SR6608产品IPSEC野蛮模式及穿越NAT功能的配置

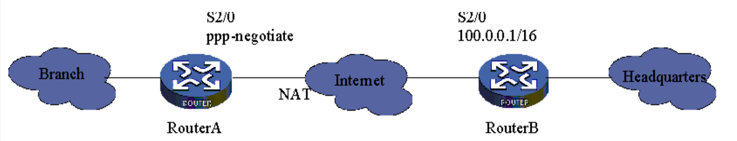
赵博　2007-12-27 发表

SR6608产品IPSEC野蛮模式及穿越NAT功能的配置

一、　组网需求：

分公司LAN通过专线接入总公司内部网，Router A的Serial2/0接口为固定IP地址，Router B动态获取IP地址。分公司自动获得的IP地址为私有IP地址，Router A的Serial2/0接口的IP地址为公网地址，故Router B上需要配置NAT穿越功能。为了保证信息安全采用IPSec/IKE方式创建安全隧道。

二、　组网图：



对应版本：SR6608-CMW520-B2109

三、　配置步骤：

(1)配置Router A

```
# 配置本端安全网关设备的名字。
<RouterA> system-view
[RouterA] ike local-name routera
# 配置acl。
[RouterA] acl number 3101 match-order auto
[RouterA-acl-adv-3101] rule permit ip source any destination any
[RouterA-acl-adv-3101] quit
# 配置地址池。
[RouterA] ip pool 1 10.0.0.2 10.0.0.10
# 配置IKE对等体peer。
[RouterA] ike peer peer
[RouterA-ike-peer-peer] exchange-mode aggressive
[RouterA-ike-peer-peer] pre-shared-key abc
[RouterA-ike-peer-peer] id-type name
[RouterA-ike-peer-peer] remote-name routerb
[RouterA-ike-peer-peer] quit
# 创建IPSec安全提议prop。
[RouterA] ipsec proposal prop
[RouterA-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterA-ipsec-proposal-prop] transform esp
[RouterA-ipsec-proposal-prop] esp encryption-algorithm des
[RouterA-ipsec-proposal-prop] esp authentication-algorithm sha1
[RouterA-ipsec-proposal-prop] quit
# 创建安全策略policy并指定通过IKE协商建立SA。
[RouterA] ipsec policy policy 10 isakmp
# 配置安全策略policy引用IKE对等体peer。
[RouterA-ipsec-policy-isakmp-policy-10] ike-peer peer
# 配置安全策略policy引用访问控制列表3101。
[RouterA-ipsec-policy-isakmp-policy-10] security acl 3101
# 配置安全策略policy引用IPSec安全提议prop。
[RouterA-ipsec-policy-isakmp-policy-10] proposal prop
[RouterA-ipsec-policy-isakmp-policy-10] quit
# 进入串口Serial2/0并配置IP地址。
[RouterA] interface serial 2/0
[RouterA-Serial2/0] ip address 100.0.0.1 255.255.0.0
# 配置串口Serial2/0引用安全策略组policy。
[RouterA-Serial2/0] ipsec policy policy
[RouterA-Serial2/0] remote address pool 1
```

(2)配置Router B

```
# 配置本端安全网关设备的名字。
```

```
<RouterB> system-view
[RouterB] ike local-name routerb
# 配置acl。
[RouterB] acl number 3101 match-order auto
[RouterB-acl-adv-3101] rule permit ip source any destination any
[RouterB-acl-adv-3101] quit
# 配置IKE对等体peer。
[RouterB] ike peer peer
[RouterB-ike-peer-peer] exchange-mode aggressive
[RouterB-ike-peer-peer] pre-shared-key abc
[RouterB-ike-peer-peer] id-type name
[RouterB-ike-peer-peer] remote-name routera
[RouterB-ike-peer-peer] remote-ip 10.0.0.1
[RouterB-ike-peer-peer] nat traversal
[RouterB-ike-peer-peer] quit
# 创建IPSec安全提议prop。
[RouterB] ipsec proposal prop
[RouterB-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterB-ipsec-proposal-prop] transform esp
[RouterB-ipsec-proposal-prop] esp encryption-algorithm des
[RouterB-ipsec-proposal-prop] esp authentication-algorithm sha1
[RouterB-ipsec-proposal-prop] quit
# 创建安全策略policy并指定通过IKE协商建立SA。
[RouterB] ipsec policy policy 10 isakmp
# 配置安全策略policy引用IKE对等体peer。
[RouterB-ipsec-policy-isakmp-policy-10] ike-peer peer
# 配置安全策略policy引用访问控制列表3101。
[RouterB-ipsec-policy-isakmp-policy-10] security acl 3101
# 配置安全策略policy引用IPSec安全提议prop。
[RouterB-ipsec-policy-isakmp-policy-10] proposal prop
[RouterB-ipsec-policy-isakmp-policy-10] quit
# 进入串口Serial2/0并配置接口动态协商IP地址。
[RouterB] interface serial 2/0
[RouterB-Serial2/0] ip address ppp-negotiate
# 配置串口Serial2/0引用安全策略组policy。
[RouterB-Serial2/0] ipsec policy policy
```

四、 配置关键点：

略