AR系列路由器标准IPSec的典型配置

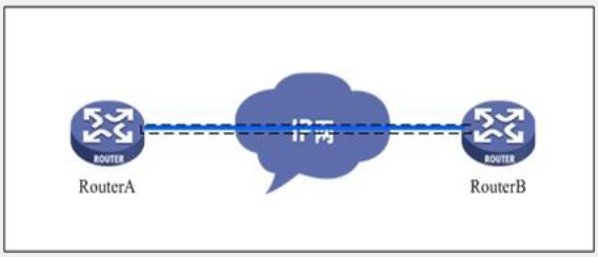
姚忆斌 2006-09-14 发表

AR系列路由器标准ipsec的典型配置

【需求】

两台路由器通过internet采用ipsec tunnel方式互通。

【组网图】



【配置脚本】

RouterA配置脚本

```
#
sysname RouterA
#
radius scheme system
#
domain system
#
ike proposal 1
#
ike peer a
pre-shared-key huawei-3com
remote-address 202.0.0.2
#
ipsec proposal a
#
ipsec policy a 1 isakmp
security acl 3000
ike-peer a
proposal a
#
acl number 3000
rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
interface Ethernet1/0/0
ip address 192.168.1.1 255.255.255.0
#
interface Serial2/0/0
link-protocol ppp
ip address 202.0.0.1 255.255.255.0
ipsec policy a
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 202.0.0.2 preference 60
#
user-interface con 0
user-interface vty 0 4
#
return
```

RouterB配置脚本

```
#
sysname RouterB
#
radius scheme system
#
domain system
#
ike proposal 1
#
ike peer b
pre-shared-key huawei-3com
remote-address 202.0.0.1
#
ipsec proposal b
#
ipsec policy b 1 isakmp
security acl 3000
ike-peer b
proposal b
#
acl number 3000
rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
interface Ethernet1/0/0
ip address 192.168.2.1 255.255.255.0
#
interface Serial2/0/0
link-protocol ppp
ip address 202.0.0.2 255.255.255.0
ipsec policy b
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 202.0.0.1 preference 60
#
user-interface con 0
user-interface vty 0 4
#
return
```

【验证】

确认RouterA上建立ike sa

[RouterA]disp ike sa

total phase-1 SAs: 1

connection-id	peer	flag	phase	doi
2	202.0.0.2	RD|ST	**1**	IPSEC
3	202.0.0.2	RD|ST	**2**	IPSEC

flag meaning

RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT

【提示】

1、 当路由器即需要配置ipsec，又需要使用NAT的，一定要在NAT
的ACL中deny掉ipsec保护的流。否则需要进行ipsec保护的流
会先会被NAT的ACL匹配，进行NAT，而无法触发ipsec的建立。