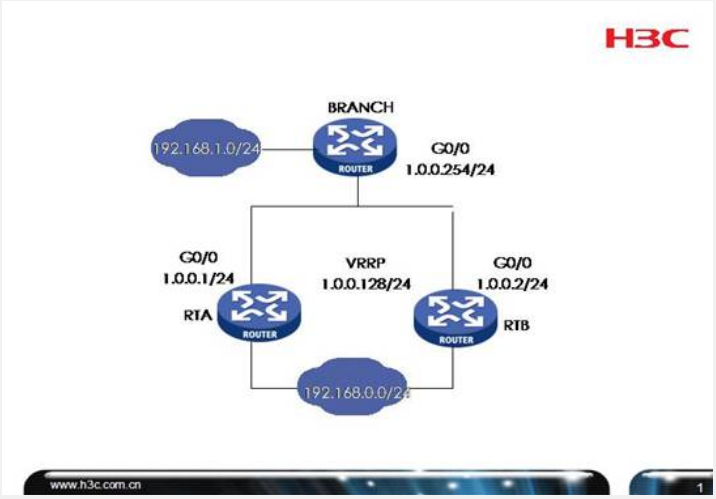
SR6600路由器与VRRP虚地址建立IPSec功能的配置

管祥杰 2008-12-11 发表

SR6600路由器
与VRRP虚地址建立IPSec功能的配置

关键字：SR66;IPSec;IKE;DPD;VRRP

一、组网需求：
RTA、RTB、Branch都连接在一台交换机上，RTA和RTB组VRRP，虚地址是1.0.0.128，RTA作为VRRP Master，RTB作为Backup，Branch和VRRP虚地址之间建立基于IKE的IPSec。实际应用中，建议RTA和RTB连接内网接口也启用VRRP，对内提供统一网关。
设备清单：SR6600路由器3台
二、组网图：



三、配置步骤：
设备和版本：SR6600

RTA配置

```
#
//配置DPD组vrrp，采用默认配置10秒空闲计时，5秒应答等候超时
ike dpd vrrp
#
//IKE Peer配置
ike peer Branch
 pre-shared-key h3c
 remote-address 1.0.0.254
 local-address 1.0.0.128
 //指定dpd组
 dpd vrrp
#
//IPSec提议配置
ipsec proposal def
#
//IPSec策略配置
ipsec policy branch 1 isakmp
 security acl 3000
 ike-peer branch
 proposal def
#
//ACL配置
acl number 3000
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
//对接接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.0.0.1 255.255.255.0
 //配置VRRP组1的虚地址1.0.0.128，使用默认优先级
 vrrp vrid 1 virtual-ip 1.0.0.128
 //绑定IPSec策略
 ipsec policy branch
#
//内网接口
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
 //静态路由配置，使其进入IPSec接口
 ip route-static 192.168.1.0 255.255.255.0 1.0.0.254
#
```

RTB配置

```
#
//配置DPD组vrrp，采用默认配置10秒空闲计时，5秒应答等候超时
ike dpd vrrp
#
//IKE Peer配置
ike peer Branch
 pre-shared-key h3c
 remote-address 1.0.0.254
 local-address 1.0.0.128
 //指定dpd组
 dpd vrrp
#
//IPSec提议配置
ipsec proposal def
#
//IPSec策略配置
ipsec policy branch 1 isakmp
 security acl 3000
 ike-peer branch
 proposal def
#
//ACL配置
//ACL配置
acl number 3000
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
//对接接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.0.0.2 255.255.255.0
 //配置VRRP组1的虚地址1.0.0.128
 vrrp vrid 1 virtual-ip 1.0.0.128
 //配置VRRP组1的优先级为80，使RTB成为Backup
 vrrp vrid 1 priority 80
 //绑定IPSec策略
 ipsec policy branch
#
#
//内网接口
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
#
 //静态路由配置，使其进入IPSec接口
 ip route-static 192.168.1.0 255.255.255.0 1.0.0.254
#
```

Branch上配置

```
#
//配置DPD组vrrp，采用默认配置10秒空闲计时，5秒应答等候超时
ike dpd vrrp
#
//IKE Peer配置
ike peer center
 pre-shared-key h3c
 remote-address 1.0.0.128
 local-address 1.0.0.254
 //指定dpd组
 dpd vrrp
#
//IPSec提议配置
ipsec proposal def
#
//IPSec策略配置
ipsec policy center 1 isakmp
 security acl 3000
 ike-peer center
 proposal def
#
//ACL配置
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255

#
//对接接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.0.0.254 255.255.255.0
 //绑定IPSec策略
 ipsec policy center
#
//内网接口
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
 //静态路由配置，使其进入IPSec接口
 ip route-static 192.168.0.0 255.255.255.0 1.0.0.128
#
```

四、配置关键点:

1) RTA和RTB上配置VRRP，参考VRRP典型配置；

2) RTA和RTB的IPSec配置一致，都指定IKE Local-address为VRRP虚地址；

3) Branch上IKE指定对端地址为VRRP虚地址

4）SR66需要B02版本才能支持该功能