SecPath 1800F混合模式下双机热备典型配置

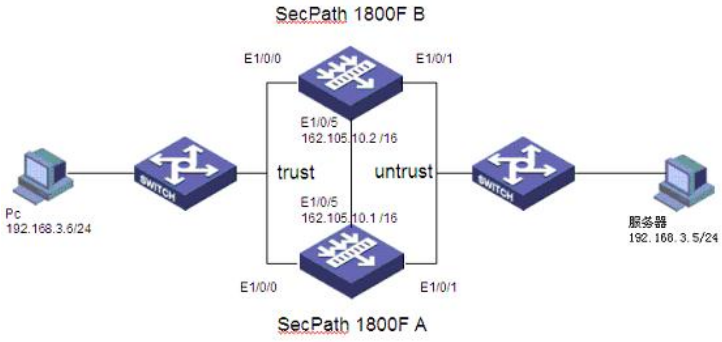
雷浩【技术大咖】 2006-10-11 发表

SecPath 1800F混合模式下双机热备典型配置

一、组网需求:

SecPath 1800F两台；防火墙的上下行设备采用二层交换机进行连接。

二、组网图:



三、配置步骤:

适用版本:

非P2P限流版 Secpath1800F Version 3.30 RELEASE 0336.01(08) 及以上版本

P2P限流版 Secpath1800F Version 3.30 RELEASE 0332.13(08)及以上版本

SecPath 1800F A配置:

```
#
 sysname SecPath 1800F A
#
 hrp enable                                  // 使能HRP
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit interzone local untrust direction inbound
 firewall packet-filter default permit interzone local untrust direction outboun
d
 firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outboun
d
 firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
#
 bypass switch-back auto
#
 firewall mode composite
#
 firewall statistic system enable
 firewall p2p include bt
 firewall p2p include edonkey
 firewall p2p include thunder
 undo firewall p2p include fasttrack
 undo firewall p2p include gnutella
 undo firewall p2p include pplive
 undo firewall p2p include ppstream
 undo firewall p2p include bt-dht
 undo firewall p2p include edk-kad
#
interface Aux0
 async mode flow
```

```
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
 ip address 162.105.10.1 255.255.0.0
 vrrp vrid 1 virtual-ip 162.105.10.3          // 配置vrrp备份组1的虚拟IP
 vrrp vrid 1 track Ethernet1/0/0              // 配置接口监视
 vrrp vrid 1 track Ethernet1/0/1              // 配置接口监视
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface GigabitEthernet2/0/0
#
interface GigabitEthernet2/0/1
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust                          // 接口加入域中
 set priority 85
 add interface Ethernet1/0/0
#
firewall zone untrust                        // 接口加入域中
 set priority 5
 add interface Ethernet1/0/1
#
firewall zone dmz
 set priority 50
#
firewall zone name hrp                       // 创建HRP 域，加入接口
 set priority 10
 add interface Ethernet1/0/5
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone local hrp
#
firewall interzone trust untrust
#
firewall interzone trust dmz
#
firewall interzone trust hrp
#
```

```
firewall interzone dmz untrust
#
firewall interzone hrp untrust
#
firewall interzone dmz hrp
#
vrrp group 1                                  // 创建VRRP管理组
 add interface Ethernet1/0/5 vrrp vrid 1 data    // 添加VRRP备份组
 vrrp-group enable                            // 使能VGMP功能
 vrrp-group priority using-vrrppriority      // VGMP的优先级使用VRRP的优先级
 vrrp-group preempt delay 0                    // 使能抢占功能
 undo vrrp-group group-send
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
SecPath 1800F B配置:
#
 sysname SecPath 1800F B
#
 hrp enable                                    // 使能HRP
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit interzone local untrust direction inbound
 firewall packet-filter default permit interzone local untrust direction outbound
firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outbound
firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
#
 firewall mode composite                       // 混合模式
#
 firewall statistic system enable
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
```

```
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
 ip address 162.105.10.2 255.255.0.0
 vrrp vrid 1 virtual-ip 162.105.10.3          // 配置vrrp备份组1的虚拟IP
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface GigabitEthernet2/0/0
#
interface GigabitEthernet2/0/1
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet1/0/0
#
firewall zone untrust
 set priority 5
 add interface Ethernet1/0/1
#
firewall zone dmz
 set priority 50
#
firewall zone name hrp
 set priority 10
 add interface Ethernet1/0/5
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone local hrp
#
firewall interzone trust untrust
#
firewall interzone trust dmz
#
firewall interzone trust hrp
#
firewall interzone dmz untrust
#
firewall interzone hrp untrust
#
firewall interzone dmz hrp
#
vrrp group 1
 add interface Ethernet1/0/5 vrrp vrid 1 data    // 添加VRRP备份组
 vrrp-group enable                              // 使能VGMP功能
 vrrp-group priority using-vrrppriority      // VGMP的优先级使用VRRP的优先级
 vrrp-group preempt delay 0                    // 使能抢占功能
 undo vrrp-group group-send
#
```

```
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

四、配置关键点:

1. VGMP的优先级使用VRRP的优先级，将添加的到VRRP管理组中的VRRP备份组的优先级相加后除去添加的VRRP备份组的个数。但需要注意累积的VRRP优先级不应包含含有transfer-only参数的VRRP的优先级。当使用vrrp的优先级作为VGMP的优先级后，接口下VRRP的命令就可以使用了。
2. 在防火墙上执行display vrrp-group verbose，查看VGMP的状态是否正确，接口下的vrrp是否已经up，如果是down状态说明接口协议层有问题，检查接口；如果两台防火墙接口都是peerdown状态，说明VRRP的协商报文没有联通，查看两台防火墙的vrrp虚拟ip是否相同等。