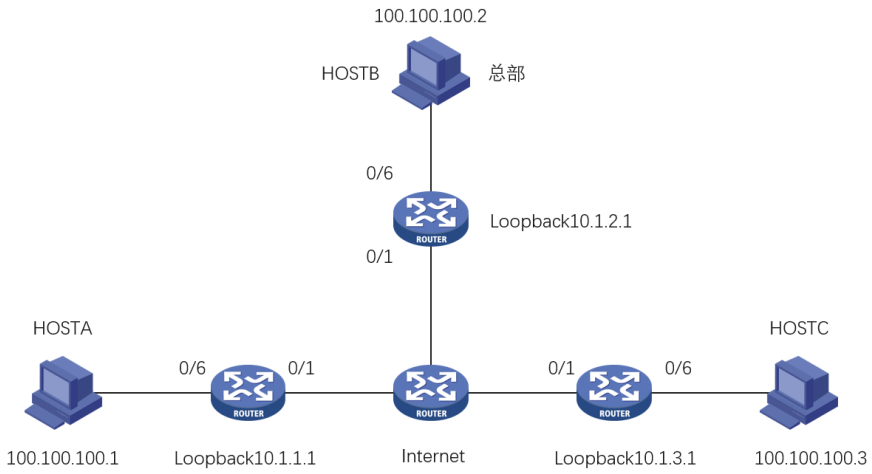
MSR810系列路由器建立IPSec VPN 总部分支网段重叠典型配置

IPSec VPN VxLAN 窦祖尧 2019-12-06 发表

组网及说明



现场HOSTB为总部，HOSTA和HOSTC为分支需要通过IPSEC VPN和总部互访（分支之间也需要互相访问），总部使用固定地址，分支4G拨号动态获地址和总部使用野蛮模式建立IPSEC隧道。由于两个分支和总部内网网段冲突，不可以直接通过ipsec隧道去访问总部，可以通过建立静态vxlan隧道实现大二层互通。

配置步骤

HOSTA

```
# 配置接口Loopback0的IP地址，作为隧道的源端地址
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
# 接口下调用ipsec策略
interface GigabitEthernet1/0/1
ip address 1.1.1.1 255.255.0.0
 ipsec apply policy policy1
# 配置去往公网的默认路由
ip route-static 0.0.0.0 0 1.1.1.2
# IPSEC感兴趣流
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
rule 1 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
ipsec transform-set transform1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy policy1 1 isakmp
 transform-set transform1
 security acl 3000
 remote-address 2.2.2.2
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 exchange-mode aggressive
 local-identity fqdn devicea
 match remote identity address 2.2.2.2 255.255.0.0
#
ike keychain keychain1
 pre-shared-key address 2.2.2.2 255.255.0.0 key H3c
#
```

HOSTB

```
# 配置接口Loopback0的IP地址，作为隧道的源端地址
interface LoopBack0
 ip address 10.1.2.1 255.255.255.0
# 接口下调用ipsec策略
interface GigabitEthernet1/0/1
ip address 2.2.2.2 255.255.0.0
 ipsec apply policy policy1
# 配置去往公网的静态路由
ip route-static 0.0.0.0 0 2.2.2.1
#
ipsec transform-set transform1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy-template template1 1
 transform-set transform1
 local-address 2.2.2.2
 ike-profile profile1
#
ipsec policy-template template1 2
 transform-set transform1
 local-address 2.2.2.2
 ike-profile profile2
#
ipsec policy policy1 1 isakmp template template1
#
ipsec policy policy1 2 isakmp template template2
#
ike profile profile1
 keychain keychain1
 exchange-mode aggressive
 match remote identity fqdn devicea
#
ike profile profile2
 keychain keychain2
 exchange-mode aggressive
 match remote identity fqdn devicec
#
ike keychain keychain1
 pre-shared-key address 1.1.1.1 255.255.0.0 key H3C
#
ike keychain keychain2
 pre-shared-key address 3.3.3.2 255.255.0.0 key H3C
#
```

HOSTC

```
# 配置接口Loopback0的IP地址，作为隧道的源端地址
interface LoopBack0
 ip address 10.1.3.1 255.255.255.0
# 接口下调用ipsec策略
interface GigabitEthernet1/0/1
 ip address 3.3.3.2 255.255.0.0
 ipsec apply policy policy1
# 配置去往公网的静态路由
 ip route-static 0.0.0.0 0 3.3.3.1
# 配置IPSEC感兴趣流
acl advanced 3000
 rule 0 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
rule 0 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec transform-set transform1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy policy1 1 isakmp
```

```
 transform-set transform1
 security acl 3000
 remote-address 2.2.2.2
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 exchange-mode aggressive
 local-identity fqdn devicec
 match remote identity address 2.2.2.2 255.255.0.0
#
ike keychain keychain1
 pre-shared-key address 2.2.2.2 255.255.0.0 key H3C
```

2.总部和分支1建立vxlan隧道tunnel100，总部和分支2建立vxlan隧道200，分支1通过分支2和总部建立vxlan隧道tunnel300

HOSTA

```
# 开启L2VPN能力
 l2vpn enable
# 创建vsi实例test和vxlan 1 并使Tunnel100和Tunnel300关联vxlan1
vsi test
 vxlan 1
  tunnel 100
  tunnel 300
# 接口关联VSI实例vpn1
interface GigabitEthernet1/0/6
xconnect vsi test
# 在HOSTA和HOSTB之间建立VXLAN隧道
interface Tunnel100 mode vxlan
 source 10.1.1.1
 destination 10.1.2.1
# 在HOSTA和HOSTC之间建立VXLAN隧道
interface Tunnel300 mode vxlan
 source 10.1.1.1
 destination 10.1.3.1
#
```

HOSTB

```
# 开启L2VPN能力
 l2vpn enable
# 创建vsi实例test和vxlan 1 并使Tunnel100和Tunnel200关联vxlan1
vsi test
 vxlan 1
  tunnel 100
  tunnel 200
# 接口关联VSI实例vpn1
interface GigabitEthernet1/0/6
xconnect vsi test
# 在HOSTA和HOSTB之间建立VXLAN隧道
interface Tunnel100 mode vxlan
 source 10.1.2.1
 destination 10.1.1.1
# 在HOSTC和HOSTB之间建立VXLAN隧道
interface Tunnel200 mode vxlan
 source 10.1.2.1
 destination 10.1.3.1
#
```

HOSTC

```
# 开启L2VPN能力
 l2vpn enable
# 创建vsi实例test和vxlan 1 并使Tunnel200和Tunnel300关联vxlan1
vsi test
 vxlan 1
  tunnel 200
 tunnel 300
```

```
# 接口关联VSI实例vpn1
interface GigabitEthernet1/0/6
xconnect vsi test
# 在HOSTC和HOSTB之间建立VXLAN隧道
interface Tunnel200 mode vxlan
 source 10.1.3.1
 destination 10.1.2.1
# 在HOSTA和HOSTC之间建立VXLAN隧道
interface Tunnel300 mode vxlan
 source 10.1.3.1
 destination 10.1.1.1
```

配置关键点

当现场出现总部和分支内网网段相同的时候，我们内网访问的流量无法使用ipsec隧道进行互访，所以我们需要创建一个vxlan over ipsec的网络，使用ipsec使设备的loopback接口互通，然后使用loopback接口建立vxlan隧道，这样就能实现总部和分支之间同网段互相访问。如果两个分支之间互相访问，那么我们就需要在两个分支之创建一个vxlan隧道，实际流量还是要经过我们的总部设备的转发。

附件下载：MSR810系列路由器建立IPSec VPN 总部分支网段重叠典型配置.pdf