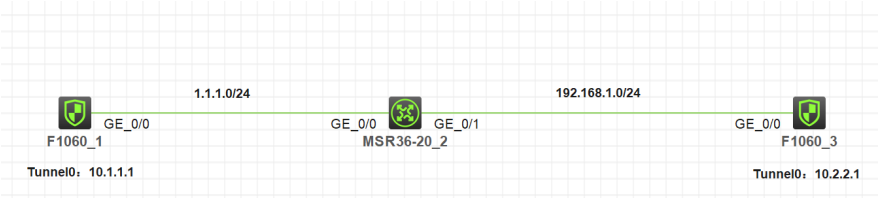
IPSec VPN主模式NAT穿越（涉及DNAT）

IPSec VPN　孔凡安　2021-11-04 发表

组网及说明



注：如无特别说明，描述中的 FW1 或 MSR1 对应拓扑中设备名称末尾数字为 1 的设备，FW2 或 MSR2 对应拓扑中设备名称末尾数字为 2 的设备，以此类推；另外，同一网段中，IP 地址的主机位为其设备编号，如 FW1 的 g0/0 接口若在 1.1.1.0/24 网段，则其 IP 地址为 1.1.1.1/24，以此类推

****

实验需求:

1.MSR2接口作nat server 映射内网地址10.2.2.1.

2.FW1和FW3建立IPsec隧道,涉及nat穿越.

3.不涉及安全域和安全策略

配置步骤

主要配置:

FW1:

```
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.1 255.255.255.0
 ipsec apply policy ply
#
 ip route-static 10.2.2.0 24 1.1.1.2
#
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.2.0 0.0.0.255
#
ipsec transform-set ts
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm md5
#
ipsec policy ply 1 isakmp
 transform-set ts
 security acl 3000
 local-address 1.1.1.1
 remote-address 1.1.1.2
 ike-profile pf
#
ike profile pf
 keychain key
 local-identity address 1.1.1.1
 match remote identity address 1.1.1.2 255.255.255.255
 proposal 1
#
ike proposal 1
#
ike keychain key
 pre-shared-key address 1.1.1.2 255.255.255.255 key cipher $c$3$7tR4Xas8kMaW0BNkLtmL6SYAz
YgdWUGDxw==
```

MSR2:

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.2 255.255.255.0
 nat server global 1.1.1.2 inside 192.168.1.3
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 192.168.1.2 255.255.255.0
```

FW3:

```
#
interface LoopBack0
 ip address 10.2.2.1 255.255.255.0
#
```

```
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address 192.168.1.3 255.255.255.0
 ipsec apply policy pay
#
 ip route-static 1.1.1.0 24 192.168.1.2
 ip route-static 10.1.1.0 24 192.168.1.2
```

配置关键点

触发需要公网一侧，因为内网测无法找到对端.