S5800交换机使用PBR实现不同VPN实例通信配置

MPLS L3VPN　丁犁　2013-10-30 发表

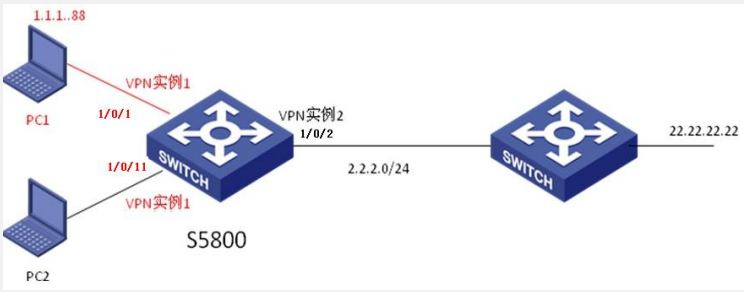
S5800交换机使用PBR实现不同VPN实例通信配置案例

一、 组网需求：

S5800交换机作为MCE设备，1/0/1接口属于VPN实例1，1/0/2接口属于VPN实例2.VPN实例1无法访问外网，VPN实例2可以访问外网，且两实例之间数据不能互访。

目前VPN实例1中有PC需要临时访问外网，同时该PC仍然不能访问VPN实例2中的网络，管理员可以在不改动VPN实例配置的情况下，使用PBR策略路由在S5800交换机上实现需求。

二、 组网图：



三、 配置步骤：

1. 确认交换机版本

S5800交换机需使用F1803L02版本

2. 在S5800交换机上部署VPN实例，使得PC1与PC2无法通信

```
#
ip vpn-instance 1
 route-distinguisher 1:1
 vpn-target 12:1 export-extcommunity
 vpn-target 12:1 import-extcommunity
#
ip vpn-instance 2
 route-distinguisher 2:2
 vpn-target 13:1 export-extcommunity
 vpn-target 13:1 import-extcommunity
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip binding vpn-instance 1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip binding vpn-instance 2
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/11
 port link-mode route
 ip binding vpn-instance 1
```

ip address 11.1.1.1 255.255.255.0

#

使用静态路由保障VPN实例2能够与远端22.22.22.0/24网段通信

#

ip route-static vpn-instance 2 22.22.22.0 255.255.255.0 2.2.2.2

#

[S5800]dis ip routing-table vpn-instance 1

Routing Tables: 1

Destinations : 4 Routes : 4

Destination/Mask Proto Pre Cost NextHop Interface

1.1.1.0/24 Direct 0 0 1.1.1.1 GE1/0/1

1.1.1.1/32 Direct 0 0 127.0.0.1 InLoop0

127.0.0.0/8 Direct 0 0 127.0.0.1 InLoop0

127.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0

[S5800]dis ip routing-table vpn-instance 2

Routing Tables: 2

Destinations : 5 Routes : 5

Destination/Mask Proto Pre Cost NextHop Interface

2.2.2.0/24 Direct 0 0 2.2.2.1 GE1/0/2

2.2.2.1/32 Direct 0 0 127.0.0.1 InLoop0

22.22.22.0/24 Static 60 0 2.2.2.2 GE1/0/2

127.0.0.0/8 Direct 0 0 127.0.0.1 InLoop0

127.0.0.1/32 Direct 0 0 127.0.0.1 InLoop0

3. 配置PBR，并将其运用在对应接口

acl number 2000

rule 0 permit source 1.1.1.88 0

#

acl number 3000

rule 0 permit ip destination 1.1.1.88 0

#

policy-based-route test permit node 10

if-match acl 2000

apply ip-address default next-hop vpn-instance 2 2.2.2.2

#

policy-based-route test1 permit node 10

if-match acl 3000

apply ip-address default next-hop vpn-instance 1 1.1.1.88

#

interface GigabitEthernet1/0/1

port link-mode route

ip binding vpn-instance 1

ip address 1.1.1.1 255.255.255.0

```
 ip policy-based-route test
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip binding vpn-instance 2
 ip address 2.2.2.1 255.255.255.0
 ip policy-based-route test1
#
```

4. 测试结果

PC1 能够访问22.22.22.0/24网络，VPN实例1中其他PC无法访问22.22.22.0/24网络；

PC1 能够与VPN实例1中PC互访；PC1不能够访问VPN实例2中资源。

四、 配置关键点：

1. S5800交换机需使用指定版本，否则在VPN实例接口下配置PBR后，策略路由无法生效。
2. 在设备VPN实例中，策略路由与实例路由的优先级从高到底为：

   apply ip-address next-hop vpn-instance x x.x.x.x(优先级最高)

   ip route-static vpn-instance xx x.x.x.x x.x.x.x x.x.x.x(第二优先级)

   apply ip-address default next-hop vpn-instance x x.x.x.x(优先级最低)
3. 使用apply ip-address default next-hop vpn-instance方式时，需要在设备上行行接口分别使能不同的PBR，保障流量来回交互。