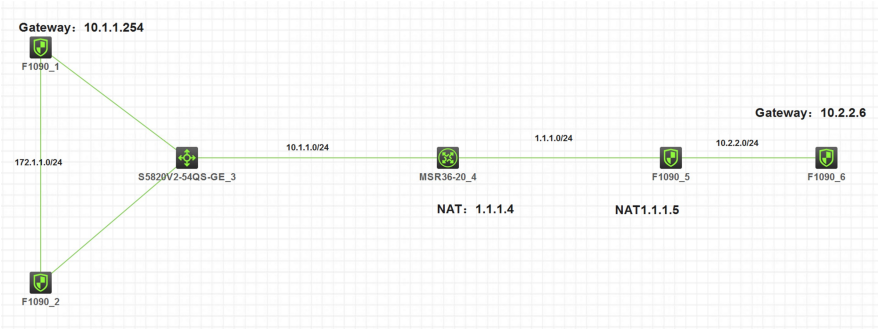
高可靠性组网下建立IKEv2的IPsec隧道（双向NAT场景）

IPSec VPN VRRP NAT 孔凡安 2022-03-04 发表

组网及说明



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 g1/0/0 接口若在 10.1.1.0/24 网段，则其 IP 地址为 10.1.1.1/24，以此类推

需求：

1.FW1和FW2使用RBM+VRRP的组网方式，和对端FW6建立IKEv2的IPsec隧道。

2.主链路故障时，RBM-S可以继续建立隧道。

3.涉及双向的NAT穿越，MSR4和FW5模拟公网区域，其中FW5上对FW6私网地址10.2.2.6做了映射。

配置步骤

1. RBM和VRRP的配置，略。可参考官网典配。

2.IP地址、路由、安全域、安全策略：略。需要使FW1、FW2以及FW6上有去往公网的路由.

3.IKEv2以及IPsec部分的配置

<table>
<tr><td>IKEv2 Keychain</td><td>
<table>
<tr><th>本端</th><th>对端</th></tr>
<tr><td>ikev2 keychain key
 peer FW6
  address 1.1.1.5 255.255.255.255
  identity address 10.2.2.6
  pre-shared-key ciphertext c3$lbDzJNN8lrjou3UKPGIHfhdum/VU4iCUlw==</td><td>ikev2 keychain key
 peer FW1
  address 1.1.1.4 255.255.255.255
  identity address 10.1.1.254
  pre-shared-key ciphertext c3$metIl3uckFXpsF+njYLyGZIjrMlw9YCSmA==</td></tr>
</table>
</td></tr>
<tr><td>IKEv2 Profile</td><td>
<table>
<tr><th>本端</th><th>对端</th></tr>
<tr><td>ikev2 profile pf
 authentication-method local pre-share
 authentication-method remote pre-share
 keychain key
 dpd interval 10 on-demand
 identity local address 10.1.1.254
 match remote identity address 10.2.2.6 255.255.255.255</td><td>ikev2 profile pf
 authentication-method local pre-share
 authentication-method remote pre-share
 keychain key
 dpd interval 10 on-demand
 identity local address 10.2.2.6
 match remote identity address 10.1.1.254 255.255.255.255</td></tr>
</table>
</td></tr>
<tr><td>IPsec Transform</td><td>ipsec transform-set ts
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1</td></tr>
<tr><td>IPsec Policy</td><td>
<table>
<tr><th>本端</th><th>对端</th></tr>
<tr><td>ipsec policy ply 1 isakmp
 transform-set ts
 security acl 3000
 local-address 10.1.1.254
 remote-address 1.1.1.5
 ikev2-profile pf</td><td>ipsec policy ply 1 isakmp
 transform-set ts
 security acl 3000
 local-address 10.2.2.6
 remote-address 1.1.1.4
 ikev2-profile pf</td></tr>
</table>
</td></tr>
<tr><td>接口下应用IPsec策略</td><td>
<table>
<tr><th>本端</th><th>对端</th></tr>
<tr><td>interface GigabitEthernet1/0/0
 ipsec apply policy ply</td><td>interface GigabitEthernet1/0/0
 ipsec apply policy ply</td></tr>
</table>
</td></tr>
</table>

配置关键点

1.RBM路由无法实现同步，需要分别在RBM_P和RBM_S设备上写各自的默认路由。

2.FW5需要映射500以及4500端口。

3. IKEv2 Profile下指定local ID写VRRP的虚地址，不写的话默认以接口地址作为local ID。