华为路由交换由浅入深系列（十一）-IPSEC VPN 互通 + 上网配置示例【包含基本 VPN+NAT+NAT 免俗】

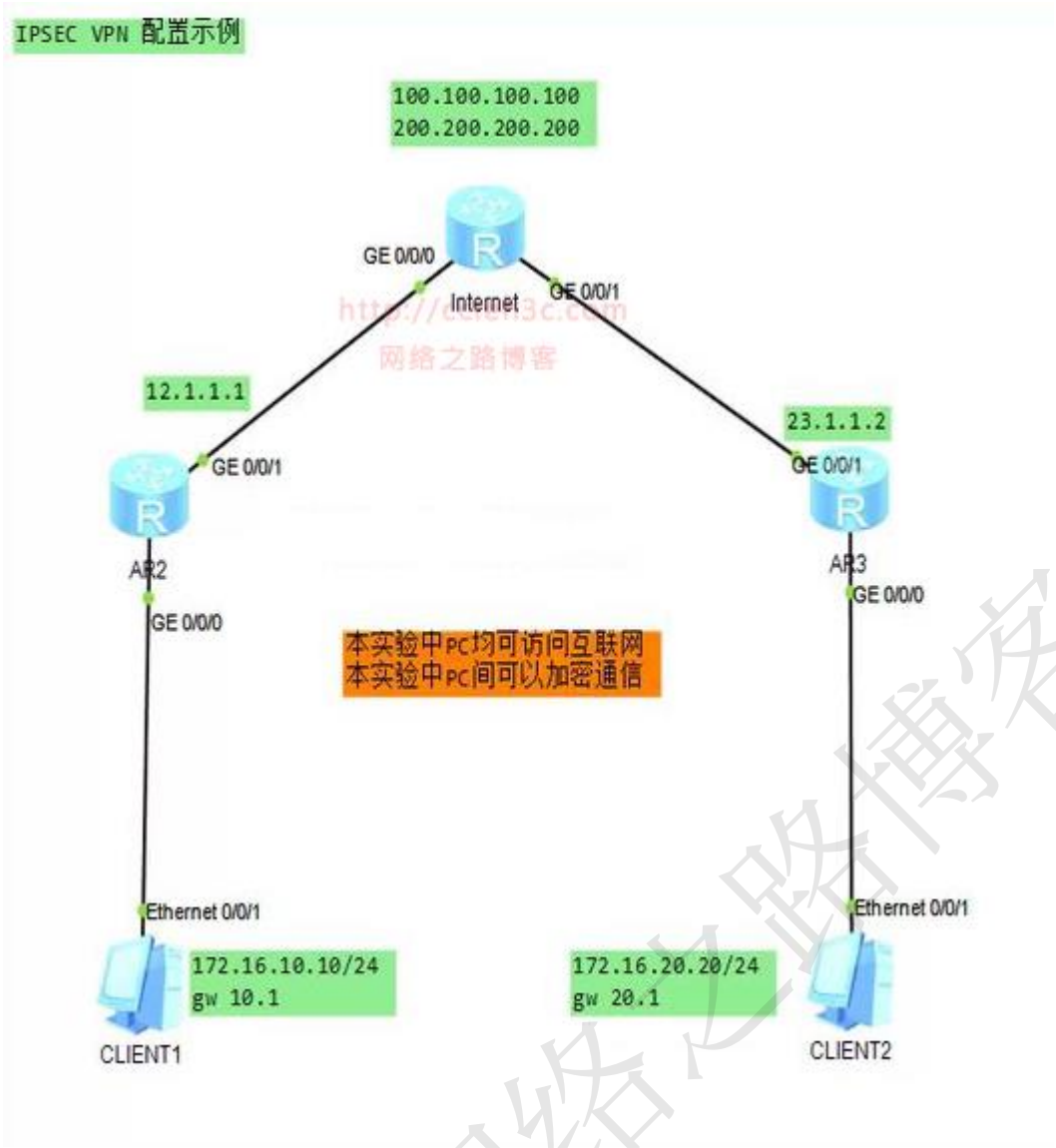
1 IPSEC VPN 互通 + 上网配置示例

2、实验目的

掌握 NAT 的配置

掌握 IPSEC VPN 的基础配置

3、实验拓扑



3、配置要点

总公司的配置

```
#
 sysname ZongGongSi
#
acl number 3000
```

```
 rule 5 deny ip source 172.16.10.0 0.0.0.255 destination 172.16.20.0 0.0.0.255
 rule 10 permit ip
acl number 3001
 rule 5 permit ip source 172.16.10.0 0.0.0.255 destination 172.16.20.0 0.0.0.255
#
ipsec proposal test
#
ike proposal 1
#
ike peer test v2
 pre-shared-key simple ccieh3c.taobao.com
 remote-address 23.1.1.2
#
ipsec policy test 10 isakmp
 security acl 3001
 ike-peer test
 proposal test
#
interface GigabitEthernet0/0/0
 ip address 172.16.10.1 255.255.255.0
#
```

```
interface GigabitEthernet0/0/1
 ip address 12.1.1.1 255.255.255.0
 ipsec policy test
 nat outbound 3000
#
ip route-static 0.0.0.0 0.0.0.0 12.1.1.2
#
```

分公司的配置

```
 sysname FenGongSi
#
acl number 3000
 rule 5 deny ip source 172.16.20.0 0.0.0.255 destination 172.16.10.0 0.0.0.255
 rule 10 permit ip
acl number 3001
 rule 5 permit ip source 172.16.20.0 0.0.0.255 destination 172.16.10.0 0.0.0.255
#
ipsec proposal test
#
ike peer test v2
```

```
 pre-shared-key simple ccieh3c.taobao.com
 remote-address 12.1.1.1
#
ipsec policy test 10 isakmp
 security acl 3001
 ike-peer test
 proposal test
#
interface GigabitEthernet0/0/0
 ip address 172.16.20.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 23.1.1.2 255.255.255.0
 ipsec policy test
 nat outbound 3000
#
ip route-static 0.0.0.0 0.0.0.0 23.1.1.1
#
```


互联网的配置

```
 #
 sysname Internet
#
interface GigabitEthernet0/0/0
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 23.1.1.1 255.255.255.0
#
interface LoopBack100
 ip address 100.100.100.100 255.255.255.0
#
interface LoopBack200
 ip address 200.200.200.200 255.255.255.0
#
```


四、互通测试

主机上 ping 分支 上网

```
PC>ping 172.16.20.20

Ping 172.16.20.20: 32 data bytes, Press Ctrl_C to break
From 172.16.20.20: bytes=32 seq=1 ttl=127 time=47 ms
From 172.16.20.20: bytes=32 seq=2 ttl=127 time=47 ms
From 172.16.20.20: bytes=32 seq=3 ttl=127 time=31 ms
From 172.16.20.20: bytes=32 seq=4 ttl=127 time=16 ms
```

```
From 172.16.20.20: bytes=32 seq=5 ttl=127 time=31 ms

--- 172.16.20.20 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 16/34/47 ms

PC>ping 100.100.100.100

Ping 100.100.100.100: 32 data bytes, Press Ctrl_C to break
From 100.100.100.100: bytes=32 seq=1 ttl=254 time=31 ms
From 100.100.100.100: bytes=32 seq=2 ttl=254 time=15 ms
From 100.100.100.100: bytes=32 seq=3 ttl=254 time=31 ms
From 100.100.100.100: bytes=32 seq=4 ttl=254 time=47 ms
From 100.100.100.100: bytes=32 seq=5 ttl=254 time=47 ms

--- 100.100.100.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/34/47 ms
```

路由器上校验

```
<ZongGongSi>dis ike sa v2
  Conn-ID  Peer           VPN    Flag(s)             Phase
 -----------------------------------------------------------------
     3    23.1.1.2        0      RD                  2
     2    23.1.1.2        0      RD                  1

  Flag Description:
  RD--READY    ST--STAYALIVE    RL--REPLACED    FD--FADING    TO--TIMEOUT
  HRT--HEARTBEAT    LKG--LAST KNOWN GOOD SEQ NO.    BCK--BACKED UP

<ZongGongSi>dis ipsec sa brief

Number of SAs:2
  Src address     Dst address       SPI     VPN   Protocol     Algorithm
-------------------------------------------------------------------------------
    23.1.1.2        12.1.1.1 2433519709      0    ESP    E:DES A:MD5-96
```

```
12.1.1.1        23.1.1.2 2579144653       0     ESP    E:DES A:MD5-96
```

博主也只是业余时间写写技术文档，请大家见谅，大家觉得不错的话，可以推荐给朋友哦，博主会努力推出更好的系列文档的。如果大家有任何疑问或者文中有错误跟疏忽的地方，欢迎大家留言指出，博主看到后会第一时间修改，谢谢大家的支持，更多技术文章尽在网络之路博客，http://ccieh3c.com。