SR6600路由器IPSec多网段独立保护功能的配置

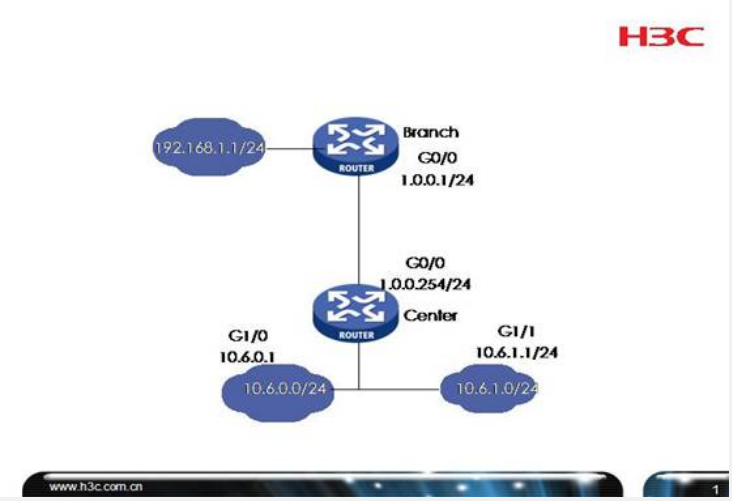
管祥杰 2008-12-11 发表

SR6600路由器IPSec多网段独立保护功能的配置

关键词：SR66;GRE;IPSec;IKE;VPN;多网段独立保护

一、组网需求:
总部内部有多个网段，要求分支内网访问总部不同网段时使用独立的加密密钥
设备清单：SR6600路由器2台

二、组网图:



三、配置步骤:
设备和版本：SR6600

Center的配置

```
#
//创建与分支的IKE Peer，可根据实际需要可以采用野蛮模式和NAT穿越
ike peer branch
 //预共享密钥
 pre-shared-key h3c-sr66
 //分支路由器的地址
 remote-address 1.0.0.1
 //指定本端地址
 local-address 1.0.0.254
#
//建立IPSec提议
ipsec proposal default
#
//建立IPSec策略branch，序号10，用于保护分支与10.6.0.0/24的流量
ipsec policy branch 10 isakmp
 //对匹配ACL 3000的流量使用该策略
 security acl 3000
 //指定所使用的IKE Peer
 ike-peer branch
 //指定使用的IPSec提议
 proposal default
#
//建立IPSec策略branch，序号20，用于保护分支与10.6.1.0/24的流量
ipsec policy branch 20 isakmp
 //对匹配ACL 3001的流量使用该策略
 security acl 3001
 //指定所使用的IKE Peer
 ike-peer branch
 //指定使用的IPSec提议
 proposal default
#
//ACL 3000，匹配从10.6.0.0/24到192.168.1.0/24的流量
acl number 3000
 rule 0 permit ip source 10.6.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
//ACL 3001，匹配从10.6.1.0/24到192.168.1.0/24的流量
acl number 3001
 rule 0 permit ip source 10.6.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
//总部外网出口G0/0
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 //总部路由器的出口地址
 ip address 1.0.0.254 255.255.255.0
//绑定IPSec策略branch
 ipsec policy branch
#
interface Ethernet GigabitEthernet1/0
 port link-mode route
 combo enable copper
 //公司总部内网接口地址
 ip address 10.6.0.1 255.255.255.0
#
interface GigabitEthernet1/1
 port link-mode route
 combo enable copper
 //公司总部内网接口地址
 ip address 10.6.1.1 255.255.255.0
#
//配置一条目的地址为分支内网的静态路由
 ip route-static 192.168.1.0 255.255.255.0 1.0.0.1
#
```

Branch配置

```
#
//创建与总部的IKE Peer，可根据实际需要可以采用野蛮模式和NAT穿越
ike peer center
 //预共享密钥
 pre-shared-key h3c-sr66
 //分支路由器的地址
 remote-address 1.0.0.254
 //指定本端地址
 local-address 1.0.0.1
#
//建立IPSec提议
ipsec proposal default
#
//建立IPSec策略center，序号10，用于保护分支与10.6.0.0/24的流量
ipsec policy center 10 isakmp
 //对匹配ACL 3000的流量使用该策略
 security acl 3000
 //指定所使用的IKE Peer
 ike-peer center
 //指定使用的IPSec提议
 proposal default
#
//建立IPSec策略center，序号20，用于保护分支与10.6.1.0/24的流量
ipsec policy center 20 isakmp
 //对匹配ACL 3001的流量使用该策略
 security acl 3001
 //指定所使用的IKE Peer
 ike-peer center
 //指定使用的IPSec提议
 proposal default
#
//ACL 3000，匹配从192.168.1.0/24到10.6.0.0/24的流量
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 10.6.0.0 0.0.0.255
//ACL 3001，匹配从192.168.1.0/24到的流量10.6.1.0/24
acl number 3001
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 10.6.1.0 0.0.0.255
#
//分支外网出口G0/0
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 //分支的出口地址
 ip address 1.0.0.1 255.255.255.0
//绑定IPSec策略center
 ipsec policy center
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 //分支内网接口地址
 ip address 192.168.1.1 255.255.255.0
#
//配置一条目的地址时总部内网的静态路由
 ip route-static 10.0.0.0 255.0.0.0 1.0.0.254
#
```

四、配置关键点：

1) 总部ACL配置需要注意**不能配置Deny的规则**，否则部分流量可能会被丢弃；

2) 分支的ACL需要与总部ACl互为镜像；

3) 两端路由器都需要配置多序号安全策略；

4) 安全提议必须使用隧道模式；

5) 所有的IPSec策略都绑定在对应的外网出接口上；

6) 必须保证总部和分支出接口能互通。