

SR6600路由器IPSEC Over GRE功能的配置

管祥杰 2008-12-11 发表

SR6600路由器IPSEC Over GRE功能的配置

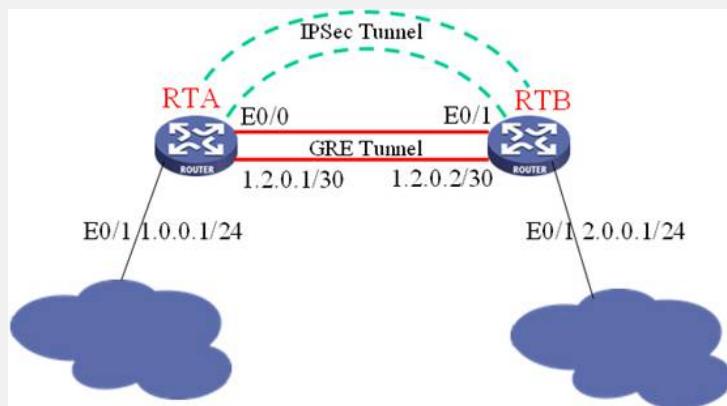
关键词：SR66;IPSec;IKE;GRE

一、组网需求：

RTA和RTB之间建立GRE隧道，RTA和RTB下挂网段间流量走GRE，在GRE中对流量进行加密

设备清单：SR6600路由器2台

二、组网图：



三、配置步骤：

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，注意是GRE Tunnel的地址  
remote-address 1.2.1.2  
#  
//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  
#  
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GRE隧道  
interface Tunnel0  
//隧道口地址，用于IKE协商和GRE封装  
ip address 1.2.1.1 255.255.255.252  
source 1.2.0.1  
destination 1.2.0.2  
//将IPSec策略绑定到GRE隧道  
ipsec policy rtb  
#  
//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 Tunnel0  
#
```

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 1.2.1.1
#
//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GRE隧道
interface Tunnel0
//隧道口地址， 用于IKE协商和GRE封装
ip address 1.2.1.2 255.255.255.252
source 1.2.0.2
destination 1.2.0.1
将IPSec策略绑定到GRE隧道上
ipsec policy rta
#
//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 Tunnel0
#

```

四、配置关键点：

- 1) 和基本IPSec配置较为相似；
- 2) IKE Peer的Remote address是对方的GRE隧道口IP地址， 不是物理接口地址；
- 3) IPSec策略绑定到GRE隧道上；
- 4) 定义静态路由或策略路由将需要加密的流量引入到GRE隧道上。