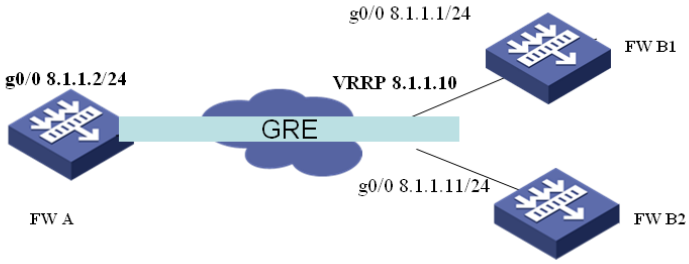
防火墙使用VRRP虚地址建立GRE典型配置

巫继雨 2009-09-07 发表

防火墙使用VRRP虚地址建立GRE典型配置

一、组网需求:



两端防火墙设备计划建立GRE隧道，但由于一端为VRRP组网，所以需要使用VRRP的虚地址来创建GRE Tunnel。在VRRP发生切换的时候，相应的GRE隧道也可以发生切换，进行备份。

【注意】：GRE Tunnel接口上是无法运行VRRP协议的，但可以运行OSPF、IPSec、组播等协议。

二、配置步骤:

1. FW A配置

```
#
interface Tunnel100
 ip address 100.1.1.2 255.255.255.252
 source 8.1.1.2
 destination 8.1.1.10            //destination地址指向VRRP虚地址
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface Tunnel100         //Tunnel口也必须加入安全域

 set priority 85
```

2. FW B配置

B1和B2的配置完全相同

```
#
interface Tunnel100
 ip address 100.1.1.1 255.255.255.252
 source 8.1.1.10                 //source地址使用VRRP虚地址

 destination 8.1.1.2
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface Tunnel100         //Tunnel口也必须加入安全域
 set priority 85
```

完成上述配置后，发现接口协议UP，也可以ping通本端，但却无法ping通对端。

```
[FW_B1]dis ip inter br
*down: administratively down
(s): spoofing
 Interface                IP Address      Physical Protocol     Description
 Tunnel100                  100.1.1.1       up       up           Tunnel100...
[FW_B1]ping 100.1.1.1
  PING 100.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 100.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
[FW_B1]ping 100.1.1.2
  PING 100.1.1.2: 56  data bytes, press CTRL_C to break
    Request time out
```

三、原因分析

原因在于B1设备属于V3平台防火墙，在引用VRRP虚地址作为GRE的source地址时，GRE Tunnel只是在控制平面协议UP了，但无法真正在数据平面完成数据转发。

解决办法：

在B1上配置Loopback地址(B2上配置相同)，使得GRE隧道引用的VRRP虚地址以实际接口的形式存在，这样就可以完成数据转发了。

[FW_B1]ip address 8.1.1.10 255.255.255.255　//注意掩码为32位即可

[FW_B1]ping 100.1.1.2

　PING 100.1.1.2: 56　data bytes, press CTRL_C to break

Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=1 ms

对于V5的防火墙来说，不存在上述问题，即可以直接使用VRRP虚地址来建立GRE隧道。

四、配置关键点：

1，GRE隧道使用VRRP的虚地址作为source(destination)地址；

2，配置和VRRP虚地址一样(掩码不同)的Loopback地址。