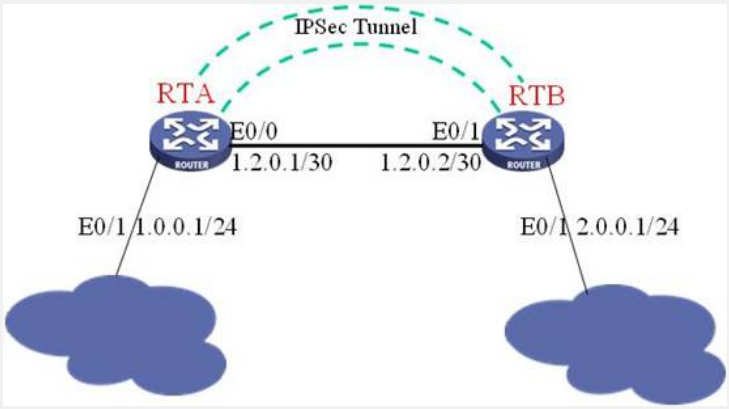
MSR路由器IPSEC + IKE功能的配置

丘子隽 2006-10-14 发表

MSR路由器
IPSEC + IKE功能的配置

关键词：MSR;IPSec;IKE

一、**组网需求**：
RTA和RTB各接一个网段，要求2个网段之间的IP流在RTA和RTB之间用IPSec加密传送
设备清单：MSR路由器2台
二、组网图：



三、配置步骤：
适用设备和版本：MSR、Version 5.20, Beta 1105后所有版本。

RTA配置

```
#
//定义IKE提议，使用IKE必配
ike proposal 1
#
//定义IKE对等体，IKE必配
ike peer rtb
 //使用预设口令身份验证
 pre-shared-key 123
 //对等体的IP地址
 remote-address 1.2.0.2
#
//定义IPSec提议
ipsec proposal rtb
#
//定义IPSec策略，协商方式为isakmp，即使用IKE协商
ipsec policy rtb 1 isakmp
 //定义需要加密传送的ACL
 security acl 3000
 //选择使用的IKE对等体
 ike-peer rtb
 //选择安全策略
 proposal rtb
#
//安全ACL
acl number 3000
 rule 0 permit ip source 1.0.0.0 0.0.0.255 destination 2.0.0.0 0.0.0.255
#
interface Ethernet0/0
 port link-mode route
 description connects to RTB
 ip address 1.2.0.1 255.255.255.252
 //将安全策略绑定在端口下
 ipsec policy rtb
#
interface Ethernet0/1
 port link-mode route
 description connects to 1.0.0.0/24 subnet
 ip address 1.0.0.1 255.255.255.0
#
 //定义静态路由，可以使用动态路由代替
 ip route-static 2.0.0.0 255.255.255.0 1.2.0.2
#
```

RTB配置

```
#
//定义IKE提议，使用IKE必配
ike proposal 1
#
//定义IKE对等体，IKE必配
ike peer rta
 //使用预设口令身份验证
 pre-shared-key 123
 //对等体的IP地址
 remote-address 1.2.0.1
#
//定义IPSec提议
ipsec proposal rta
#
//定义IPSec策略，协商方式为isakmp，即使用IKE协商
ipsec policy rta 1 isakmp
 //定义需要加密传送的ACL
 security acl 3000
 //选择使用的IKE对等体
 ike-peer rta
 //选择安全策略
 proposal rta
#
//安全ACL
acl number 3000
 rule 0 permit ip source 2.0.0.0 0.0.0.255 destination 1.0.0.0 0.0.0.255
#
interface Ethernet0/0
 port link-mode route
 description connects to RTA
 ip address 1.2.0.2 255.255.255.252
 //将安全策略绑定在端口下
 ipsec policy rta
#
interface Ethernet0/1
 port link-mode route
 description connects to 2.0.0.0/24 subnet
 ip address 2.0.0.1 255.255.255.0
#
 //定义静态路由，可以使用动态路由代替
 ip route-static 1.0.0.0 255.255.255.0 1.2.0.1
#
```

四、**配置关键点**:

1) 先定义ACL和保证需要加密的数据IP可达;

2) 要定义IKE Proposal、IKE Peer、IPSec Proposal和IPSec Policy;

3) 注意上述配置中只有IPSec Policy配置需要引用IPSec Proposal和IKE Peer，其余配置个不相干;

4) 将定义好的IPSec Policy绑定到指定的出接口;

5) ACL一定不要最后添加一条deny ip的规则，该配置会导致不需要加密的流量被丢弃。