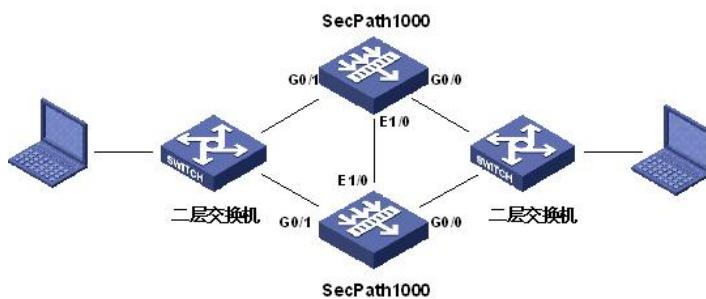


### SecPath防火墙双机热备功能的配置 (-)

#### 一、组网需求：

SecPath防火墙在双机热备的情况下做Session 的同步，单主模式。

#### 二、组网图：



#### 三、配置步骤：

适用版本 ESS 1621 之后的所有版本

```
#  
sysname Quidway-1  
#  
firewall packet-filter enable  
firewall packet-filter default permit  
#  
firewall statistic system enable  
#  
radius scheme system  
server-type huawei  
#  
domain system  
#  
local-user secpaht  
password cipher )=.#LQK.]+Q=^Q`MAF4<!!  
service-type ssh telnet terminal  
level 3  
#  
interface Aux0  
async mode flow  
#  
interface Ethernet1/0 // 该选项为选配，可以不配  
地址  
ip address 1.1.1.2 255.255.255.0  
#  
interface Ethernet1/1  
#  
interface GigabitEthernet0/0  
ip address 192.168.1.253 255.255.255.0  
#  
interface GigabitEthernet0/1  
ip address 10.1.1.253 255.255.255.0  
#  
interface Encrypt2/0  
#  
interface NULL0  
#
```

```
firewall zone local
set priority 100
#
firewall zone trust
add interface GigabitEthernet0/0
set priority 85
#
firewall zone untrust
add interface GigabitEthernet0/1
set priority 5
#
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
#
rdo 1          // 配置rdo 组, 未加深部分为设备自动生成项
priority 105    // 配置组的优先级
ha-interface interface Ethernet1/0 // 配置同步状态使用的端口
vif 1 interface GigabitEthernet0/0 virtual-ip 192.168.1.200 // 配
置虚接口地址
vif 2 interface GigabitEthernet0/1 virtual-ip 10.1.1.200      // 配
置虚接口地址
#
user-interface con 0
authentication-mode scheme
user-interface aux 0
authentication-mode scheme
user-interface vty 0 4
authentication-mode scheme
```

```
sysname Quidway-2
#
firewall packet-filter enable
firewall packet-filter default permit
#
firewall statistic system enable
#
radius scheme system
server-type huawei
#
domain system
#
local-user secpth
password cipher )=.#LQK.[)+Q=^Q`MAF4<1!!
service-type ssh telnet terminal
level 3
#
interface Aux0
async mode flow
#
interface GigabitEthernet0/0
```

```

ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet0/1
ip address 10.1.1.254 255.255.255.0
#
interface Ethernet1/0          // 选配项，可以不配地址、不加
                                入域
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface GigabitEthernet0/0
set priority 85
#
firewall zone untrust
add interface GigabitEthernet0/1
set priority 5
#
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
#
rdo 1          // 配置rdo组，配置说明同上
ha-interface interface GigabitEthernet1/0
vif 1 interface GigabitEthernet0/0 virtual-ip 192.168.1.200
vif 2 interface GigabitEthernet0/1 virtual-ip 10.1.1.200
#
user-interface con 0
authentication-mode scheme
user-interface aux 0
authentication-mode scheme
user-interface vty 0 4
authentication-mode scheme

```

#### 四、配置关键点：

注意优先级的使用，大优先级的设备为主设备，当vif组中的端口down后 rdo优先级的值会相应减小（reduce 后面的数值）。同步后的session在前面有remote的标识项。