SR6600路由器中心单IKE Peer、单IPSec策略及序号、多分支功能的配置

管祥杰 2008-12-11 发表

SR6600路由器中心单IKE Peer、单IPSec策略及序号、多分支功能的配置

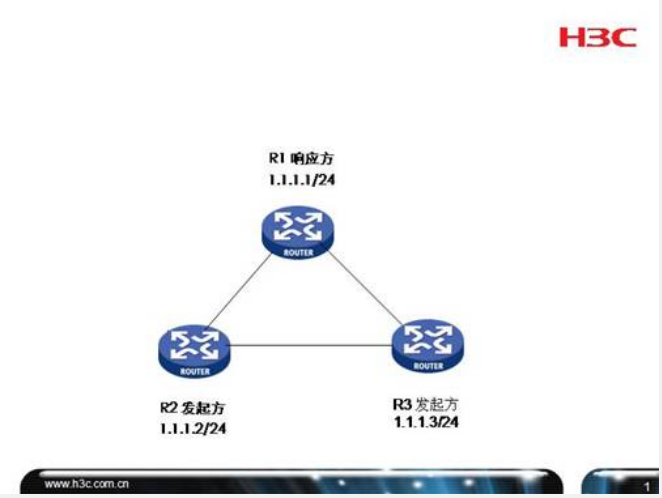
关键字：SR66; IPSec; IKE; 单策略序号; 多分支

一、组网需求：

3台SR66连接在同一个二层链路上，RT1作为IPSec响应方模拟总部；RT2和RT3作为IPSec发起方模拟分支；要求RT1只配置一个IKE Peer、一个IPSec策略序号。

设备清单：SR6600路由器3台

二、组网图：



三、配置步骤：

RT1配置

```
#
//配置总部IKE Peer，注意不需要配置remote-address和remote-name
ike peer branch
 pre-shared-key h3c
 local-address 1.1.1.1
#
ipsec proposal def
#
//IPSec策略模板配置
ipsec policy-template branch 1
 ike-peer branch
 proposal def
#
//IPSec策略配置
ipsec policy hk 1 isakmp template branch
#
interface GigabitEthernet0/0
 port link-mode route
 //互联接口主地址，用于建立IKE连接和隧道封装外层IP地址
 ip address 1.1.1.1 255.255.255.0
 //接口下绑定IPSec策略
 ipsec policy hk
#
interface GigabitEthernet0/1
 port link-mode route
 //连接业务网段接口1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0
 port link-mode route
 //连接业务网段接口2
 ip address 20.1.1.1 255.255.255.0
#
 //默认路由，使流量进入G0/0
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
```

RT2配置

```
#
//分支IKE Peer配置，必须要配置remoted-address
ike peer center
 pre-shared-key h3c
 remote-address 1.1.1.1
 local-address 1.1.1.2
#
ipsec proposal def
#
//IPSec策略配置，根据ACL3000定义的两条流建立两对IPSec SA（即IPSec隧道）
ipsec policy hk 1 isakmp
 security acl 3000
 ike-peer center
 proposal def
#
//ACL 3000配置，定义了两条数据流
acl number 3000
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 5 permit ip source 20.2.2.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 //主地址，用于建立IKE和IPSec隧道外层封装IP地址
 ip address 1.1.1.2 255.255.255.0
 //接口绑定IPSec策略
 ipsec policy hk
#
interface GigabitEthernet0/1
 port link-mode route
 //连接业务网段接口1
 ip address 10.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0
 port link-mode route
 //连接业务网段接口2
 ip address 20.2.2.1 255.255.255.0
#
 //默认路由，使流量进入G0/0
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
```

RT3配置

```
#
//分支IKE Peer配置，必须要配置remoted-address
ike peer center
 pre-shared-key h3c
 remote-address 1.1.1.1
 local-address 1.1.1.3
#
ipsec proposal def
#
//IPSec策略配置，根据ACL3000定义的两条流建立两对IPSec SA（即IPSec隧道）
ipsec policy hk 1 isakmp
 security acl 3000
 ike-peer center
 proposal def
#
//ACL 3000配置，定义了两条数据流
acl number 3000
 rule 0 permit ip source 10.3.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 5 permit ip source 20.3.3.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 //主地址，用于建立IKE和IPSec隧道外层封装IP地址
 ip address 1.1.1.3 255.255.255.0
 //接口绑定IPSec策略
 ipsec policy hk
#
interface GigabitEthernet0/1
 port link-mode route
 //连接业务网段接口1
 ip address 10.3.3.1 255.255.255.0
#
interface GigabitEthernet1/0
 port link-mode route
 //连接业务网段接口2
 ip address 20.3.3.1 255.255.255.0
#
 //默认路由，使流量进入G0/0
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
```

四、配置关键点:

1) 总部采用模板方式建立IPSec，在IKE Peer的配置中不要指定Remote-address和Remote-Name；

2) 总部和各个分支之间都采用相同的Preshare-key。