

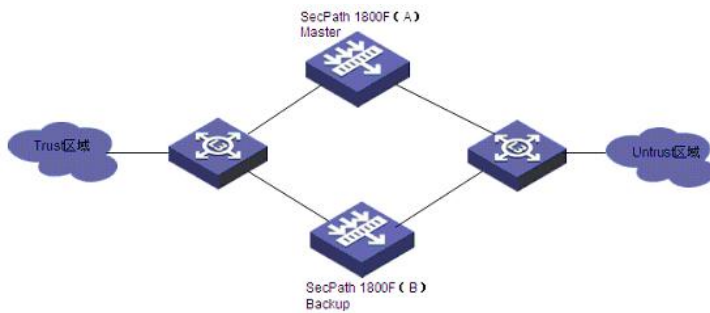
SecPath 1800F路由模式下双机热备的负载分担典型配置

一、组网需求:

SecPath 1800F两台; 在SecPath 1800F A中管理组1的状态为master, 管理组2的状态为slave; SecPath 1800F B中管理组1的状态为slave, 管理组2的状态为master。当从trust域来的业务当网关指向备份组1的虚拟IP时, 则通过SecPath 1800F A来转发, 当网关执行备份组3的虚拟IP时, 则由SecPath 1800F B来转发, 从而实行业务的分流。

Quidway S3500两台, 用作Trust区域和Untrust区域接入。

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 A
#
hrp enable // 启用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
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 outbound
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 route
#
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
  ip address 192.168.10.1 255.255.255.0 // 配置接口地址
  vrrp vrid 1 virtual-ip 192.168.10.4 // 配置虚拟地址
  vrrp vrid 3 virtual-ip 192.168.10.5 // 配置虚拟地址
#
interface Ethernet1/0/1
  ip address 192.168.3.1 255.255.255.0 // 配置接口地址
  vrrp vrid 2 virtual-ip 192.168.3.4 // 配置虚拟地址
  vrrp vrid 4 virtual-ip 192.168.3.5 // 配置虚拟地址
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
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 // 接口加入域中
#
firewall zone untrust
  set priority 5
  add interface Ethernet1/0/1 // 接口加入域中
#
firewall zone dmz
  set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust
#
firewall interzone trust dmz
#
firewall interzone dmz untrust
#
vrrp group 1 // 配置VRRP组
```

```

add interface Ethernet1/0/0 vrrp vrid 1 data // 加相应的虚拟地址到VRRP组
add interface Ethernet1/0/1 vrrp vrid 2 data // 加相应的虚拟地址到VRRP组
vrrp-group enable // 启用VRRP组
vrrp-group priority 105 // 设置组的优先级
vrrp-group preempt delay 0 // 设置抢占时间和方式
undo vrrp-group group-send
vrrp group 2 // 配置VRRP组
add interface Ethernet1/0/0 vrrp vrid 3 data // 加相应的虚拟地址到VRRP组
add interface Ethernet1/0/1 vrrp vrid 4 data // 加相应的虚拟地址到VRRP组
vrrp-group enable // 启用VRRP组
vrrp-group preempt delay 0 // 设置抢占时间和方式
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 B
#
hrp enable // 启用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
#
firewall mode route // 路由模式
#
firewall statistic system enable
#
interface Aux0
async mode flow
link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
ip address 192.168.10.2 255.255.255.0 // 配置接口地址

```

```

vrpp vrid 1 virtual-ip 192.168.10.4 // 配置虚拟地址
vrpp vrid 3 virtual-ip 192.168.10.5 // 配置虚拟地址
#
interface Ethernet1/0/1
ip address 192.168.3.2 255.255.255.0 // 配置接口地址
vrpp vrid 2 virtual-ip 192.168.3.4 // 配置虚拟地址
vrpp vrid 4 virtual-ip 192.168.3.5 // 配置虚拟地址
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
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 // 接口加入域中
#
firewall zone untrust
set priority 5
add interface Ethernet1/0/1 // 接口加入域中
#
firewall zone dmz
set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust
#
firewall interzone trust dmz
#
firewall interzone dmz untrust
#
vrpp group 1 // 配置VRRP组
add interface Ethernet1/0/0 vrrp vrid 1 data // 加相应的虚拟地址到VRRP组
add interface Ethernet1/0/1 vrrp vrid 2 data // 加相应的虚拟地址到VRRP组
vrpp-group enable // 启用VRRP组
vrpp-group preempt delay 0 // 设置抢占时间和方式
undo vrrp-group group-send
vrpp group 2 // 配置VRRP组
add interface Ethernet1/0/0 vrrp vrid 3 data // 加相应的虚拟地址到VRRP组
add interface Ethernet1/0/1 vrrp vrid 4 data // 加相应的虚拟地址到VRRP组
vrpp-group enable // 启用VRRP组
vrpp-group priority 105 // 设置组的优先级
vrpp-group preempt delay 0 // 设置抢占时间和方式

```

```
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
```

一、配置关键点:

1. VGMP的优先级默认优先级为100。VGMP优先级的递减算法: 递减后的优先级 = 优先级 - 优先级/16, 当主防火墙出故障时, 递减后的优先级应比slave防火墙的优先级低, 才可进行主备状态切换, 否则出故障的防火墙仍然为主状态, 从而导致业务会中断。
2. 在接口下配置VRRP备份组时, 虚拟IP需要和接口地址同一网段。