AR系列路由器与VRRP备份组虚地址之间建立IPSEC的典型配置

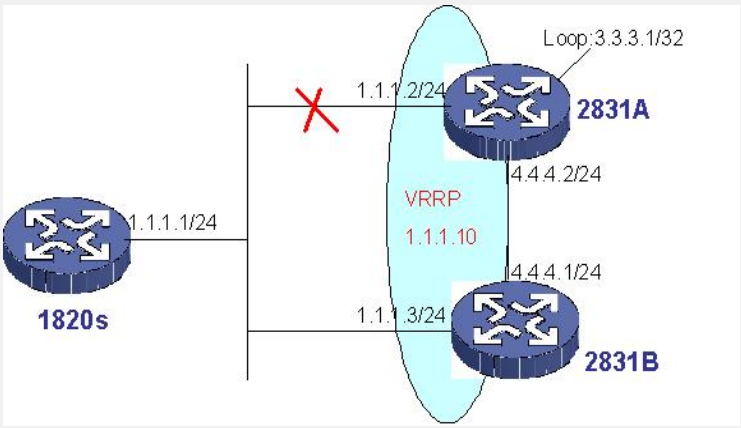
沈杨豪 2006-11-01 发表

AR系列路由器与VRRP备份组虚地址之间建立IPSEC的典型配置

【需求】

AR系列路由器与VRRP备份组虚地址之间建立IPSEC安全隧道。并要求在VRRP备份组主备切换时安全隧道能够迅速自动恢复。

【组网图】



【配置脚本】

1820s配置脚本

```
#
sysname 1820s
#
ike proposal 1                    //配置ike proposal
#
ike dpd dpd1                      //配置ike dpd
interval-time 1
time-out 1
#
ike peer vrrp                     //配置ike peer
pre-shared-key shen
remote-address 1.1.1.10
local-address 1.1.1.1
dpd dpd1
#
ipsec proposal pro                //配置ipsec proposal
#
ipsec policy pol 1 isakmp         //配置ipsec policy
security acl 3000
ike-peer vrrp
proposal pro
#
acl number 3000                   //配置安全acl
rule 0 permit ip source 2.2.2.1 0 destination 3.3.3.0 0.0.0.255
rule 1 deny ip
#
interface Ethernet1/0
ip address 1.1.1.1 255.255.255.0
ipsec policy pol                  //接口上应用ipsec policy
#
interface LoopBack0
ip address 2.2.2.1 255.255.255.255
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.10 preference 60
                                  //缺省路由指向vrrp虚地址
#
```

2831A配置脚本

```
#
sysname 2831-A
#
vrrp ping-enable                    //使虚地址支持ping操作
#
ike proposal 1                      //配置ike proposal
#
ike dpd dpd1                        //配置ike dpd
interval-time 1
time-out 1
#
ike peer 1820s                      //配置ike peer
pre-shared-key shen
remote-address 1.1.1.1
local-address 1.1.1.10
dpd dpd1
#
ipsec proposal pro                  //配置ipsec proposal
#
ipsec policy pol 1 isakmp           //配置ipsec policy
security acl 3000
ike-peer 1820s
proposal pro
#
acl number 3000                     //配置安全acl
rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.1 0
rule 1 deny ip
#
interface Ethernet2/0
ip address 1.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 1.1.1.10   //接口上配置vrrp组，优先级默认为100
ipsec policy pol                    //接口上应用ipsec policy
#
interface Ethernet2/1
ip address 4.4.4.2 255.255.255.0
#
interface LoopBack0
ip address 3.3.3.1 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.1 0.0.0.0
network 4.4.4.0 0.0.0.255
#
ip route-static 2.2.2.1 255.255.255.255 1.1.1.1 preference 60
ip route-static 2.2.2.1 255.255.255.255 4.4.4.1 preference 80
#
return
```

2831B配置脚本

```
#
sysname 2831-B
#
vrrp ping-enable                    //使虚地址支持ping操作
#
ike proposal 1                      //配置ike proposal
#
ike dpd dpd1                        //配置ike dpd
interval-time 1
time-out 1
#
ike peer 1820s                      //配置ike peer
pre-shared-key shen
remote-address 1.1.1.1
local-address 1.1.1.10
dpd dpd1
#
ipsec proposal pro                  //配置ipsec proposal
#
ipsec policy pol 1 isakmp           //配置ipsec policy
security acl 3000
ike-peer 1820s
proposal pro
#
acl number 3000                     //配置安全acl
rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.1 0
rule 1 deny ip
#
interface Ethernet0/0
ip address 1.1.1.3 255.255.255.0
vrrp vrid 1 virtual-ip 1.1.1.10     //接口上配置vrrp组
vrrp vrid 1 priority 90             //配置vrrp组优先级为90
ipsec policy pol                    //接口上应用ipsec policy
#
interface Ethernet0/1
ip address 4.4.4.1 255.255.255.0
#
interface LoopBack0
ip address 3.3.3.2 255.255.255.255
#
ospf 1
area 0.0.0.0
network 3.3.3.2 0.0.0.0
network 4.4.4.0 0.0.0.255
#
ip route-static 2.2.2.1 255.255.255.255 1.1.1.1 preference 60
ip route-static 2.2.2.1 255.255.255.255 4.4.4.2 preference 80
#
return
```

【验证】

2831A由于优先级高成为备份组的master，此时在1820s上ping 2831A的环回地址3.3.3.1。IPSEC隧道成功建立，如下所示：

```
<1820s>dis ike sa
  total phase-1 SAs: 1
  connection-id  peer           flag       phase   doi
 ----------------------------------------------------------------
     52         1.1.1.10       RD|ST       1     IPSEC
     53         1.1.1.10       RD|ST       2     IPSEC

 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

现将图示链路断开后，2831B成为备份组master，再在1820s上ping 2831A的环回地址3.3.3.1。IPSEC隧道也成功建立，如下所示：

```
 <1820s>dis ike sa
  total phase-1 SAs: 1
  connection-id  peer           flag       phase   doi
 ----------------------------------------------------------------
     55         1.1.1.10       RD|ST       1     IPSEC
     56         1.1.1.10       RD|ST       2     IPSEC

 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

可以看到，此时的sa与之前的sa是不一样的，说明主备切换时安全隧道能够自动恢复

。

【提示】

1、此应用需要用到ike dpd特性。

2、在备份组中的路由器上配置ike peer时，一定要配置local address为虚地址。