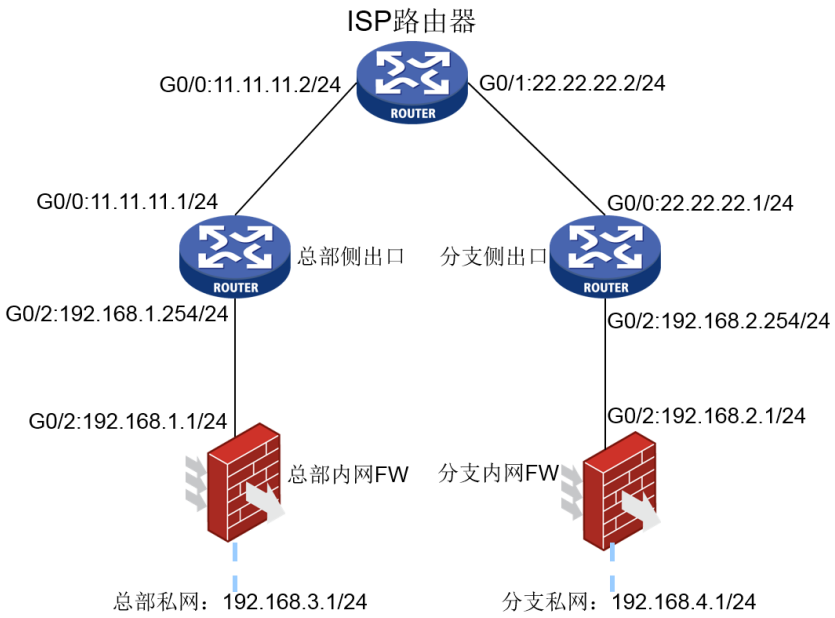
V7防火墙两端设备都在私网环境下，通过主模式建立ipsec vpn典型配置

IPSec VPN　徐猛　2019-04-19 发表

组网及说明

现场总部侧和分支侧有保护某条流量安全互访的需要，两侧出口下联均接了一台我们的V7防火墙，现场希望保护的流量为192.168.3.0/24到192.168.4.0/24。现场不希望使用出口路由进行建立ipsec隧道，希望能够使用两端私网的防火墙建立主模式的ipsec隧道。



配置步骤

（1）首先保证公网侧两端出口设备路由可达

（2）分别在两端出口设备的公网接口上配置nat outbound，以及nat server，其中nat server配置中需要将防火墙的应用ipsec策略的接口地址映射出去，映射的端口包括Isakmp端口500，4500，以及ESP/AH端口50，51：

总部侧出口路由器公网口配置：

```
 nat server protocol udp global 11.11.11.1 4500 inside 192.168.1.1 4500
 nat server protocol udp global 11.11.11.1 500 inside 192.168.1.1 500
 nat server protocol 50 global 11.11.11.1 inside 192.168.1.1
 nat server protocol 51 global 11.11.11.1 inside 192.168.1.1
```

分支侧出口路由器公网口配置：

```
 nat server protocol udp global 22.22.22.1 4500 inside 192.168.2.1 4500
 nat server protocol udp global 22.22.22.1 500 inside 192.168.2.1 500
 nat server protocol 50 global 22.22.22.1 inside 192.168.2.1
 nat server protocol 51 global 22.22.22.1 inside 192.168.2.1
```

（3）防火墙配置，需要注意，防火墙基本的安全域需要配置通：

总部防火墙：

```
 acl advanced 3000
  rule 0 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.4.0 0.0.0.255
#
ipsec transform-set 1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 local-address 192.168.1.1          //本端地址需要写防火墙接口私网地址
 remote-address 22.22.22.1          //对端地址需要写为分支出口地址
 ike-profile 1
#
```

```
ike profile 1
 keychain 1
 match remote identity address 22.22.22.1 255.255.255.255        //对端地址需要写为分支出口地址
#
ike keychain 1
 pre-shared-key address 22.22.22.1 255.255.255.255 key simple 123456        //对端地址需要写为分支出口地址
#
分支侧防火墙：
acl advanced 3000
 rule 0 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
#
ipsec transform-set 1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 local-address 192.168.2.1              //本端地址需要写防火墙接口私网地址
 remote-address 11.11.11.1              //对端地址需要写为总部出口地址
 ike-profile 1
#
ike profile 1
 keychain 1
 match remote identity address 11.11.11.1 255.255.255.255              //对端地址需要写为总部出口地址
#
ike keychain 1
 pre-shared-key address 11.11.11.1 255.255.255.255 key simple 123456              //对端地址需要写为总部出口地址
```

配置关键点