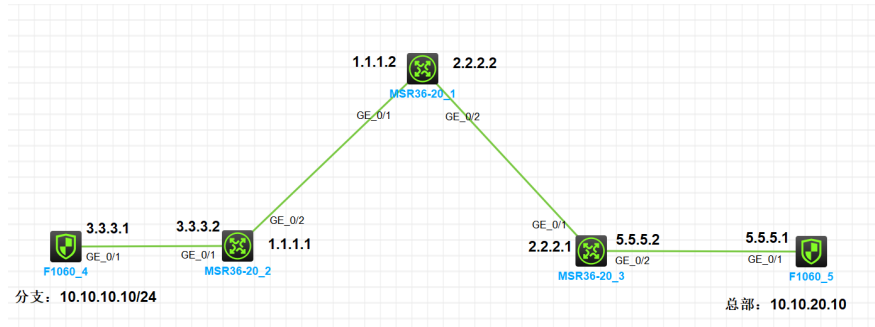


知 安全防火墙V7 ikev2 IPSEC 双NAT穿越案例

IPSec VPN 孔梦龙 2023-04-19 发表

组网及说明

分支使用3.3.3.1封装，然后SNAT的地址是1.1.1.1，做的静态NAT；总部使用5.5.5.1封装，然后SNAT的地址是2.2.2.1，做的静态NAT；



配置步骤

分支的配置:

```
#
interface LoopBack0
ip address 10.10.10.10 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 3.3.3.1 255.255.255.0
ipsec apply policy kml
#
security-zone name Local
#
ip route-static 0.0.0.0 0 3.3.3.2
#
acl advanced 3555
rule 0 permit ip source 10.10.10.10 0 destination 10.10.20.10 0
#
domain system
#
user-group system
#
ipsec transform-set 1
esp encryption-algorithm aes-cbc-128
esp authentication-algorithm sha1
#
ipsec policy kml 1 isakmp
transform-set 1
security acl 3555
local-address 3.3.3.1
remote-address 2.2.2.1
ikev2-profile profile1
#
ip http enable
ip https enable
#
ikev2 keychain keychain1
peer peer1
address 2.2.2.1 255.255.255.255
identity address 2.2.2.1
pre-shared-key ciphertext $c$3$RnjWJmcZYfFN4ib5DQM/rA29MhiNkA==
#
ikev2 profile profile1
authentication-method local pre-share
authentication-method remote pre-share
keychain keychain1
identity local fqdn fenzhi
match remote identity fqdn zongbu
#
ikev2 proposal proposal1
encryption aes-cbc-256
integrity md5
dh group1
#
ikev2 policy policy1
proposal proposal1
match local address 3.3.3.1
#
```

```
security-policy ip
rule 0 name 00
```

```
action pass
```

```
#
```

```
配置关键点
```

```
穿越需要使用静态NAT
```

```
总部配置：
```

```
#
```

```
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 5.5.5.1 255.255.255.0
ipsec apply policy kml
```

```
#
```

```
ip route-static 0.0.0.0 0 5.5.5.2
```

```
#
```

```
info-center loghost 127.0.0.1 port 3301 format default
info-center source CFGLOG loghost level informational
```

```
#
```

```
acl advanced 3555
rule 0 permit ip source 10.10.20.10 0 destination 10.10.10.10 0
```

```
#
```

```
#
```

```
user-group system
```

```
#
```

```
ipsec transform-set 1
esp encryption-algorithm aes-cbc-128
esp authentication-algorithm sha1
```

```
#
```

```
ipsec policy kml 1 isakmp
transform-set 1
security acl 3555
local-address 5.5.5.1
remote-address 1.1.1.1
ikev2-profile profile1
```

```
#
```

```
ip http enable
ip https enable
```

```
#
```

```
ikev2 keychain keychain1
peer peer1
address 1.1.1.1 255.255.255.0
identity address 1.1.1.1
pre-shared-key ciphertext $c$3$LTtjoYHD+e3LiqPjg+a7FBYy2XNmI==
```

```
#
```

```
ikev2 profile profile1
authentication-method local pre-share
authentication-method remote pre-share
keychain keychain1
identity local fqdn zongbu
match remote identity fqdn fenzhi
```

```
#
```

```
ikev2 proposal proposal1
encryption aes-cbc-256
integrity md5
dh group1
```

```
#
```

```
ikev2 policy policy1
proposal proposal1
match local address 5.5.5.1
```

```
#
```

```
security-policy ip
rule 0 name 00
```

action pass

#

return