

SR6600路由器IPSec穿越NAT功能的配置

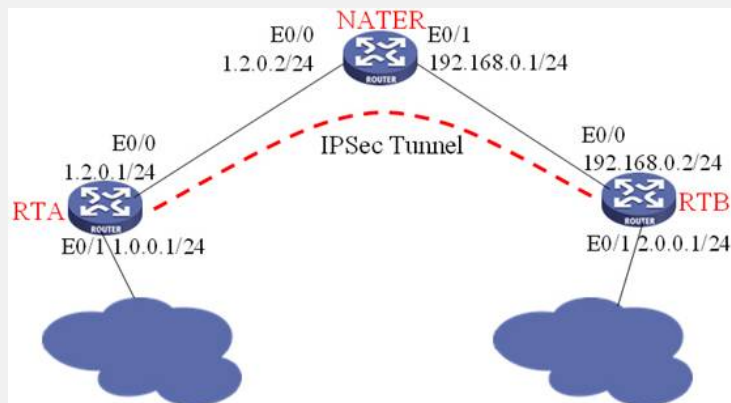
关键字: SR66;IPSec;NAT;野蛮模式;静态NAT

一、组网需求:

RTA、RTB之间通过NATER路由器进行静态地址转换, RTA、RTB之间建立支持NAT穿越的野蛮模式IPSec

设备清单: SR6600路由器3台

二、组网图:



三、配置步骤:

RTA配置

```

#
//指定本端的IKE名字
ike local-name rta
#
ike proposal 1
#
ike peer rtb
//指定为野蛮模式
exchange-mode aggressive
pre-shared-key 123
//使用name识别
id-type name
//对端名字
remote-name rtb
//使能NAT检测与穿越
nat traversal
#
ipsec proposal rtb
#
ipsec policy rtb 1 isakmp
security acl 3000
ike-peer rtb
proposal rtb
#
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 GigabitEthernet0/0
port link-mode route
description connects to NATER
ip address 1.2.0.1 255.255.255.0
ipsec policy rtb
#
interface GigabitEthernet0/1
port link-mode route
description connects to 1.0.0.0/24 subnet
ip address 1.0.0.1 255.255.255.0
#
ip route-static 2.0.0.0 255.255.255.0 1.2.0.3
#

```

RTB配置

```

#
//定义本端IKE名字
ike local-name rtb
#
ike proposal 1
#
ike peer rta
//指定使用野蛮模式
exchange-mode aggressive
pre-shared-key 123
//使用名字标识
id-type name
//对端名字
remote-name rta
//对端地址，私网侧必须配置
remote-address 1.2.0.1
//使能NAT探测和穿越
nat traversal
#
ipsec proposal rta
#
ipsec policy rta 1 isakmp
security acl 3000
ike-peer rta
proposal rta
#
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 GigabitEthernet0/0
port link-mode route
description connects NATER
ip address 192.168.0.2 255.255.255.0
ipsec policy rta
#
interface GigabitEthernet0/1
port link-mode route
description connects to 2.0.0.0/24 subnet
ip address 2.0.0.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.0.1
#

```

NATER配置

```
#
//定义静态NAT转换
nat static 192.168.0.2 1.2.0.3
#
interface GigabitEthernet0/0
port link-mode route
//在公网接口绑定NAT转换
nat outbound static
description connects to RTA
ip address 1.2.0.2 255.255.255.0
#
//私网接口
interface GigabitEthernet0/1
port link-mode route
description connects to RTB
ip address 192.168.0.1 255.255.255.0
#
```

四、配置关键点：

- 1) 先配置NAT，保证RTA和RTB经过NAT保证互通；
- 2) RTA和RTB都要定义IKE Local-Name；
- 3) 使用IKE Peer的野蛮模式；
- 4) 指定IKE Peer的id-type为name；
- 5) RTA和RTB都需要指定remote-name；
- 6) RTB还需要指定remote-address，因为RTB处于私网侧；
- 7) RTA和RTB都需要使能NAT探测与穿越。