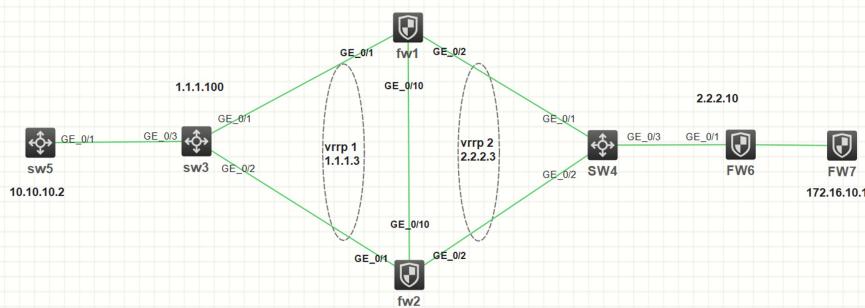


# RBM+VRRP 组网下ipsec 典型配置案例

VRRP IPSec VPN 戴航 2022-06-05 发表

## 组网及说明



基本组网如上，本实验采用HCL模拟器完成。fw1与fw2建立RBM，上下行采用vrrp对接。sw3、sw4为2层交换机，当防火墙RBM连接意外断开时，可以通过交换机透传vrrp报文，靠vrrp自身的协商机制实现主备。在fw1、fw2均使用vrrp 2的虚地址进行ipsec配置，正常情况下流量走fw1，只有fw1和fw6建立ipsec sa，由于RBM还不支持ipsec的同步，因此正常情况下fw2不和fw6建ipsec，当主备切换时流量上到fw2，感兴趣流自动触发fw2和fw6建立ipsec隧道，同时由于fw6只和vrrp虚地址建立连接，无法感知到fw1和fw2的主备切换，因此需要配置dpd保活探测，当主备切换时能及时协商新的ike sa和ipsec sa。

## 配置步骤

### 一、fw1基本配置：

```
配置接口ip地址和vrrp虚地址，g1/0/10口作为RBM接口
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.1.1 255.255.255.0
vrrp vrid 1 virtual-ip 1.1.1.3 active
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 2.2.2.1 255.255.255.0
vrrp vrid 2 virtual-ip 2.2.2.3 active
#
interface GigabitEthernet1/0/10
port link-mode route
ip address 10.0.0.1 255.255.255.0
```

接口加安全域，RBM接口不需加安全域，设备默认放通

```
security-zone name Trust
import interface GigabitEthernet1/0/1
#
security-zone name Untrust
import interface GigabitEthernet1/0/2
```

### 配置静态路由

```
ip route-static 10.10.10.0 24 1.1.1.100
ip route-static 172.16.10.0 24 2.2.2.10
```

### 配置RBM，设备作为主管理设备，主备模式

```
remote-backup group
data-channel interface GigabitEthernet1/0/10
configuration sync-check interval 12
local-ip 10.0.0.1
remote-ip 10.0.0.2
device-role primary
```

配置明细化的安全策略，放通local和trust、untrust域之间的vrrp报文，放通local和untrust间的ike协商报文，放通trust和untrust之间的数据报文。

```
security-policy ip
rule 1 name 1
action pass
source-zone local
destination-zone trust
service vrrp
rule 2 name 2
action pass
source-zone trust
destination-zone local
service vrrp
rule 3 name 3
action pass
source-zone local
destination-zone untrust
service vrrp
rule 4 name 4
action pass
source-zone untrust
destination-zone local
service vrrp
```

```

rule 5 name ike
action pass
source-zone local
source-zone untrust
destination-zone local
配置关键点
destination-zone untrust
1seRBM不支持ipsec的同步，因此需要在主备防火墙上分别配置ipsec，使用同一个vrrp虚地址作为local ip，所有ipsec的配置相同；
2action pass安全域、静态路由等RBM无法同步，需要在两台设备上分别配置；
3so需要配置dpd保活，当主备切换时，使对端设备能及时删除旧的ike sa和ipsec sa，协商新的ike sa
destination-zone untrust
source-ip-host 10.10.10.1
destination-ip-host 172.16.10.1
service ping
rule 7 name test2
action pass
source-zone untrust
destination-zone trust
source-ip-host 172.16.10.1
destination-ip-host 10.10.10.1
service ping

```

#### 配置感兴趣流

```

acl advanced 3000
rule 0 permit ip source 10.10.10.0 0.0.0.255 destination 172.16.10.0 0.0.0.255

```

```

配置ipsec，由于RBM无法同步ipsec配置和表项，因此需要配置dpd保活探测，当主备切换时能新建ips
ec sa
ipsec transform-set 1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha256
#
ipsec policy 1 1 isakmp
transform-set 1
security acl 3000
local-address 2.2.2.3
remote-address 2.2.2.10
ike-profile 1
#
ike profile 1
keychain 1
dpd interval 10 periodic
local-identity address 2.2.2.3
match remote identity address 2.2.2.10 255.255.255.255
proposal 1
#
ike proposal 1
encryption-algorithm 3des-cbc
dh group14
authentication-algorithm sha256
#
ike keychain 1
pre-shared-key address 2.2.2.10 255.255.255.255 key simple 123456

```

#### 在出接口g1/0/2上应用ipsec策略

```

interface GigabitEthernet1/0/2
ipsec apply policy 1

```

#### 二、fw2 基本配置：

```

配置接口ip地址和vrrp虚地址，g1/0/10口作为RBM接口
interface GigabitEthernet1/0/1
port link-mode route
ip address 1.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 1.1.1.3 active

```

```
#  
interface GigabitEthernet1/0/2  
port link-mode route  
ip address 2.2.2.2 255.255.255.0  
vrrp vrid 2 virtual-ip 2.2.2.3 active  
#  
interface GigabitEthernet1/0/10
```