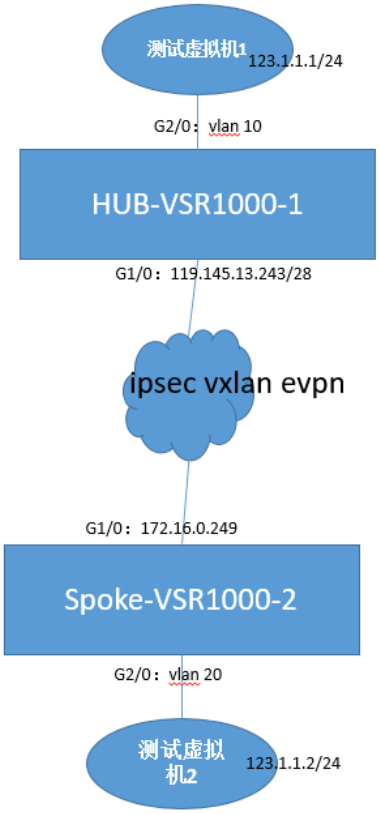
EVPN vxlan over ipsec实现hub+spoke架构二层互通

IPSec VPN VxLAN EVPN 陈仲阳 2022-06-09 发表

组网及说明

1，客户需求

测试虚拟机1和测试虚拟机2属于不同vlan的同一网段，现在需要通过二层互通。hub设备有配置公网地址。spoke属于内网设备，可以访问公网。



2，需求实现说明

（1）hub与spoke之间是需要通过ipsec隧道建立连接

（2）虚拟机二层互通需要配置evpn隧道自动建立

3，vsr1000版本

Version 7.1.064, Release 1340P1201

配置步骤

1，HUB-VSR1000-1配置

```
l2vpn enable
vxlan tunnel mac-learning disable
vsi vpna
  vxlan 10
evpn encapsulation vxlan
  route-distinguisher auto
  vpn-target auto export-extcommunity
  vpn-target auto import-extcommunity
interface LoopBack0
  ip address 100.0.0.1 255.255.255.255
interface GigabitEthernet1/0
   ip address 119.145.13.243 255.255.255.240
   ipsec apply policy p1
interface GigabitEthernet2/0.10
   vlan-type dot1q vid 10
    xconnect vsi vpna
bgp 100
  peer 100.0.0.2 as-number 100
  peer 100.0.0.2 connect-interface LoopBack0
  address-family l2vpn evpn
    peer 100.0.0.2 enable
    peer 100.0.0.2 reflect-client
ipsec transform-set ts1
    esp encryption-algorithm aes-cbc-128
    esp authentication-algorithm sha1
ipsec policy-template policy-t1 65535
   transform-set ts1
   ike-profile ike-p1
   ipsec policy p1 65535 isakmp template policy-t1
ike profile ike-p1
    keychain ike-k1
   dpd interval 10 periodic
   match remote identity address 0.0.0.0 0.0.0.0
   priority 65535
ike keychain ike-k1
   pre-shared-key address 0.0.0.0 0.0.0.0 key simple  xxxx  priority 65535
```

2，Spoke-VSR1000-2配置

```
vxlan tunnel mac-learning disable
l2vpn enable
vsi vpna
   vxlan 10
   evpn encapsulation vxlan
     route-distinguisher auto
     vpn-target auto export-extcommunity
     vpn-target auto import-extcommunity
interface LoopBack0
   ip address 100.0.0.2 255.255.255.255
 interface GigabitEthernet1/0
   ip address 172.16.0.249 255.255.255.0
   ipsec apply policy p1
 interface GigabitEthernet2/0.20
   vlan-type dot1q vid 20
   xconnect vsi vpna
bgp 100
  peer 100.0.0.1 as-number 100
  peer 100.0.0.1 connect-interface LoopBack0
```

```
  address-family l2vpn evpn
   peer 100.0.0.1 enable
acl advanced 3001
   rule 0 permit ip source 100.0.0.2 0 destination 100.0.0.1 0
ipsec transform-set ts1
```