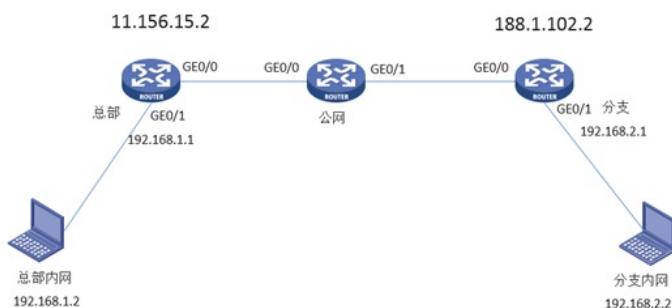


ipsec vpn隐藏两边真实ip地址典型配置举例

IPSec VPN 孙兆强 2022-05-31 发表

组网及说明



分支与总部建立ipsec，因为安全要求，两边需要隐藏真实ip地址。地址对应关系如下：

192.168.1.2-----11.156.15.2

192.168.2.2-----188.1.102.2

配置步骤

总部配置

```
interface GigabitEthernet0/0
port link-mode route
combo enable copper
ip address 172.168.1.1 255.255.255.0
nat outbound 3002
nat static enable
ipsec apply policy 1
#
interface GigabitEthernet0/1
port link-mode route
combo enable copper
ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0 172.168.1.2
#
acl advanced 3000
rule 0 permit ip source 11.156.15.0 0.0.0.255 destination 188.1.102.0 0.0.0.255
#
acl advanced 3001
rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 188.1.102.0 0.0.0.255
#
acl advanced 3002
rule 0 deny ip source 11.156.15.0 0.0.0.255 destination 188.1.102.0 0.0.0.255
rule 5 permit ip
#
ipsec transform-set 1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
#
ipsec policy 1 1 isakmp
transform-set 1
security acl 3000
local-address 172.168.1.1
remote-address 172.168.2.1
ike-profile 1
#
nat static outbound 192.168.1.2 11.156.15.2 acl 3001 reversible
#
ike profile 1
keychain 1
local-identity address 172.168.1.1
match remote identity address 172.168.2.1 255.255.255.255
match local address 172.168.1.1
proposal 1
#
ike proposal 1
encryption-algorithm 3des-cbc
authentication-algorithm md5
#
ike keychain 1
pre-shared-key address 172.168.2.1 255.255.255.255 key cipher $c$3$q2ZNr6l8Ppj147aKkeLLNDO
ofxOajA==
#
```

分支配置

```
interface GigabitEthernet0/0
port link-mode route
combo enable copper
ip address 172.168.2.1 255.255.255.0
```

```

nat static enable
ipsec apply policy 1
#
配置关键点
interface GigabitEthernet0/1
port流量进入路由器要做源地址转换，到达对端之后要做目的地址转换所以要用静态地址转换。因为要
    双向互通所以要加reversible参数。
ip address 192.168.2.1 255.255.255.0 1.102.2 acl 3001 reversible
# 因为用户还要上公网所以要在静态nat中加入acl限制只有访问对端的流量才进行静态nat的转换。
3p router static转发出去时处理顺序是先nat再进行ipsec，所以可以在公网完成源地址转换及ipsec封
# 装。流量进入则处理顺序相反。
acl advanced 3000
rule 0 permit ip source 188.1.102.0 0.0.0.255 destination 11.156.15.0 0.0.0.255
#
acl advanced 3001
rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 11.156.15.0 0.0.0.255
#
acl advanced 3002
rule 0 deny ip source 188.1.102.0 0.0.0.255 destination 11.156.15.0 0.0.0.255
rule 5 permit ip
#
ipsec transform-set 1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
#
ipsec policy 1 1 isakmp
transform-set 1
security acl 3000
local-address 172.168.2.1
remote-address 172.168.1.1
ike-profile 1
#
nat static outbound 192.168.2.2 188.1.102.2 acl 3001 reversible
#
ike profile 1
keychain 1
local-identity address 172.168.2.1
match remote identity address 172.168.1.1 255.255.255.255
match local address 172.168.2.1
proposal 1
#
ike proposal 1
encryption-algorithm 3des-cbc
authentication-algorithm md5
#
ike keychain 1
pre-shared-key address 172.168.1.1 255.255.255.255 key cipher $c$3$MWIDyiWv5ekIRKunSbCXO
0OgTDSX6w==
#
验证配置
从分支内网ping 11.156.15.2
在分支查看ike sa及ipsec sa
[fenzhi]dis ike sa
  Connection-ID  Remote          Flag      DOI
-----
  1        172.168.1.1    RD      IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[fenzhi]dis ipse s
[fenzhi]dis ipse sa
-----
Interface: GigabitEthernet0/0
-----

```

IPsec policy: 1
Sequence number: 1
Mode: ISAKMP