步骤2：静态路由的配置。可以使用动态路由代替

　　(1)路由R5的配置

　　ip route 0.0.0.0 0.0.0.0 100.1.1.2

　　(2)路由器R6的配置

　　ip route 10.1.1.0 255.255.255.0 100.1.1.1

　　ip route 10.1.2.0 255.255.255.0 200.1.1.2

　　(3)路由器R7的配置

　　ip route 0.0.0.0 0.0.0.0 200.1.1.1

　　(4)网络连通性测试

　　C1、C2能互通

　　步骤3：GRE VPN的配置

　　(1)路由R5的配置

　　//创建GRE隧道，指定封装后的源地址和目的地址

　　interface Tunnel0

　　ip address 192.168.1.2 255.255.255.252

　　tunnel source 100.1.1.1

　　tunnel destination 200.1.1.2

　　exit

　　//通过tunnel访问对端私网的路由

　　ip route 10.1.2.0 255.255.255.0 Tunnel0 //可以使用动态路由代替

　　配置关键点：

　　1)两端的隧道地址要处于同一网段;

　　2)不要忘记配置通过tunnel访问对方私网的路由。

　　(2)路由器R7的配置

　　interface Tunnel0

　　ip address 192.168.1.1 255.255.255.252

　　tunnel source 200.1.1.2

　　tunnel destination 100.1.1.1

　　exit

　　ip route 10.1.1.0 255.255.255.0 Tunnel0 //可以使用动态路由代替

　　(3)测试

R5#show int tunnel 0

　　Tunnel0 is up, line protocol is up

　　Hardware is Tunnel

　　Internet address is 192.168.1.2/30

　　MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,

　　reliability 255/255, txload 1/255, rxload 1/255

　　Encapsulation TUNNEL, loopback not set

　　Keepalive not set

　　Tunnel source 100.1.1.1, destination 200.1.1.2

　　Tunnel protocol/transport GRE/IP

　　Key disabled, sequencing disabled

　　Checksumming of packets disabled

　　Tunnel TTL 255

　　Fast tunneling enabled

　　Tunnel transmit bandwidth 8000 (kbps)

　　Tunnel receive bandwidth 8000 (kbps)

　　Last input 00:10:34, output 00:09:15, output hang never

　　Last clearing of "show interface" counters never

　　Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

　　Queueing strategy: fifo

　　Output queue: 0/0 (size/max)

　　5 minute input rate 0 bits/sec, 0 packets/sec

　　5 minute output rate 0 bits/sec, 0 packets/sec

　　117 packets input, 12742 bytes, 0 no buffer

　　Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

　　0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

　　91 packets output, 10843 bytes, 0 underruns

　　0 output errors, 0 collisions, 0 interface resets

　　0 output buffer failures, 0 output buffers swapped out

　　步骤4：IPSEC 的配置

　　(1)路由R5的配置

　　/IKE第一阶段需要核实远程对等体的身份，然后建立一个安全的已验证的通道进行通信。IKE第一阶段的协商有：采用加密和散列算法保护自身的技术、采用预共享/公钥加密/数字签名的验证方法、采用(Diffe-Hellman组)会话密钥生成参数。/IKE第一阶段协商后，建立一个双向的ISAKMP/IKE SA进行通信。

　　crypto isakmp policy 10 //定义IPSec策略，协商方式为isakmp，即使用IKE协商

　　authentication pre-share //采用预共享身份验证

　　exit

　　crypto isakmp key cisco123 address 200.1.1.2 //预设身份验证口令、对等体的IP地址。H3C产品对等体IP地址为TUNNEL接口地址。

　　crypto ipsec transform-set myset esp-des esp-sha-hmac //定义IPSec转换集myset(封装协议、加密算法、验证算法)

　　mode tunnel //定义隧道模式

　　exit

　　/IKE第2阶段可以保护用户数据并建立IPSEC的SA。IKE第2阶段的协商有：采用ESP/AH保护套(封装协议)、保护套的算法(采用DES、3DES、AES、SHA)、正在受保护的网络或IP流量、协商协议的可选密钥材料。IKE第2阶段协商结束后，IKE建立两个单向IPSEC SA，用于用户数据处理(一个发送用户数据、另一个接收加密数据)。

　　crypto map mymap 10 ipsec-isakmp //定义加密图mymap、IPSEC协商

　　set peer 200.1.1.2 //选择使用的IKE对等体。H3C对等体IP为TUNNEL接口地址。

　　set transform-set myset //将转换集应用到加密图中

　　match address 100 //需要加密传送的ACL

　　exit

　　access-list 100 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255 //定义需要加密传送的ACL

　　interface Tunnel0 //蒋IPSec策略绑定到GRE隧道

　　crypto map mymap

　　exit

　　(2)路由器R7的配置

　　crypto isakmp policy 10

　　authentication pre-share

　　exit

　　crypto isakmp key cisco123 address 100.1.1.1

　　crypto ipsec transform-set myset esp-des esp-sha-hmac

　　mode tunnel

　　exit

　　crypto map mymap 10 ipsec-isakmp

　　set peer 100.1.1.1

　　set transform-set myset

　　match address 100

　　exit

　　access-list 100 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255

　　interface Tunnel0

　　crypto map mymap

　　exit

　　配置关键点：

　　(1) 和基本IPSec配置较为相似;

　　(2)H3C设备配置，IKE Peer的Remote address是对方的GRE隧道口IP地址，不是物理接口地址;

　　(3) IPSec策略绑定到GRE隧道上;

　    (4) 定义静态路由或策略路由将需要加密的流量引入到GRE隧道上。

　　(3)测试

R5#show crypto isakmp sa

　　dst src state conn-id slot status

　　100.1.1.1 200.1.1.2 QM\_IDLE 1 0 ACTIVE

　　R5#show crypto ipsec sa

　　interface: Tunnel0

　　Crypto map tag: mymap, local addr 100.1.1.1

　　protected vrf: (none)

　　local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

　　remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)

　　current\_peer 200.1.1.2 port 500

　　PERMIT, flags={origin\_is\_acl,}

　　#pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 18

　　#pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18

　　#pkts compressed: 0, #pkts decompressed: 0

　　#pkts not compressed: 0, #pkts compr. failed: 0

　　#pkts not decompressed: 0, #pkts decompress failed: 0

　　#send errors 0, #recv errors 0

　　local crypto endpt.: 100.1.1.1, remote crypto endpt.: 200.1.1.2

　　path mtu 1476, ip mtu 1476, ip mtu idb Tunnel0

　　current outbound spi: 0xF993D0F9(4187214073)

　　inbound esp sas:

　　spi: 0xCC4B30B9(3427479737)

　　transform: esp-des esp-sha-hmac ,

　　in use settings ={Tunnel, }

　　conn id: 2001, flow\_id: SW:1, crypto map: mymap

　　sa timing: remaining key lifetime (k/sec): (4606609/2980)

　　IV size: 8 bytes

　　replay detection support: Y

　　Status: ACTIVE

　　inbound ah sas:

　　inbound pcp sas:

　　outbound esp sas:

　　spi: 0xF993D0F9(4187214073)

　　transform: esp-des esp-sha-hmac ,

　　in use settings ={Tunnel, }

　　conn id: 2002, flow\_id: SW:2, crypto map: mymap

　　sa timing: remaining key lifetime (k/sec): (4606609/2979)

　　IV size: 8 bytes

　　replay detection support: Y

　　Status: ACTIVE

　　outbound ah sas:

　　outbound pcp sas:

　　四、路由器的相关配置文件

　　R5#show run

　　Building configuration...

　　!

　　hostname r1

　　!

　　crypto isakmp policy 10

　　authentication pre-share

　　crypto isakmp key cisco123 address 200.1.1.2

　　!

　　!

　　crypto ipsec transform-set myset esp-des esp-sha-hmac

　　!

　　crypto map mymap 10 ipsec-isakmp

　　set peer 200.1.1.2

　　set transform-set myset

　　match address 100

　　!

　　interface Tunnel0

　　ip address 192.168.1.2 255.255.255.252

　　tunnel source 100.1.1.1

　　tunnel destination 200.1.1.2

　　crypto map mymap

　　!

　　interface Serial0/0

　　ip address 100.1.1.1 255.255.255.252

　　serial restart-delay 0

　　!

　　interface FastEthernet1/0

　　ip address 10.1.1.1 255.255.255.0

　　duplex auto

　　speed auto

　　!

　　ip route 0.0.0.0 0.0.0.0 100.1.1.2

　　ip route 10.1.2.0 255.255.255.0 Tunnel0

　　!

　　!

　　access-list 100 permit ip 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255

　　!

　　R6#show run

　　Building configuration...

　　hostname r2

　　!

　　interface Serial0/0

　　ip address 100.1.1.2 255.255.255.252

　　serial restart-delay 0

　　!

　　interface Serial0/1

　　ip address 200.1.1.1 255.255.255.252

　　serial restart-delay 0

　　!

　　!

　　ip route 10.1.1.0 255.255.255.0 100.1.1.1

　　ip route 10.1.2.0 255.255.255.0 200.1.1.2

　　!

　　R7#show run

　　Building configuration...

　　hostname r3

　　!

　　!

　　crypto isakmp policy 10

　　authentication pre-share

　　crypto isakmp key cisco123 address 100.1.1.1

　　!

　　!

　　crypto ipsec transform-set myset esp-des esp-sha-hmac

　　!

　　crypto map mymap 10 ipsec-isakmp

　　set peer 100.1.1.1

　　set transform-set myset

　　match address 100

　　!

　　interface Tunnel0

　　ip address 192.168.1.1 255.255.255.252

　　tunnel source 200.1.1.2

　　tunnel destination 100.1.1.1

　　crypto map mymap

　　!

　　interface Serial0/0

　　ip address 200.1.1.2 255.255.255.252

　　serial restart-delay 0

　　!

　　interface FastEthernet1/0

　　ip address 10.1.2.1 255.255.255.0

　　duplex auto

　　speed auto

　　!

　　ip route 0.0.0.0 0.0.0.0 200.1.1.1

　　ip route 10.1.1.0 255.255.255.0 Tunnel0

　　!

　　access-list 100 permit ip 10.1.2.0 0.0.0.255 10.1.1.0 0.0.0.255

　　!