双链路备份环境中IPSec应用的方案

丘子隽 2008-08-03 发表

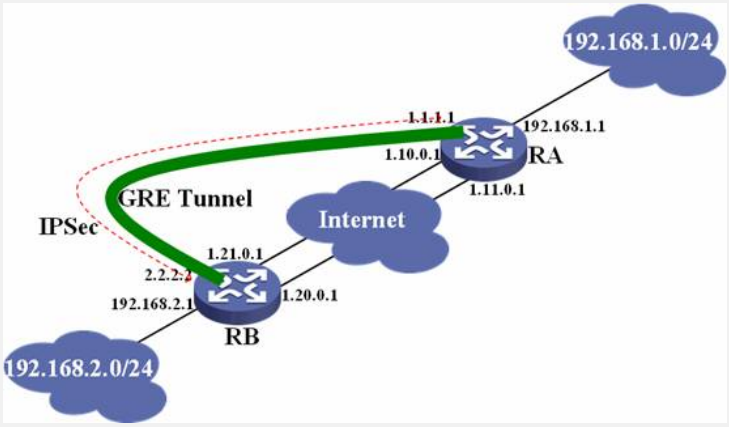
双链路备份环境中IPSec应用的方案

一、组网需求:

RB和RA各有两条链路连接到互联网，可以实现主备链路的切换，提高应用的可靠性。出于安全的考虑，要求对RA和RB之间私网数据进行IPSec加密。

设备清单：MSR二台。

二、组网图:



三、配置步骤:

RA配置

```
#
// IPSec ACL，必配
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
#
// IKE配置，必配
ike peer 2040
 pre-shared-key simple h3c
 remote-address 1.2.0.2
#
// IPSec Proposal配置，必配
ipsec proposal def
#
// IPSec Policy配置，必配
ipsec policy 83 1 isakmp
 security acl 3000
 ike-peer 2040
 proposal def
#
// 主链路
interface Ethernet0/0.10
 vlan-type dot1q vid 10
 ip address 1.10.0.1 255.255.255.0
#
// 备份链路
interface Ethernet0/0.11
 vlan-type dot1q vid 11
 ip address 1.11.0.1 255.255.255.0
#
// 用于建立GRE隧道的环回接口
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
// 内网接口
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
// GRE隧道接口，必配
interface Tunnel0
 // GRE接口地址
 ip address 1.2.0.1 255.255.255.252
 source LoopBack0
 destination 2.2.2.2
 // 在GRE接口中应用IPSec Policy
 ipsec policy 83
#
 // 路由部分配置，内网路由下一跳为对端GRE接口地址
 ip route-static 2.2.2.2 255.255.255.255 1.10.0.2
 ip route-static 2.2.2.2 255.255.255.255 1.11.0.2 preference 100
 ip route-static 192.168.2.0 255.255.255.0 1.2.0.2
#
```

RB配置

```
#
// IPSec ACL，必配
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
#
// IKE配置，必配
ike peer 2000
 pre-shared-key simple h3c
 remote-address 1.2.0.1
#
// IPSec Proposal配置，必配
ipsec proposal def
#
// IPSec Policy配置，必配
ipsec policy 83 1 isakmp
 security acl 3000
 ike-peer 20000
 proposal def
#
// 主链路
interface Ethernet0/0.20
 vlan-type dot1q vid 20
 ip address 1.20.0.1 255.255.255.0
#
// 备份链路
interface Ethernet0/0.21
 vlan-type dot1q vid 21
 ip address 1.21.0.1 255.255.255.0
#
// 用于建立GRE隧道的环回接口
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
// 内网接口
interface Vlan-interface1
 ip address 192.168.2.1 255.255.255.0
#
// GRE隧道接口，必配
interface Tunnel0
 // GRE接口地址
 ip address 1.2.0.2 255.255.255.252
 source LoopBack0
 destination 1.1.1.1
 // 在GRE接口中应用IPSec Policy
 ipsec policy 83
#
 // 路由部分配置，内网路由下一跳为对端GRE接口地址
 ip route-static 1.1.1.1 255.255.255.255 1.20.0.2
 ip route-static 1.1.1.1 255.255.255.255 1.21.0.2 preference 100
 ip route-static 192.168.1.0 255.255.255.0 1.2.0.1
#
```

四、方案说明

1) IPSec Policy是下发在接口的，数据包只有在满足下列前提下会被加密

1. 出接口配置了IPSec策略
2. 接口上已经建立了IPSec SA
3. 数据包满足IPSec SA中的数据流

2) 数据包在满足下列条件时会被解密

1. 入接口配置了IPSec策略
2. 入接口已经建立了IPSec SA
3. 数据包ESP头中SA和接口IPSec SA一致

3) 在双链路环境中，要即做到加密，又做到链路备份会比较困难

1. 在一个发起方的IKE Peer中，只能和一个remote-address发起协商，因此把IPSec策略下发到物理接口时，只能建立2对SA（1个主对主和1个备对备或2个主对备），没有办法建立4对（1个主对主、2个主对备、1个备对备）。
2. 如果把IPSec策略下发到物理接口，假设采用主对主和备对备方式配置，那么当RA主接口和RB备用接口同时Down，那么此时IPSec SA将无法使用，客户内网流量将被中断。因此在物理接口下发IPSec策略方案不可行。

4) 既然物理接口下发策略受到诸多限制，那么可以建立一个GRE虚接口，GRE接口Up的条件是双方路由可达，在主备环境中可以轻松地实现这一点，然后把IPSec策略下发到GRE隧道中，因此IPSec SA可以保证和GRE接口同时存活，再把私网数据导入到GRE隧道中即可实现加密。

5) 这个方案的关键之处在于把IPSec加密和链路备份分开实现，通过GRE隧道屏蔽传输链路的切换，为IPSec SA建立一个始终UP的接口，最终做到网络切换，SA不切换。

6) 这个方案可行的一个前提是要把GRE的源、目的地址路由引入到Internet中，并且要求Internet可以根据主备链路状况进行路由切换。