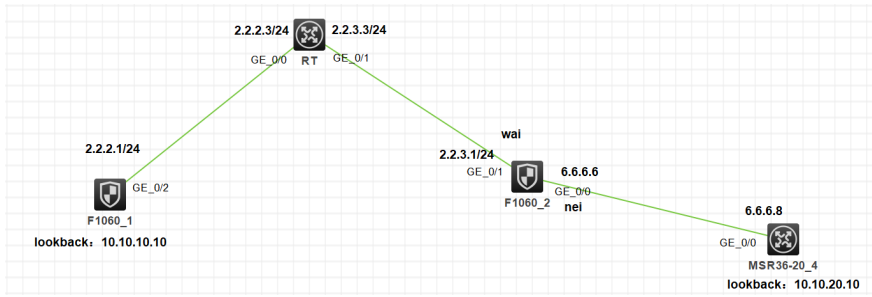知 防火墙做跨VPN实例的IPSEC在野蛮模式下的配置

IPSec VPN   孔梦龙   2022-11-11 发表

组网及说明

组网如下：

左边的配置：

ipsec transform-set 55
 esp encryption-algorithm des-cbc esp
authentication-algorithm sha1
#
ipsec policy kml 1 isakmp
 transform-set 55
 security acl 3555
 local-address 2.2.2.1
 remote-address 2.2.3.1
 ike-profile 55
 #
 ike identity fqdn kkk
#
ike profile 55
 keychain 55
 exchange-mode aggressive
 local-identity fqdn kkk
 match remote identity fqdn mmm
 proposal 5
#
ike proposal 5
 encryption-algorithm aes-cbc-192
 authentication-algorithm sha384
#
ike keychain 55
 pre-shared-key address 2.2.3.1 255.255.255.255 key cipher c3$i7oakHB51RdWFJEoTaWMSHRp
DD94mw==
#
acl advanced 3555 rule 5 permit ip source 10.10.10.10 0 destination 10.10.20.10 0
#
interface GigabitEthernet1/0/2
 port link-mode route combo enable copper
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy kml
#

总部的配置：
#
 interface GigabitEthernet1/0/0
 port link-mode route combo enable copper
 ip binding vpn-instance nei
 ip address 6.6.6.6 255.255.255.0
#
 interface GigabitEthernet1/0/1
 port link-mode route combo enable copper
 ip binding vpn-instance wai
 ip address 2.2.3.1 255.255.255.0
 ipsec apply policy kml
#

#
ipsec transform-set 55
 esp encryption-algorithm des-cbc esp
authentication-algorithm sha1
#
 ipsec policy-template kml 1
 transform-set 55
 local-address 2.2.3.1

```
  ike-profile 55
#
  ipsec policy kml 1 isakmp template kml
```

```
#
  ike profile 55
  keychain 55
  exchange-mode aggressive
  local-identity fqdn mmm
  match remote identity fqdn kkk
  proposal 5 inside-vpn vpn-instance nei
#
ike proposal 5
  encryption-algorithm aes-cbc-192
  authentication-algorithm sha384
#
  ike keychain 55 vpn-instance wai
  pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$0DWxPGR1yV9RUjYQcLmQJAe1MFm4yw
==
#
 #
  ip route-static vpn-instance nei 10.10.10.10 32 vpn-instance wai 2.2.3.3
  ip route-static vpn-instance nei 10.10.20.10 32 6.6.6.8
  ip route-static vpn-instance wai 2.2.2.1 32 2.2.3.3
#
acl advanced 3555
  rule 0 permit ip vpn-instance nei source 10.10.20.10 0 destination 10.10.10.10 0
 #
```