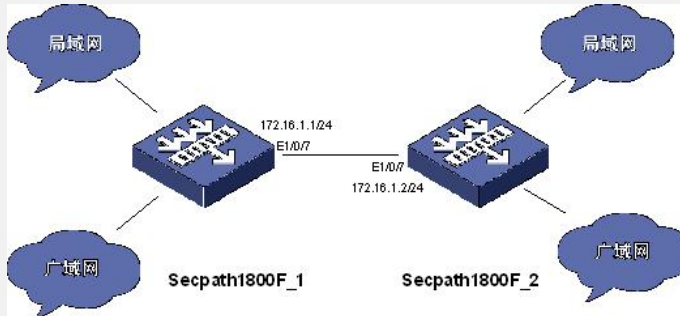


Secpath1800F HRP功能的配置

一、组网需求:

防火墙通过一个直接互连的接口做HRP来达到两个防火墙上session互相备份的目的。

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

Secpath1800F_A :

```
#
sysname Secpath1800A
#
acl number 3001
rule 0 permit ip
#
hrp enable // 启用hrp
hrp interface Ethernet1/0/7 // 选择hrp使用的防火墙接口
#
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
#
firewall statistic system enable
#
interface Aux0
async mode flow
link-protocol ppp
#
interface Ethernet0/0/0
```

```

#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
portswitch
#
interface Ethernet1/0/1
portswitch
#
interface Ethernet1/0/2
portswitch
#
interface Ethernet1/0/3
ip address 3.3.3.3 255.255.255.0
#
interface Ethernet1/0/4
portswitch
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
ip address 192.11.1.1 255.255.255.0
#
interface Ethernet1/0/7
ip address 172.16.1.1 255.255.255.0           // 配置接口地址
vrrp vrid 100 virtual-ip 172.16.1.101       // 配置虚拟地址
vrrp vrid 200 virtual-ip 172.16.1.102       // 配置虚拟地址
vrrp vrid 200 priority 102                 // 配置优先级
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface Ethernet1/0/1
#
firewall zone untrust
set priority 5
add interface Ethernet1/0/0
#
firewall zone dmz
set priority 50
add interface Ethernet1/0/7
#
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 Ethernet1/0/7 vrrp vrid 100 data // 加相应的虚拟地址到VRRP组
vrrp-group enable                           // 启用VRRP组(与hrp相关)
vrrp-group priority 102                     // 设置组的优先级 (注意此处为102)

```

```

vrp-group preempt delay 0 // 设置抢占方式和等待时间
undo vrrp-group group-send
vrrp group 2
add interface Ethernet1/0/7 vrrp vrid 200 data // 此组未设优先级, 使用
默认值100
vrrp-group enable
vrrp-group preempt delay 0
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

Secpath1800F_B :
#
acl number 3001
rule 0 permit ip
#
sysname Secpath1800F_B
#
hrp enable // 启用hrp
hrp interface Ethernet1/0/7 // 选择hrp使用的防火墙接口
#
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
#
firewall statistic system enable
#
interface Aux0
async mode flow
link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
portswitch
#

```

```

interface Ethernet1/0/1
portswitch
#
interface Ethernet1/0/2
portswitch
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
ip address 192.158.1.1 255.255.255.0
#
interface Ethernet1/0/5
portswitch
#
interface Ethernet1/0/6
portswitch
#
interface Ethernet1/0/7 // 配置接口的虚拟地址及相应优先级
ip address 172.16.1.2 255.255.255.0
vrrp vrid 100 virtual-ip 172.16.1.101
vrrp vrid 100 priority 102
vrrp vrid 200 virtual-ip 172.16.1.102
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface Ethernet1/0/1
#
firewall zone untrust
set priority 5
add interface Ethernet1/0/0
#
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 // 注意此组使用默认优先级值10
0
add interface Ethernet1/0/7 vrrp vrid 100 data
vrrp-group enable
vrrp-group preempt delay 0
undo vrrp-group group-send
vrrp group 2 // 注意此组使用优先级102
add interface Ethernet1/0/7 vrrp vrid 200 data
vrrp-group enable
vrrp-group priority 102
vrrp-group preempt delay 0
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：

配置时注意两个VRRP组的优先级差值不要超过5；HRP成功启用后，可以做到session同步，通常

建立的session（不包括半连接的session）在10秒钟内都会备份到备份防火墙上，ICMP的

session不会备份；配置时只能从主防火墙上配置，相应的配置会同步到从属防火墙上。

注意：不是所有的配置都能从主防火墙同步到从属防火墙，所有在从属防火墙上能做配置的操作

在主防火墙上操作时都不会对从属防火墙做备份。