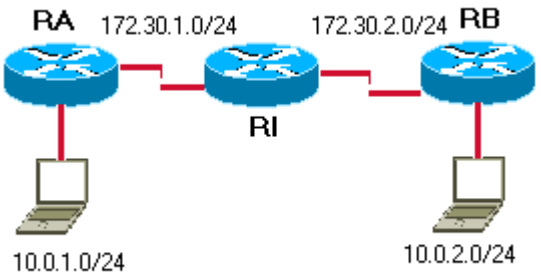
Cấu hình VPN cơ bản

Cấu hình VPN cơ bản

Tác giả Lê Anh Đức

Mô tả: Bài lab thực hiện cấu hình hai router , tạo một kênh private giữa hai mạng LAN của 2 router qua một môi trường public.



Ta thấy qua topo trên, một công ty gồm 2 chi nhánh , muốn tạo một kết nối private qua một môi trường truyền public ta sử dụng VPN để thực hiện nhiệm
vụ này, ta tạo một kênh riêng giữa 2 router: RA, RB, qua môi trường internet với RI là ISP. Bất cứ traffic TCP nào từ 10.0.1.0/24 đến 10.0.2.0/24 đều sẽ được
mã hoá và gửi ra môi trường public.

Cấu hình

RA

Building configuration...

Current configuration : 945 bytes

!

version 12.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname RA

!

!

memory-size iomem 10

ip subnet-zero

!

!

!

!

crypto isakmp policy 100 ← **tạo IKE pha 1**

 hash md5

 authentication pre-share

crypto isakmp key cisco address 172.30.2.2

!

!

crypto ipsec transform-set mine esp-des ← **Cấu hình IPSec**

!

crypto map lee 10 ipsec-isakmp ←**Tạo crypto map**

 set peer 172.30.2.2

```
 set transform-set mine
 match address 110
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
 ip address 10.0.1.1 255.255.255.0
```

half-duplex

!

interface Serial0/0

ip address 172.30.1.2 255.255.255.0

no fair-queue

crypto map lee ← **gắn crypto map vào interface**

!

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0 ← **tạo default gateway ra internet**

ip http server

!

!

access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255 ← **Tạo ACL để xác định traffic được mã hoá**

!

call rsvp-sync

!

!

mgcp profile default

!

dial-peer cor custom

!

!

!

!

!

line con 0

line aux 0

line vty 0 4

!

!

end

RB

Building configuration...

*Mar 1 00:39:18.794: %SYS-5-CONFIG_I: Configured from console by console

Current configuration : 962 bytes

!

version 12.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname RB

```
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
crypto isakmp policy 100
 hash md5
 authentication pre-share
crypto isakmp key cisco address 172.30.1.2
!
!
crypto ipsec transform-set mine esp-des
!
crypto map lee 10 ipsec-isakmp
 set peer 172.30.1.2
 set transform-set mine
 match address 100
!
!
```

```
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
!
!
!
interface Ethernet0/0
 ip address 10.0.2.1 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 172.30.2.2 255.255.255.0
```

```
 no fair-queue
 clockrate 64000
 crypto map lee
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip http server
!
!
access-list 100 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
```

line con 0

line aux 0

line vty 0 4

!

!

end

RI

Building configuration...

Current configuration:

!

version 12.1

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname RI

!

!

!

!

!

!

memory-size iomem 10

ip subnet-zero

!

!

!

!

interface Ethernet0/0

 no ip address

 shutdown

!

interface Serial0/0

 ip address 172.30.1.1 255.255.255.0

 no fair-queue

 clockrate 64000

!

interface Serial0/1

 ip address 172.30.2.1 255.255.255.0

!

ip classless

ip route 10.0.1.0 255.255.255.0 Serial0/0 **← sử dụng static route**

```
ip route 10.0.2.0 255.255.255.0 Serial0/1

no ip http server

!

!

line con 0

 transport input none

line aux 0

line vty 0 4

!

no scheduler allocate

end
```

Thực hiện

Sau khi đã cấu hình cho các router thấy được nhau(sử dụng default route kết hợp với static routing) ta bước qua cấu hình VPN.

Các bước cấu hình VPN gồm những bước sau:

B1: Cấu hình IKE

- Bật IKE(nếu đã bị tắt thì bật lại, mặc định trên router là đã được bật):

  Router(config)# crypto isakmp enable

- Tạo IKE policy:

  Router(config)# crypto isakmp policy priority

- Tạo các IKE policy ở mode config-isakmp: (authentication, encryption, hash,…)

B2: Cấu hình IPSec

- Cấu hình transform-set: tạo transform set giúp ta áp các chính sách bảo mật cho traffic, có thể có 3 transform trong một set, mỗi set được giới hạn: 1AH và 2ESP. Mode mặc định cho transform là tunnel.

  Router(config)# crypto ipsec transform-set name [trans1 [trans2[trans3]]]

  Router(cfg-crypto-trans)#

- Tạo crypto ACL: thực hiện các chức năng sau: xác định các dòng dữ liệu được bảo vệ bởi IPSec, chọn outbound traffic được bảo vệ,…

  + Tạo ACL để xác định loại traffic cần được bảo vệ

  +Tạo crypto map

  Router(config)# crypto map name seq ipsec-manual| ipsec-iaskmp

  ➔sử dụng các sequence no khác nhau cho mỗi peer, nhiều peer có thể được xác định trong cùng một crypto map.

  + Áp crypto map vào interface

Router RA

RA(config)#crypto isakmp enable ←Bật crypto isakmp

RA(config)#crypto isakmp policy 100

RA(config-isakmp)#hash md5

RA(config-isakmp)#authentication pre-share ←xác định các phương pháp xác minh

RA(config-isakmp)#exit

RA(config)#crypto isakmp identity address ←xác định cách xác định peer qua địc chỉ chứ không phải qua hostname

RA(config)#crypto isakmp key cisco address 172.30.2.2 ←xác định key

cho preshare key của peer

RA(config)#crypto ipsec transform-set mine esp-des ←xác định giải thuật mã hoá là esp-des cho transform-set tên mine

RA(cfg-crypto-trans)#exit

RA(config)#crypto map lee 10 ipsec-isakmp ←tạo crypto map tên lee

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

RA(config-crypto-map)#set peer 172.30.2.2 ←xác định peer là interface bên kia

RRA(config-crypto-map)#set transform-set mine ← áp transform set mine vào crypto map lee

RA(config-crypto-map)#match address 110 ←xác định ACL

RA(config-crypto-map)#exit

RA(config)#access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255←tạo ACL để xác định traffic được mã hoá

RA(config)#int s0/0

RA(config-if)#crypto map lee ←áp cryto map lee vào interface S0/0

Router RB: cấu hình tương tự như RA:

RB(config)#crypto isakmp enable

RB(config)#crypto isakmp policy 100

RB(config-isakmp)#hash md5

RB(config-isakmp)#authentication pre-share

```
RB(config-isakmp)#exit

RB(config)#crypto isakmp identity address

RB(config)#crypto isakmp key cisco address 172.30.1.2

RB(config)#crypto ipsec transform-set mine esp-des

RB(cfg-crypto-trans)#exit

RB(config)#crypto map lee 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

    and a valid access list have been configured.

RB(config-crypto-map)#set peer 172.30.1.2

RB(config-crypto-map)#set transform-set mine

RB(config-crypto-map)#match address 100

RB(config-crypto-map)#exit

RB(config)#access-list 100 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255

RB(config)#int s0/0

RB(config-if)#crypto map lee
```

- **Chú ý:** các giải thuật mã hoá và các phương pháp xác minh phải được đồng bộ giữa 2 bên.

Kiểm tra:

Ta sử dụng các lệnh show và debug để kiểm tra: ý tưởng: bật telnet service
trên hai pc cám vào 2 LAN ở 2 đầu và telnet qua lại, ghi nhận debug trên 2 router:

Ví dụ:

Trên RA:

RA#sh crypto map

Crypto Map "lee" 10 ipsec-isakmp

Peer = 172.30.2.2

Extended IP access list 110

access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255

Current peer: 172.30.2.2

Security association lifetime: 4608000 kilobytes/3600 seconds

PFS (Y/N): N

Transform sets={ mine, }

Interfaces using crypto map lee:

Serial0/0

RA#sh crypto isakmp policy

Protection suite of priority 100

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Message Digest 5

authentication method: Pre-Shared Key

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

Default protection suite

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Rivest-Shamir-Adleman Signature

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

RA#sh crypto ipsec transform-set

Transform set mine: { esp-des }

will negotiate = { Tunnel, },

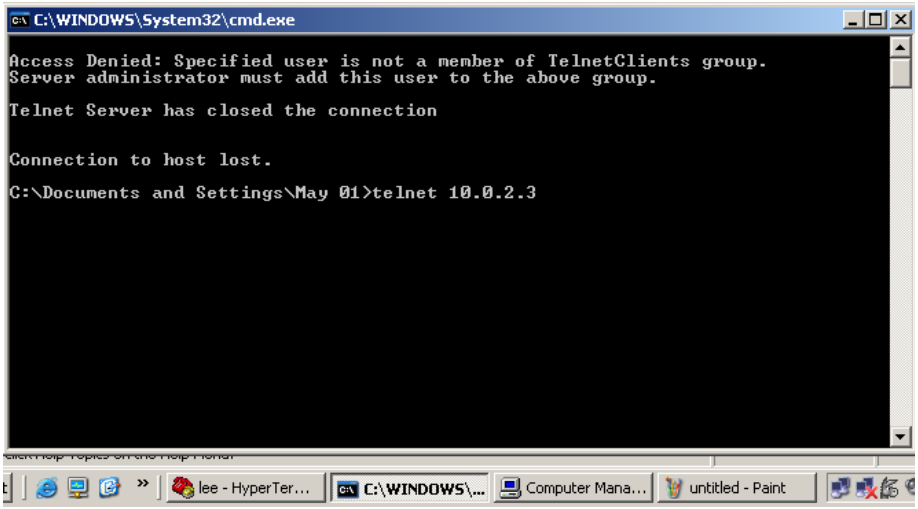
RA#debug crypto ipsec

Crypto IPSEC debugging is on

RA#debug crypto isakmp

Crypto ISAKMP debugging is on

Telnet trên pc1:



Và xem debug trên RA:

RA#

*Mar 1 00:49:32.924: IPSEC(sa_request): ,

  (key eng. msg.) OUTBOUND local= 172.30.1.2, remote= 172.30.2.2,

    local_proxy= 10.0.1.0/255.255.255.0/6/0 (type=4),

    remote_proxy= 10.0.2.0/255.255.255.0/6/0 (type=4),

    protocol= ESP, transform= esp-des ,

    lifedur= 3600s and 4608000kb,

    spi= 0x9B717872(2607904882), conn_id= 0, keysize= 0, flags= 0x400C

*Mar 1 00:49:32.924: ISAKMP: received ke message (1/1)

*Mar 1 00:49:32.924: ISAKMP: local port 500, remote port 500

*Mar 1 00:49:32.928: ISAKMP (0:1): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM

*Mar 1 00:49:32.928: ISAKMP (0:1): Old State = IKE_READY New State = IKE_I_MM1

*Mar 1 00:49:32.928: ISAKMP (0:1): beginning Main Mode exchange

*Mar 1 00:49:32.928: ISAKMP (0:1): sending packet to 172.30.2.2 (I) MM_NO_STATE

*Mar 1 00:49:33.173: ISAKMP (0:1): received packet from 172.30.2.2 (I) MM_NO_STATE

*Mar 1 00:49:33.177: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar 1 00:49:33.177: ISAKMP (0:1): Old State = IKE_I_MM1 New State = IKE_I_MM2

*Mar 1 00:49:33.177: ISAKMP (0:1): processing SA payload. message ID = 0

*Mar 1 00:49:33.177: ISAKMP (0:1): found peer pre-shared key matching 172.30.2.2

*Mar 1 00:49:33.177: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 100 policy

*Mar 1 00:49:33.181: ISAKMP: encryption DES-CBC

*Mar 1 00:49:33.181: ISAKMP: hash MD5

*Mar 1 00:49:33.181: ISAKMP: default group 1

*Mar 1 00:49:33.181: ISAKMP: auth pre-share

*Mar 1 00:49:33.181: ISAKMP: life type in seconds

*Mar 1 00:49:33.181: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80

*Mar 1 00:49:33.181: ISAKMP (0:1): atts are acceptable. Next payload is 0

*Mar 1 00:49:33.353: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar 1 00:49:33.353: ISAKMP (0:1): Old State = IKE_I_MM2 New State = IKE_I_MM2

*Mar 1 00:49:33.357: ISAKMP (0:1): sending packet to 172.30.2.2 (I) MM_SA_SETUP

*Mar 1 00:49:33.357: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar 1 00:49:33.357: ISAKMP (0:1): Old State = IKE_I_MM2 New State = IKE_I_MM3

*Mar 1 00:49:33.714: ISAKMP (0:1): received packet from 172.30.2.2 (I) MM_SA_SETUP

*Mar 1 00:49:33.714: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar 1 00:49:33.714: ISAKMP (0:1): Old State = IKE_I_MM3 New State = IKE_I_MM4

*Mar 1 00:49:33.718: ISAKMP (0:1): processing KE payload. message ID = 0

*Mar 1 00:49:33.926: ISAKMP (0:1): processing NONCE payload. message ID = 0

*Mar 1 00:49:33.926: ISAKMP (0:1): found peer pre-shared key matching 172.30.2.2

*Mar 1 00:49:33.930: ISAKMP (0:1): SKEYID state generated

*Mar 1 00:49:33.930: ISAKMP (0:1): processing vendor id payload

*Mar 1 00:49:33.930: ISAKMP (0:1): vendor ID is Unity

*Mar 1 00:49:33.930: ISAKMP (0:1): processing vendor id payload

*Mar 1 00:49:33.930: ISAKMP (0:1): vendor ID is DPD

*Mar 1 00:49:33.930: ISAKMP (0:1): processing vendor id payload

*Mar 1 00:49:33.934: ISAKMP (0:1): speaking to another IOS box!

*Mar 1 00:49:33.934: ISAKMP (0:1): processing vendor id payload

*Mar 1 00:49:33.934: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar 1 00:49:33.934: ISAKMP (0:1): Old State = IKE_I_MM4 New State = IKE_I_MM4

*Mar 1 00:49:33.938: ISAKMP (0:1): Send initial contact

*Mar 1 00:49:33.938: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR

*Mar 1 00:49:33.938: ISAKMP (1): ID payload

    next-payload : 8

    type   : 1

    protocol   : 17

    port   : 500

    length   : 8

*Mar 1 00:49:33.938: ISAKMP (1): Total payload length: 12

*Mar 1 00:49:33.942: ISAKMP (0:1): sending packet to 172.30.2.2 (I) MM_KEY_EXCH

*Mar 1 00:49:33.942: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar 1 00:49:33.946: ISAKMP (0:1): Old State = IKE_I_MM4 New State = IKE_I_MM5

*Mar 1 00:49:34.014: ISAKMP (0:1): received packet from 172.30.2.2 (I) MM_KEY_EXCH

*Mar 1 00:49:34.018: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Mar 1 00:49:34.018: ISAKMP (0:1): Old State = IKE_I_MM5 New State = IKE_I_MM6

*Mar 1 00:49:34.018: ISAKMP (0:1): processing ID payload. message ID = 0

*Mar 1 00:49:34.018: ISAKMP (0:1): processing HASH payload. message

ID = 0

*Mar 1 00:49:34.022: ISAKMP (0:1): SA has been authenticated with 172.30.2.2

*Mar 1 00:49:34.022: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE

*Mar 1 00:49:34.022: ISAKMP (0:1): Old State = IKE_I_MM6 New State = IKE_I_MM6

*Mar 1 00:49:34.026: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE

*Mar 1 00:49:34.026: ISAKMP (0:1): Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE

*Mar 1 00:49:34.026: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -695191653

*Mar 1 00:49:34.030: ISAKMP (0:1): sending packet to 172.30.2.2 (I) QM_IDLE

*Mar 1 00:49:34.034: ISAKMP (0:1): Node -695191653, Input = IKE_MESG_INTERNAL, IKE_INIT_QM

*Mar 1 00:49:34.034: ISAKMP (0:1): Old State = IKE_QM_READY New State = IKE_QM_I_QM1

*Mar 1 00:49:34.034: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

*Mar 1 00:49:34.034: ISAKMP (0:1): Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

*Mar 1 00:49:34.399: ISAKMP (0:1): received packet from 172.30.2.2 (I) QM_IDLE

*Mar 1 00:49:34.403: ISAKMP (0:1): processing HASH payload. message ID = -695191653

*Mar 1 00:49:34.403: ISAKMP (0:1): processing SA payload. message ID = -695191653

*Mar 1 00:49:34.403: ISAKMP (0:1): Checking IPSec proposal 1

*Mar 1 00:49:34.403: ISAKMP: transform 1, ESP_DES

*Mar 1 00:49:34.403: ISAKMP: attributes in transform:

*Mar 1 00:49:34.403: ISAKMP: encaps is 1

*Mar 1 00:49:34.403: ISAKMP: SA life type in seconds

*Mar 1 00:49:34.407: ISAKMP: SA life duration (basic) of 3600

*Mar 1 00:49:34.407: ISAKMP: SA life type in kilobytes

*Mar 1 00:49:34.407: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0

*Mar 1 00:49:34.407: ISAKMP (0:1): atts are acceptable.

*Mar 1 00:49:34.407: IPSEC(validate_proposal_request): proposal part #1,

  (key eng. msg.) INBOUND local= 172.30.1.2, remote= 172.30.2.2,

    local_proxy= 10.0.1.0/255.255.255.0/6/0 (type=4),

    remote_proxy= 10.0.2.0/255.255.255.0/6/0 (type=4),

    protocol= ESP, transform= esp-des ,

    lifedur= 0s and 0kb,

    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

*Mar 1 00:49:34.411: ISAKMP (0:1): processing NONCE payload. message ID = -695191653

*Mar 1 00:49:34.411: ISAKMP (0:1): processing ID payload. message ID = -695191653

*Mar 1 00:49:34.411: ISAKMP (0:1): processing ID payload. message ID = -695191653

*Mar 1 00:49:34.419: ISAKMP (0:1): Creating IPSec SAs

*Mar 1 00:49:34.419: inbound SA from 172.30.2.2 to 172.30.1.2

(proxy 10.0.2.0 to 10.0.1.0)

*Mar 1 00:49:34.419: has spi 0x9B717872 and conn_id 2000 and flags 4

*Mar 1 00:49:34.419: lifetime of 3600 seconds

*Mar 1 00:49:34.423: lifetime of 4608000 kilobytes

*Mar 1 00:49:34.423: outbound SA from 172.30.1.2 to 172.30.2.2 (proxy 10.0.1.0 to 10.0.2.0)

*Mar 1 00:49:34.423: has spi 1010876185 and conn_id 2001 and flags C

*Mar 1 00:49:34.423: lifetime of 3600 seconds

*Mar 1 00:49:34.423: lifetime of 4608000 kilobytes

*Mar 1 00:49:34.423: ISAKMP (0:1): sending packet to 172.30.2.2 (I) QM_IDLE

*Mar 1 00:49:34.427: ISAKMP (0:1): deleting node -695191653 error FALSE reason ""

*Mar 1 00:49:34.427: ISAKMP (0:1): Node -695191653, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH

*Mar 1 00:49:34.427: ISAKMP (0:1): Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE

*Mar 1 00:49:34.427: IPSEC(key_engine): got a queue event...

*Mar 1 00:49:34.427: IPSEC(initialize_sas): ,

  (key eng. msg.) INBOUND local= 172.30.1.2, remote= 172.30.2.2,

    local_proxy= 10.0.1.0/255.255.255.0/6/0 (type=4),

    remote_proxy= 10.0.2.0/255.255.255.0/6/0 (type=4),

    protocol= ESP, transform= esp-des ,

    lifedur= 3600s and 4608000kb,

    spi= 0x9B717872(2607904882), conn_id= 2000, keysize= 0, flags= 0x4

*Mar 1 00:49:34.431: IPSEC(initialize_sas): ,

  (key eng. msg.) OUTBOUND local= 172.30.1.2, remote= 172.30.2.2,

    local_proxy= 10.0.1.0/255.255.255.0/6/0 (type=4),

    remote_proxy= 10.0.2.0/255.255.255.0/6/0 (type=4),

    protocol= ESP, transform= esp-des ,

    lifedur= 3600s and 4608000kb,

    spi= 0x3C40BF19(1010876185), conn_id= 2001, keysize= 0, flags= 0xC

*Mar 1 00:49:34.435: IPSEC(create_sa): sa created,

  (sa) sa_dest= 172.30.1.2, sa_prot= 50,

    sa_spi= 0x9B717872(2607904882),

    sa_trans= esp-des , sa_conn_id= 2000

*Mar 1 00:49:34.435: IPSEC(create_sa): sa created,

  (sa) sa_dest= 172.30.2.2, sa_prot= 50,

    sa_spi= 0x3C40BF19(1010876185),

sa_trans= esp-des , sa_conn_id= 2001

RA#

*Mar 1 00:50:24.429: ISAKMP (0:1): purging node -695191653

Qua debug ta thấy quá trình tạo private tunnel giữa 2 router khi có TCP traffic gửi đến, lúc đầu là xác minh, nếu thành công sẽ mã hoá traffic và gửi sang bên peer kia.

Chú ý:

Cách bật telnet service trên 1 pc cài WinXP:

Start→control panel→Administrative tools→service

Sau đó sửa service telnet bằng cách nhấn phải chuột vào Telnet service→properties→Chọn startup type là manual→ sau đó start service lên.