1:1 export-extcommunity
[PE-vpn-instance-vpna] vpn-target 1:1 import-extcommunity
[PE-vpn-instance-vpna] quit
```
在 PE 间建立 MP-IBGP 对等体。
```
[PE] bgp 100
[PE-bgp] group 100 internal
[PE-bgp] peer 100 connect-interface loopback 0
[PE-bgp] peer 2.2.2.2 group 100
[PE-bgp] peer 3.3.3.3 group 100
```
进入 BGP-VPN 实例视图，将直连路由引入到 vpna 的路由表。
```
[PE-bgp] ipv4-family vpn-instance vpna
[PE-bgp-ipv4-vpna] import-route direct
[PE-bgp-ipv4-vpna] quit
```
进入 BGP-VPNv4 子地址族视图，配置对等体 2.2.2.2 和 3.3.3.3。
```
[PE-bgp] ipv4-family vpnv4
[PE-bgp-af-vpnv4] peer 100 enable
[PE-bgp-af-vpnv4] peer 2.2.2.2 enable
[PE-bgp-af-vpnv4] peer 2.2.2.2 group 100
[PE-bgp-af-vpnv4] peer 3.3.3.3 enable
[PE-bgp-af-vpnv4] peer 3.3.3.3 group 100
[PE-bgp-af-vpnv4] quit
[PE-bgp] quit
```
为 IKE 配置本端安全网关名为 1.1.1.1。
```
[PE] ike local-name 1.1.1.1
```
创建 GRE 隧道 Tunnel 0。
```
[PE] interface tunnel 0
[PE-Tunnel0] ip address 1.2.0.1 255.255.255.0
[PE-Tunnel0] source 100.1.1.1
[PE-Tunnel0] destination 100.2.2.2
```
使能 GRE 隧道的 keepalive 功能。
```
[PE-Tunnel0] keepalive 10 3
```
使能 Tunnel 0 的 MPLS 功能。
```
[PE-Tunnel0] mpls
[PE-Tunnel0] quit
```
创建 GRE 隧道 Tunnel 1。
```
[PE] interface tunnel 1
[PE-Tunnel1] ip address 1.3.0.1 255.255.255.0
[PE-Tunnel1] source 100.1.1.1
[PE-Tunnel1] destination 100.3.3.3
```
使能 GRE 隧道的 keepalive 功能。

```
[PE-Tunnel1] keepalive 10 3
```
使能 Tunnel 1 的 MPLS 功能。
```
[PE-Tunnel1] mpls
[PE-Tunnel1] quit
```
将 Tunnel 0 和 Tunnel 1 加入 OSPF 网络中。
```
[PE] ospf 1
[PE-ospf-1] area 0.0.0.0
[PE-ospf-1-area-0.0.0.0] network 1.2.0.0 0.0.0.255
[PE-ospf-1-area-0.0.0.0] network 1.3.0.0 0.0.0.255
[PE-ospf-1-area-0.0.0.0] quit
[PE-ospf-1] quit
```
配置访问控制列表，定义相应的数据流。
```
[PE] acl number 3000
[PE-acl-adv-3000] rule 0 permit ip vpn-instance vpna
[PE-acl-adv-3000] quit
[PE] acl number 3333
[PE-acl-adv-3333] rule 10 permit gre source 100.1.1.1 0 destination 100.2.2.2 0
[PE-acl-adv-3333] quit
[PE] acl number 3334
[PE-acl-adv-3334] rule 20 permit gre source 100.1.1.1 0 destination 100.3.3.3 0
[PE-acl-adv-3334] quit
```
创建 IPsec 安全提议 tran1，采用隧道模式封装，ESP 安全协议。
```
[PE] ipsec transform-set tran1
[PE-ipsec-transform-set-tran1] encapsulation-mode tunnel
[PE-ipsec-transform-set-tran1] transform esp
```
配置 SHA1 和 DES 算法。
```
[PE-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[PE-ipsec-transform-set-tran1] esp encryption-algorithm des
[PE-ipsec-transform-set-tran1] quit
```
配置 IKE 对等体 2.2.2.2，使用野蛮模式。
```
[PE] ike peer 2.2.2.2
[PE-ike-peer-2.2.2.2] exchange-mode aggressive
[PE-ike-peer-2.2.2.2] pre-shared-key cipher h3c
[PE-ike-peer-2.2.2.2] id-type name
[PE-ike-peer-2.2.2.2] remote-name 2.2.2.2
```
配置 IKE 对等体 NAT 穿越功能。
```
[PE-ike-peer-2.2.2.2] nat traversal
[PE-ike-peer-2.2.2.2] quit
```
配置 IKE 对等体 3.3.3.3，使用野蛮模式。
```
[PE] ike peer 3.3.3.3
[PE-ike-peer-3.3.3.3] exchange-mode aggressive
[PE-ike-peer-3.3.3.3] pre-shared-key cipher h3c
[PE-ike-peer-3.3.3.3] id-type name
[PE-ike-peer-3.3.3.3] remote-name 3.3.3.3
```
配置 IKE 对等体 NAT 穿越功能。

```
[PE-ike-peer-3.3.3.3] nat traversal
[PE-ike-peer-3.3.3.3] quit
```

创建一条 IPSec 安全策略 branch 1，协商方式为 isakmp，引用 ACL 3333，IKE 对等体 2.2.2.2，IPSec 安全提议 tran1。

```
[PE] ipsec policy branch 1 isakmp
[PE-ipsec-policy-isakmp-branch-1] security acl 3333
[PE-ipsec-policy-isakmp-branch-1] ike-peer 2.2.2.2
[PE-ipsec-policy-isakmp-branch-1] transform-set tran1
[PE-ipsec-policy-isakmp-branch-1] quit
```

创建一条 IPSec 安全策略 branch 2，协商方式为 isakmp，引用 ACL 3334，IKE 对等体 3.3.3.3，IPSec 安全提议 tran1。

```
[PE] ipsec policy branch 2 isakmp
[PE-ipsec-policy-isakmp-branch-2] security acl 3334
[PE-ipsec-policy-isakmp-branch-2] ike-peer 3.3.3.3
[PE-ipsec-policy-isakmp-branch-2] transform-set tran1
[PE-ipsec-policy-isakmp-branch-2] quit
```

在接口 Ethernet0/2 上应用 IPSec 安全策略组 branch 和 NAT 多实例。

```
[PE] interface ethernet 0/2
[PE-Ethernet0/2] ip address 20.1.1.1 255.255.255.0
[PE-Ethernet0/2] ipsec policy branch
[PE-Ethernet0/2] nat outbound 3000
[PE-Ethernet0/2] quit
```

为 VPN 实例 vpna 配置到 Internet 的缺省路由。

```
[PE] ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 ethernet0/2 20.1.1.254
```

配置到 Internet 的缺省路由。

```
[PE] ip route-static 0.0.0.0 0.0.0.0 20.1.1.254
```

3.3.2 设备PE 1 配置

配置设备接口地址。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 2.2.2.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface loopback 100
[PE1-LoopBack100] ip address 100.2.2.2 255.255.255.255
[PE1-LoopBack100] quit
[PE1] interface ethernet 0/1
[PE1-Ethernet0/1] port link-mode route
[PE1-Ethernet0/1] ip address 10.1.1.2 255.255.255.0
[PE1-Ethernet0/1] quit
[PE1] interface ethernet 0/2
[PE1-Ethernet0/2] port link-mode route
[PE1-Ethernet0/2] ip address 20.1.1.2 255.255.255.0
[PE1-Ethernet0/2] quit
```

配置 OSPF 协议，使网络互通。

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 MPLS LSR-ID，使能 MPLS 和 MPLS LDP 功能。

```
[PE1] router id 2.2.2.2
[PE1] mpls lsr-id 2.2.2.2
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

在接口 Ethernet0/1 配置 MPLS 和 MPLS LDP 功能。

```
[PE1] interface ethernet 0/1
[PE1-Ethernet0/1] mpls
[PE1-Ethernet0/1] mpls ldp
[PE1-Ethernet0/1] quit
```

创建 VPN 实例 vpna，并配置 RD 和 VPN Target 属性。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 2:1
[PE1-vpn-instance-vpna] vpn-target 1:1 export-extcommunity
[PE1-vpn-instance-vpna] vpn-target 1:1 import-extcommunity
[PE1-vpn-instance-vpna] quit
```

在 PE 间建立 MP-IBGP 对等体。

```
[PE1] bgp 100
[PE1-bgp] group 100 internal
[PE1-bgp] peer 100 connect-interface loopback0
[PE1-bgp] peer 1.1.1.1 group 100
[PE1-bgp] peer 3.3.3.3 group 100
```

进入 BGP-VPN 实例视图，将直连路由引入到 vpna 的路由表。

```
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-ipv4-vpna] import-route direct
[PE1-bgp-ipv4-vpna] quit
```

进入 BGP-VPNv4 子地址族视图，配置对等体 1.1.1.1 和 3.3.3.3。

```
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 100 enable
[PE1-bgp-af-vpnv4] peer 1.1.1.1 enable
[PE1-bgp-af-vpnv4] peer 1.1.1.1 group 100
[PE1-bgp-af-vpnv4] peer 3.3.3.3 enable
[PE1-bgp-af-vpnv4] peer 3.3.3.3 group 100
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

为 IKE 配置本端安全网关名为 2.2.2.2。

```
[PE1] ike local-name 2.2.2.2
```

创建 GRE 隧道 Tunnel 0。

```
[PE1] interface tunnel 0
[PE1-Tunnel0] ip address 1.2.0.2 255.255.255.0
[PE1-Tunnel0] source 100.2.2.2
[PE1-Tunnel0] destination 100.1.1.1
```

使能 GRE 隧道的 keepalive 功能。

```
[PE1-Tunnel0] keepalive 10 3
```

使能 Tunnel 0 的 MPLS 功能。

```
[PE1-Tunnel0] mpls
[PE1-Tunnel0] quit
```

将 Tunnel 0 加入 OSPF 网络中。

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.2.0.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置访问控制列表，定义相应的数据流。

```
[PE1] acl number 3000
[PE1-acl-adv-3000] rule 0 permit ip vpn-instance vpna
[PE1-acl-adv-3000] quit
[PE1] acl number 3333
[PE1-acl-adv-3333] rule 10 permit gre source 100.2.2.2 0 destination 100.1.1.1 0
[PE1-acl-adv-3333] quit
```

创建 IPSec 安全提议 tran1，采用隧道模式封装，ESP 安全协议。

```
[PE1] ipsec transform-set tran1
[PE1-ipsec-transform-set-tran1] encapsulation-mode tunnel
[PE1-ipsec-transform-set-tran1] transform esp
```

配置 SHA1 和 DES 算法。

```
[PE1-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[PE1-ipsec-transform-set-tran1] esp encryption-algorithm des
[PE1-ipsec-transform-set-tran1] quit
```

配置 IKE 对等体 1.1.1.1，使用野蛮模式。

```
[PE1] ike peer 1.1.1.1
[PE1-ike-peer-1.1.1.1] exchange-mode aggressive
[PE1-ike-peer-1.1.1.1] pre-shared-key cipher h3c
[PE1-ike-peer-1.1.1.1] id-type name
[PE1-ike-peer-1.1.1.1] remote-name 1.1.1.1
```

配置 IKE 对等体 NAT 穿越功能。

```
[PE1-ike-peer-1.1.1.1] nat traversal
[PE1-ike-peer-1.1.1.1] quit
```

创建 IPSec 安全策略 center，协商方式为 isakmp，引用 ACL 3333，IKE 对等体 1.1.1.1，IPSec 安全提议 tran1。

```
[PE1] ipsec policy center 1 isakmp
[PE1-ipsec-policy-isakmp-center-1] security acl 3333
```

```
[PE1-ipsec-policy-isakmp-center-1] ike-peer 1.1.1.1
[PE1-ipsec-policy-isakmp-center-1] transform-set tran1
[PE1-ipsec-policy-isakmp-branch-1] quit
```

在接口 Ethernet0/2 上应用 IPSec 安全策略组 center 和 NAT 多实例。

```
[PE1] interface ethernet 0/2
[PE1-Ethernet0/2] ipsec policy center
[PE1-Ethernet0/2] nat outbound 3000
[PE1-Ethernet0/2] quit
```

为 VPN 实例 vpna 配置到 Internet 的缺省路由。

```
[PE1] ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 ethernet0/2 20.1.1.254
```

配置到 Internet 的缺省路由。

```
[PE1] ip route-static 0.0.0.0 0.0.0.0 20.1.1.254
```

3.3.3 设备PE 2 配置

配置设备接口地址。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.3 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface loopback 100
[PE2-LoopBack100] ip address 100.3.3.3 255.255.255.255
[PE2-LoopBack100] quit
[PE2] interface ethernet 0/1
[PE2-Ethernet0/1] port link-mode route
[PE2-Ethernet0/1] ip address 10.1.1.3 255.255.255.0
[PE2-Ethernet0/1] quit
[PE2] interface ethernet 0/2
[PE2-Ethernet0/2] port link-mode route
[PE2-Ethernet0/2] ip address 20.1.1.3 255.255.255.0
[PE2-Ethernet0/2] quit
```

配置 OSPF 协议，使网络互通。

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 MPLS LSR-ID，使能 MPLS 和 MPLS LDP 功能。

```
[PE2] router id 3.3.3.3
[PE2] mpls lsr-id 3.3.3.3
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

在接口 Ethernet0/1 配置 MPLS 和 MPLS LDP 功能。

```
[PE2] interface ethernet 0/1
[PE2-Ethernet0/1] mpls
[PE2-Ethernet0/1] mpls ldp
[PE2-Ethernet0/1] quit
```
创建 VPN 实例 vpna，并配置 RD 和 VPN Target 属性。
```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 3:1
[PE2-vpn-instance-vpna] vpn-target 1:1 export-extcommunity
[PE2-vpn-instance-vpna] vpn-target 1:1 import-extcommunity
[PE2-vpn-instance-vpna] quit
```
在 PE 间建立 MP-IBGP 对等体。
```
[PE2] bgp 100
[PE2-bgp] group 100 internal
[PE2-bgp] peer 100 connect-interface loopback0
[PE2-bgp] peer 1.1.1.1 group 100
[PE2-bgp] peer 2.2.2.2 group 100
```
进入 BGP-VPN 实例视图，将直连路由引入到 vpna 的路由表。
```
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-ipv4-vpna] import-route direct
[PE2-bgp-ipv4-vpna] quit
```
进入 BGP-VPNv4 子地址族视图，配置对等体 1.1.1.1 和 2.2.2.2。
```
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 100 enable
[PE2-bgp-af-vpnv4] peer 1.1.1.1 enable
[PE2-bgp-af-vpnv4] peer 1.1.1.1 group 100
[PE2-bgp-af-vpnv4] peer 2.2.2.2 enable
[PE2-bgp-af-vpnv4] peer 2.2.2.2 group 100
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```
为 IKE 配置本端安全网关名为 3.3.3.3。
```
[PE2] ike local-name 3.3.3.3
```
创建 GRE 隧道 Tunnel 0。
```
[PE2] interface tunnel 0
[PE2-Tunnel0] ip address 1.3.0.2 255.255.255.0
[PE2-Tunnel0] source 100.3.3.3
[PE2-Tunnel0] destination 100.1.1.1
[PE2-Tunnel0] quit
```
使能 GRE 隧道的 keepalive 功能。
```
[PE2-Tunnel0] keepalive 10 3
```
使能 Tunnel 0 的 MPLS 功能。
```
[PE2-Tunnel0] mpls
[PE2-Tunnel0] quit
```
将 Tunnel 0 加入 OSPF 网络中。
```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
```

```
[PE2-ospf-1-area-0.0.0.0] network 1.3.0.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```
配置访问控制列表，定义相应的数据流。
```
[PE2] acl number 3000
[PE2-acl-adv-3000] rule 0 permit ip vpn-instance vpna
[PE2-acl-adv-3000] quit
[PE2] acl number 3333
[PE2-acl-adv-3333] rule 10 permit gre source 100.3.3.3 0 destination 100.1.1.1 0
[PE2-acl-adv-3333] quit
```
创建 IPSec 安全提议 tran1，采用隧道模式封装，ESP 安全协议。
```
[PE2] ipsec transform-set tran1
[PE2-ipsec-transform-set-tran1] encapsulation-mode tunnel
[PE2-ipsec-transform-set-tran1] transform esp
```
配置 SHA1 和 DES 算法。
```
[PE2-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[PE2-ipsec-transform-set-tran1] esp encryption-algorithm des
[PE2-ipsec-transform-set-tran1] quit
```
配置 IKE 对等体 1.1.1.1，使用野蛮模式。
```
[PE2] ike peer 1.1.1.1
[PE2-ike-peer-1.1.1.1] exchange-mode aggressive
[PE2-ike-peer-1.1.1.1] pre-shared-key cipher h3c
[PE2-ike-peer-1.1.1.1] id-type name
[PE2-ike-peer-1.1.1.1] remote-name 1.1.1.1
```
配置 IKE 对等体 NAT 穿越功能。
```
[PE2-ike-peer-1.1.1.1] nat traversal
[PE2-ike-peer-1.1.1.1] quit
```
创建 IPSec 安全策略 center，协商方式为 isakmp，引用 ACL 3333，IKE 对等体 1.1.1.1，IPSec 安全提议 tran1。
```
[PE2] ipsec policy center 1 isakmp
[PE2-ipsec-policy-isakmp-center-1] security acl 3333
[PE2-ipsec-policy-isakmp-center-1] ike-peer 1.1.1.1
[PE2-ipsec-policy-isakmp-center-1] transform-set tran1
[PE2-ipsec-policy-isakmp-center-1] quit
```
在接口 Ethernet0/1 上应用 IPSec 安全策略组 center 和 NAT 多实例。
```
[PE2] interface ethernet 0/2
[PE2-Ethernet0/2] nat outbound 3000
[PE2-Ethernet0/2] ipsec policy center
[PE2-Ethernet0/2] quit
```
为 VPN 实例 vpna 配置到 Internet 的缺省路由。
```
[PE2] ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 ethernet0/2 20.1.1.254
```
配置到 Internet 的缺省路由。
```
[PE2] ip route-static 0.0.0.0 0.0.0.0 20.1.1.254
```

3.4 验证配置

在总部 PE 路由器上通过 VPN 路由 ping Internet 的地址，看能否 ping 通。

```
<PE> ping -vpn-instance vpna 20.1.1.254
  PING 20.1.1.254: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.254: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 20.1.1.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

在总部 PE 路由器上 ping Internet 的地址，看能否 ping 通。

```
<PE> ping 20.1.1.254
  PING 20.1.1.254: 56  data bytes, press CTRL_C to break
    Reply from 20.1.1.254: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 20.1.1.254: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 20.1.1.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

在总部路由器上查看 MPLS LDP 会话。

```
<PE> display mpls ldp session

               LDP Session(s) in Public Network
 Total number of sessions: 2
 ------------------------------------------------------------------------------
 Peer-ID               Status         SsnRole  FT   MD5  KA-Sent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0             Operational    Passive  Off  Off  1665/1665
 3.3.3.3:0             Non Existent   Passive  Off  Off  0/0
 ------------------------------------------------------------------------------
 FT  : Fault Tolerance
```

在总部 PE 路由器上查看 IKE 邻居。

```
<PE> display ike peer

---------------------------
 IKE Peer: 2.2.2.2
```

```
   exchange mode: aggressive on phase 1
   pre-shared-key ******
   peer id type: name
   peer ip address: 20.1.1.2
   local ip address:
   peer name: 2.2.2.2
   nat traversal: enable
   dpd:
---------------------------


---------------------------
 IKE Peer: 3.3.3.3
   exchange mode: aggressive on phase 1
   pre-shared-key ******
   peer id type: name
   peer ip address: 20.1.1.3
   local ip address:
   peer name: 3.3.3.3
   nat traversal: enable
   dpd:
---------------------------
```

3.5 配置文件

- PE 配置：

```
#
 ike local-name 1.1.1.1
#
 router id 1.1.1.1
#
 mpls lsr-id 1.1.1.1
#
ip vpn-instance vpna
 route-distinguisher 1:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
acl number 3000
 rule 0 permit ip vpn-instance vpna
acl number 3333
 rule 10 permit gre source 100.1.1.1 0 destination 100.2.2.2 0
acl number 3334
 rule 20 permit gre source 100.1.1.1 0 destination 100.3.3.3 0
#
mpls
#
mpls ldp
```

```
#
ike peer 2.2.2.2
 exchange-mode aggressive
 pre-shared-key cipher $c$3$Ata32mmg/Sqogxj2B8z1IPQRRS0cDA==
 id-type name
 remote-name 2.2.2.2
 nat traversal
#
ike peer 3.3.3.3
 exchange-mode aggressive
 pre-shared-key cipher $c$3$jTaX3ShJo728rwzbWeHZl7raKsA2Mw==
 id-type name
 remote-name 3.3.3.3
 nat traversal
#
ipsec transform-set tran1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm des
#
ipsec policy branch 1 isakmp
 security acl 3333
 ike-peer 2.2.2.2
 transform-set tran1
#
ipsec policy branch 2 isakmp
 security acl 3333
 ike-peer 3.3.3.3
 transform-set tran1
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack100
 ip address 100.1.1.1 255.255.255.255
#
interface Ethernet0/1
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet0/2
 ip address 20.1.1.1 255.255.255.0
 nat outbound 3000
 ipsec policy branch
#
interface Tunnel0
```

```
 ip address 1.2.0.1 255.255.255.0
 source 100.1.1.1
 destination 100.2.2.2
 keepalive 10 3
 mpls
#
interface Tunnel1
 ip address 1.3.0.1 255.255.255.0
 source 100.1.1.1
 destination 100.3.3.3
 keepalive 10 3
 mpls
#
bgp 100
 undo synchronization
 group 100 internal
 peer 100 connect-interface LoopBack0
 peer 2.2.2.2 group 100
 peer 3.3.3.3 group 100
#
 ipv4-family vpn-instance vpna
  import-route direct
#
 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
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 1.2.0.0 0.0.0.255
  network 1.3.0.0 0.0.0.255
  network 10.1.1.0 0.0.0.255

#
 ip route-static 0.0.0.0 0.0.0.0 20.1.1.254
 ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 Ethernet0/2 20.1.1.254
```

- PE1 配置：

```
#
 ike local-name 2.2.2.2
#
 router id 2.2.2.2
#
 mpls lsr-id 2.2.2.2
#
```

```
ip vpn-instance vpna
 route-distinguisher 2:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
acl number 3000
 rule 0 permit ip vpn-instance vpna
acl number 3333
 rule 10 permit gre source 100.2.2.2 0 destination 100.1.1.1 0
#
mpls
#
mpls ldp
#
ike peer 1.1.1.1
 exchange-mode aggressive
 pre-shared-key cipher $c$3$DeuU8f4NqT7u6cJ8E/+7jrXIyKGw/g==
 id-type name
 remote-name 1.1.1.1
 nat traversal
#
ipsec transform-set tran1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm des
#
ipsec policy center 1 isakmp
 security acl 3333
 ike-peer 1.1.1.1
 transform-set tran1
#
interface Ethernet0/1
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet0/2
 port link-mode route
 nat outbound 3000
 ip address 20.1.1.2 255.255.255.0
 ipsec policy center
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface LoopBack100
```

```
 ip address 100.2.2.2 255.255.255.255
#
interface Tunnel0
 ip address 1.2.0.2 255.255.255.0
 source 100.2.2.2
 destination 100.1.1.1
 keepalive 10 3
 mpls
#
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 vpn-instance vpna
  import-route direct
 #
 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
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
  network 1.2.0.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 20.1.1.254
 ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 Ethernet0/2 20.1.1.254
```

- PE2 配置：

```
#
 ike local-name 3.3.3.3
#
 router id 3.3.3.3
#
 mpls lsr-id 3.3.3.3
#
ip vpn-instance vpna
 route-distinguisher 3:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
acl number 3000
```

```
 rule 0 permit ip vpn-instance vpna
acl number 3333
 rule 10 permit gre source 100.3.3.3 0 destination 100.1.1.1 0
#
mpls
#
mpls ldp
#
ike peer 1.1.1.1
 exchange-mode aggressive
 pre-shared-key cipher $c$3$+InhNF72zvL32yKkCOdR5QkPhhZc9A==
 id-type name
 remote-name 1.1.1.1
 nat traversal
#
ipsec transform-set tran1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm des
#
ipsec policy center 1 isakmp
 security acl 3333
 ike-peer 1.1.1.1
 transform-set tran1
#
interface Ethernet0/1
 port link-mode route
 ip address 10.1.1.3 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet0/2
 port link-mode route
 nat outbound 3000
 duplex full
 ip address 20.1.1.3 255.255.255.0
 ipsec policy center
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface LoopBack100
 ip address 100.3.3.3 255.255.255.255
#
interface Tunnel0
 ip address 1.3.0.2 255.255.255.0
 source 100.3.3.3
```

```
 destination 100.1.1.1
 keepalive 10 3
 mpls
#
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 vpn-instance vpna
  import-route direct
 #
 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
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 1.3.0.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 20.1.1.254
 ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 Ethernet0/2 20.1.1.254
```

4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311