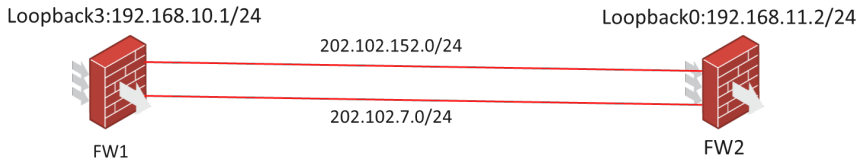
IPSec主备隧道典型配置举例

IPSec VPN　孔凡安　2021-12-28 发表

组网及说明



注：如无特别说明，同一网段中，IP 地址的主机位为其设备编号，如 FW1 的 接口若在 202.102.152.0/24 网段，则其 IP 地址为 202.102.152.1/24，以此类推。

实验环境，设置两台防火墙同网段作为隧道的两端，环回口作为感兴趣流。

主隧道在上边，即202.102.152.0/24网段，设定为主模式。

备隧道在下边，即202.102.7.0/24，设定为野蛮模式，FW2为发起方。

不涉及安全域及安全策略，默认any---any。

配置步骤

FW1配置：

```
#
ip route-static 192.168.11.0 24 202.102.152.2   //主路由
#
ip route-static 192.168.11.0 24 202.102.7.2 preference 100     //备路由
#
acl advanced 3000 description ipsec-acl rule 0 permit ip source 192.168.10.0 0.0.0.255 destination
192.168.11.0 0.0.0.255
#
ike identity fqdn FW1
#
ike keychain key  //主隧道的keychain
 pre-shared-key address 202.102.152.2 255.255.255.255 key cipher $c$3$xnKI3KVWqlwLxAN0eXbg
OD6ESAnB/8Vt6A==
#
ike keychain key1   //备隧道的keychain
 pre-shared-key address 202.102.7.2 255.255.255.255 key cipher $c$3$241FG1JxMBE9lMi93qll/IA4
MJS9+n6H/w==
#
ike proposal 1
#
ike profile pf    //主隧道的profile
 keychain key
 dpd interval 10 retry 30 on-demand
 local-identity address 202.102.152.1
 match remote identity address 202.102.152.2 255.255.255.255 proposal 1
 #
ike profile pf1
 keychain key1 dpd interval 10 retry 30 on-demand
 exchange-mode aggressive
 match remote identity fqdn FW2 proposal 1
#
ipsec transform-set ts
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
 #
ipsec policy ply 1 isakmp
 transform-set ts
 security acl 3000
 remote-address 202.102.152.2
 ike-profile pf
#
ipsec policy ply1 1 isakmp template pt1
#
ipsec policy-template pt1 1
 transform-set ts
 ike-profile pf1
#
interface GigabitEthernet6/0
 port link-mode route
 description ipsec-main
 ip address 202.102.152.1 255.255.255.0
 ipsec apply policy ply
#
interface GigabitEthernet7/0
 port link-mode route
 description ipsec-aggressive
 ip address 202.102.7.1 255.255.255.0
 ipsec apply policy ply1
```

#

FW2：

配置关键点

#

ip route-static 192.168.10.0 24 202.102.152.1 //主路由

#

ip route-static 192.168.10.0 24 202.102.7.1 preference 100 //备路由