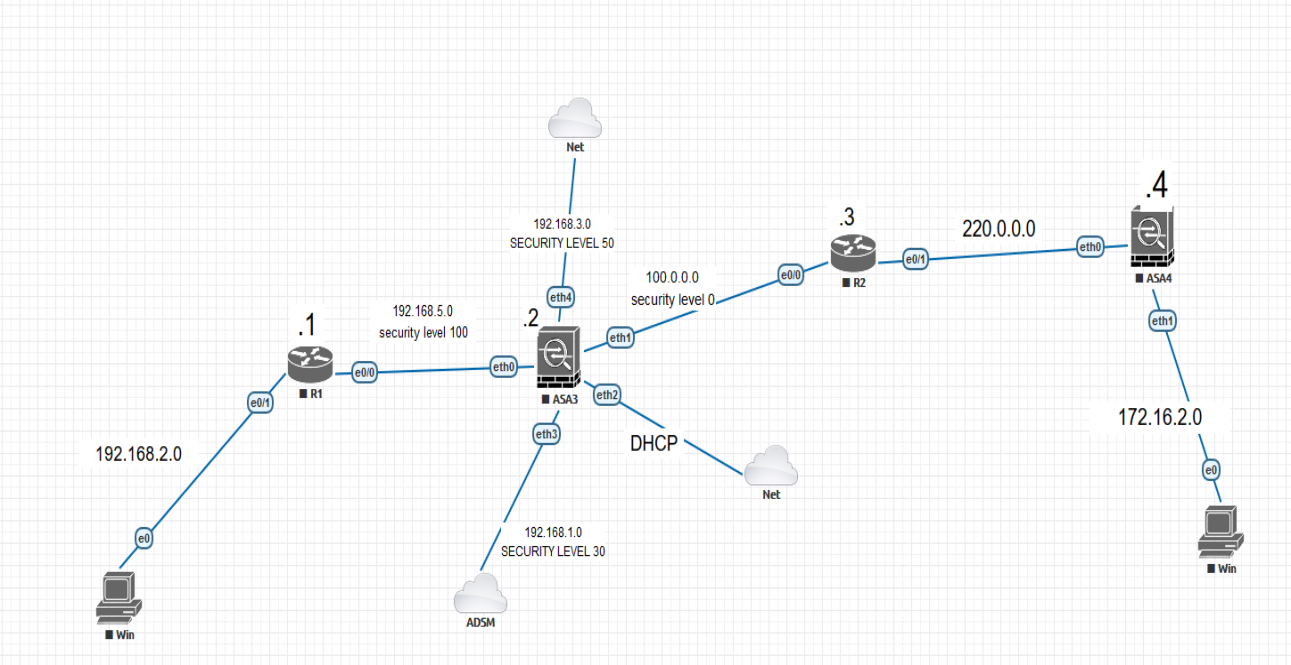
CẤU HÌNH VPN SITE TO SITE ESP MODE TUNNEL TRÊN FIREWALL ASA



Sơ đồ cấu hình VPN SITE TO SITE TỪ LAN 192.168.2.0 ĐẾN LAN 172.16.2.0 .Với các dãy địa chỉ ip được hoạch định như ảnh , ta tiến hành cấu hình.

Bước 1: Đặt ip cho các thiết bị router theo hoạch định.

Bước 2: Đặt ip cho các firewall ASA như sau :

```
ciscoasa(config)# hostname ASA3
ASA3(config)# int e4
ASA3(config-if)# nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ASA3(config-if)# security-level 50
ASA3(config-if)# main-loop: WARNING: I/O thread spun for 1000 iterations

ASA3(config-if)# ip address 192.168.3.2 255.255.255.0
ASA3(config-if)# no shut
ASA3(config-if)# exit
```

Các cổng còn lại ta tiến hành cấu hình tương tự.

Bước 3: Tiến hành cấu hình định tuyến ở nhánh Lan của ASA3

```
R1(config)#router ospf 1
R1(config-router)#netwo
R1(config-router)#network 192.168.2.0 0.0.0.255 area 0
R1(config-router)#network 192.168.5.0 0.0.0.255 area 0
R1(config-router)#exit
```

Định tuyến trên router R1 các lớp mạng 192.168.2.0 và 192.168.5.0

```
ASA3(config)# router ospf 1
ASA3(config-router)# network 192.168.5.0 255.255.255.0 area 0
```

Trên firewall ASA3 ,chúng ta chỉ nên quảng bá 1 lớp mạng thuộc Inside 192.168.5.0 , không nên thêm các quảng bá lớp mạng vùng DMZ và management lan vào ospf.

```
[OK]
ASA3(config)# route outside1 0.0.0.0 0.0.0.0 100.0.0.3
```

Trên firewall ASA 3 và 4 ta tiến hành cấu hình default route sang next hop là R2 (ở đây được xem là ISP router).

Trên router ISP là R2 , chúng ta không cấu hình thêm bất kỳ tập lệnh nào về route nữa.Và bảng định tuyến R2 như sau :

```
R2(config)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      100.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        100.0.0.0/24 is directly connected, Ethernet0/0
L        100.0.0.3/32 is directly connected, Ethernet0/0
      220.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        220.0.0.0/24 is directly connected, Ethernet0/1
L        220.0.0.3/32 is directly connected, Ethernet0/1
R2(config)#
```

Bắt đầu cấu hình vpn + ipsec

Bước 4 (pha 1): Chúng ta cấu hình lựa chọn việc vận chuyển khóa mật mã giữa 2 firewall VPN . Ở đây ta chọn IKEV1 với cổng ra outside1 , sử dụng preshare key được mã hóa 3des và hàm băm md5.

```
ASA3(config)# crypto ikev1 enable outside1
ASA3(config)# crypto ikev1 policy 2
ASA3(config-ikev1-policy)# authentication pre-share
ASA3(config-ikev1-policy)# encryption 3des
ASA3(config-ikev1-policy)# hash md5
ASA3(config-ikev1-policy)# group 2
ASA3(config-ikev1-policy)# lifetime 3600
ASA3(config-ikev1-policy)# exit
ASA3(config)#
```

Tiếp theo ta cấu hình Ipsec theo mode tunnel (l2l tức vpn lan to lan), chỉ định trỏ vào ip public của phía vpn router đối phương (ở đây là ASA4) với preshare key cisco123.

```
ASA3(config)# tunnel-group 220.0.0.4 type ise
ASA3(config)# tunnel-group 220.0.0.4 type ipsec-l2l
ASA3(config)# tunnel-group 220.0.0.4 ipsec
ASA3(config)# tunnel-group 220.0.0.4 ipsec-attributes
ASA3(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
ASA3(config-tunnel-ipsec)# exit
```

Bước 5: Tạo 2 object chỉ định 2 lớp mạng Inside và lớp mạng trỏ tới bên Lan đối phương.

```
ASA3(config)# object network INSIDE_NETWORK
ASA3(config-network-object)# subnet 192.168.2.0 255.255.255.0
ASA3(config-network-object)# exit
ASA3(config)# object network REMOTE_NETWORK
ASA3(config-network-object)# subnet 172.16.2.0 255.255.255.0
ASA3(config-network-object)# exit
```

Bước 6: Tạo 1 access list permit 2 lớp object trên

Câu lệnh là access-list VPN_TRAFFIC extended permit ip object INSIDE_NETWORK object REMOTE_NETWORK

```
access-list VPN_TRAFFIC extended permit ip object INSIDE_NETWORK object REMOTE_N
ETWORK
```

Bước 7 (pha 2): Thực hiện cấu hình giao thức đóng gói bảo vệ IPSEC ở đây chúng ta chọn ESP (Encapsulation security protocol) với giao thức mã hóa AES 256 bit và hàm băm SHA . Sau đó map với access list vừa tạo ở trên và cổng thiết lập Tunnel ra(nơi bắt đầu cấu tạo đường hầm) là outside1.

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map TO_BRANCH 1 match address VPN_TRAFFIC
crypto map TO_BRANCH 1 set pfs group5
crypto map TO_BRANCH 1 set peer 220.0.0.4
crypto map TO_BRANCH 1 set ikev1 transform-set ESP-AES-256-SHA
crypto map TO_BRANCH 1 set security-association lifetime seconds 1800
crypto map TO_BRANCH interface outside1
```

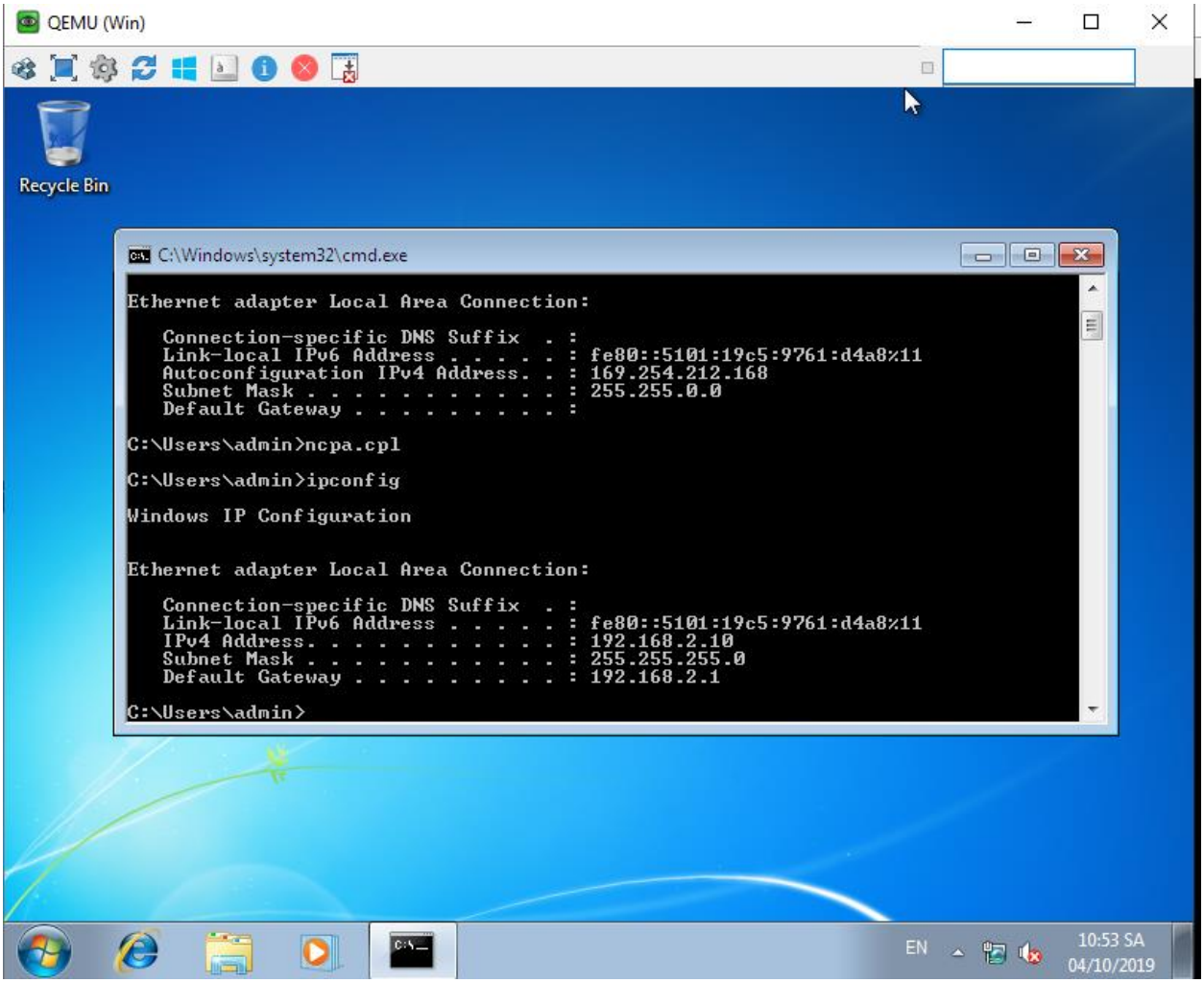
Bước 8: Tiến hành cấu hình tương tự cho firewall ASA2

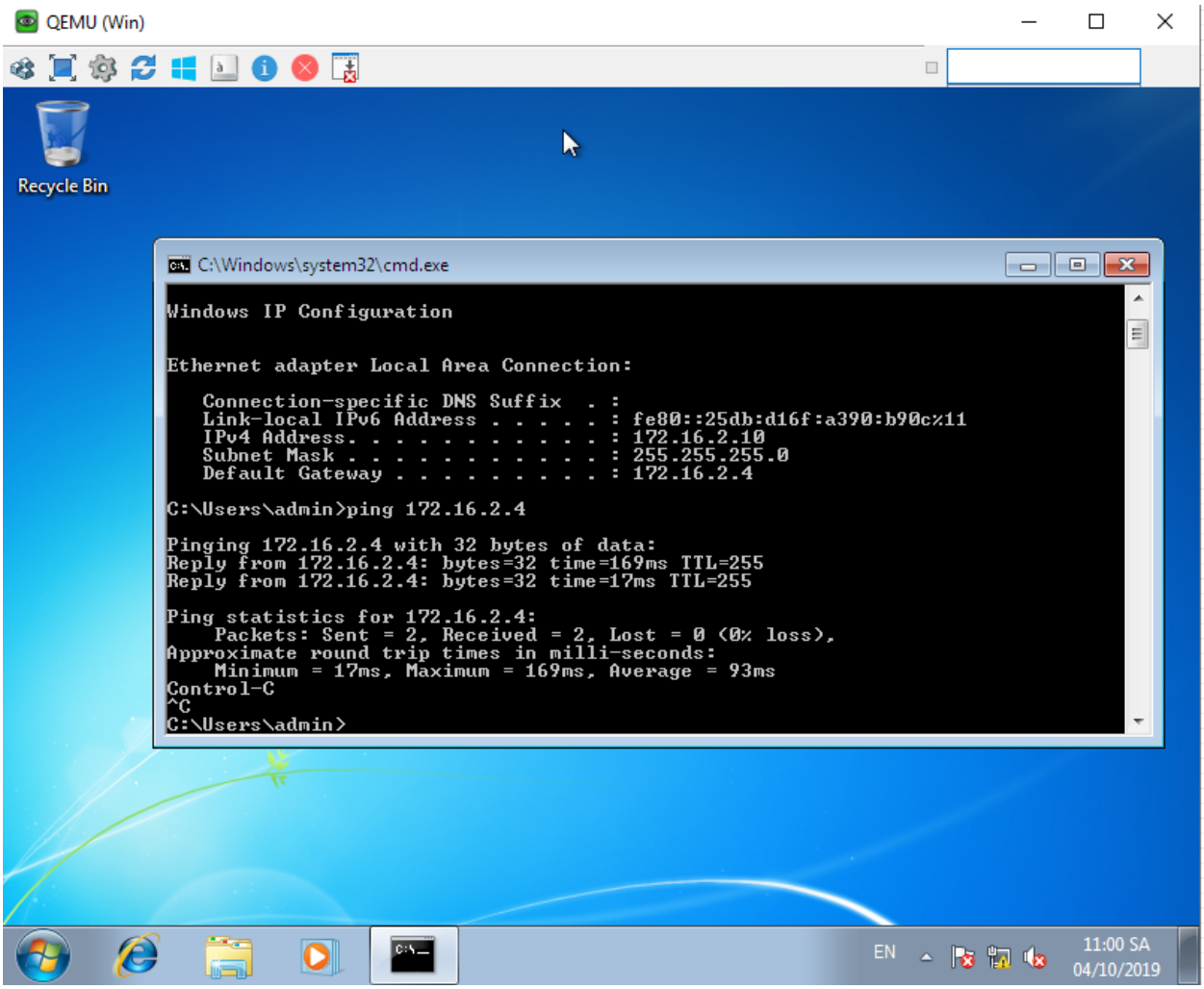
Bước 9: Cấu hình permit ICMP (cho phép ping) trên cả 2 firewall ASA.

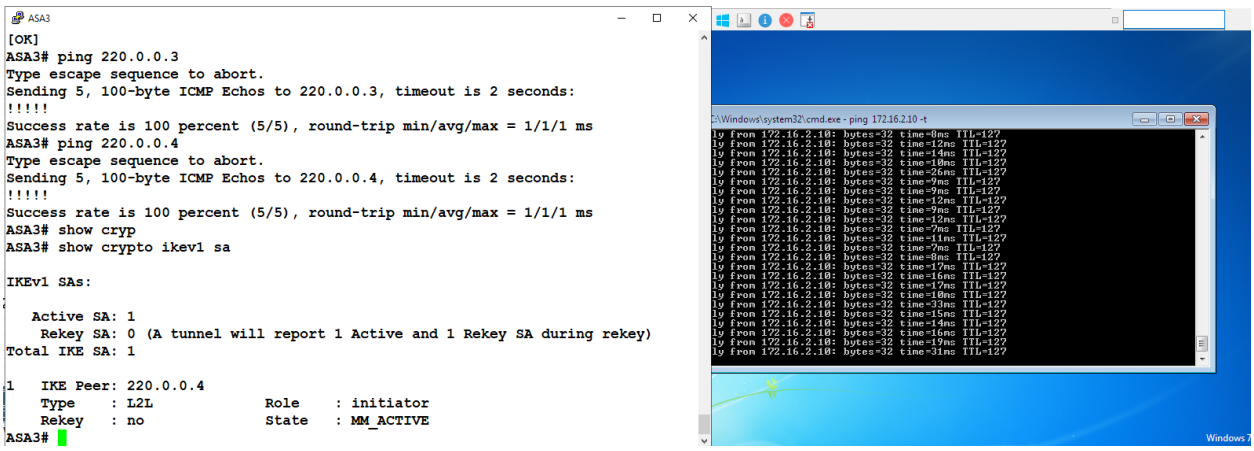
```
ASA3(config)# policy-map global_policy

ASA3(config-pmap)# class inspection_default
ASA3(config-pmap-c)# inspect icmp
ASA3(config-pmap-c)# exit
```

Nghiệm thu : Tiến hành kiểm tra giao thức VPN đã thiết lập thành công hay chưa bằng cách ping (gửi gói tin ICMP) từ mạng lan site 1 192.168.2.0/24 sang lan site 2 172.16.2.0/24

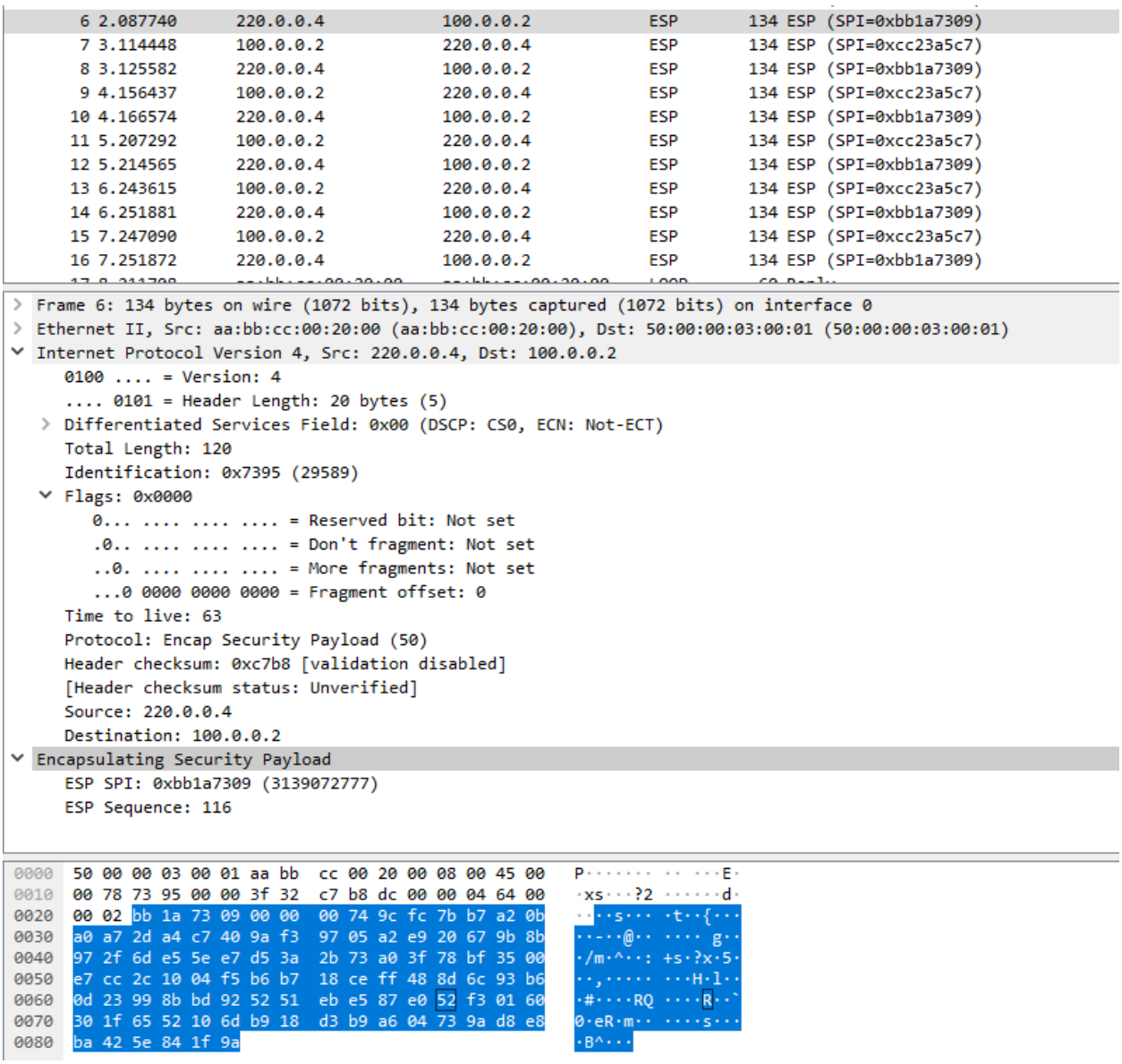

QEMU (Win)
Recycle Bin
C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5101:19c5:9761:d4a8%11
Autoconfiguration IPv4 Address. . : 169.254.212.168
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
C:\Users\admin>ncpa.cpl
C:\Users\admin>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5101:19c5:9761:d4a8%11
IPv4 Address. . . . . : 192.168.2.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
C:\Users\admin>
EN
10:53 SA
04/10/2019





Ở hình trên ta có thể quan sát được cả 2 lớp mạng đã thông nhau và firewall báo log về đã thiết lập vận chuyển khóa thành công sang peer 220.0.0.4(chính là ASA

4). Để chứng minh VPN hoạt động theo đúng đường hầm mà không phải đi theo dạng thông thường thiếu an toàn , ta xem việc bắt gói tin qua Wireshark.



6	2.087740	220.0.0.4	100.0.0.2	ESP	134 ESP (SPI=0xbb1a7309)
7	3.114448	100.0.0.2	220.0.0.4	ESP	134 ESP (SPI=0xcc23a5c7)
8	3.125582	220.0.0.4	100.0.0.2	ESP	134 ESP (SPI=0xbb1a7309)
9	4.156437	100.0.0.2	220.0.0.4	ESP	134 ESP (SPI=0xcc23a5c7)
10	4.166574	220.0.0.4	100.0.0.2	ESP	134 ESP (SPI=0xbb1a7309)
11	5.207292	100.0.0.2	220.0.0.4	ESP	134 ESP (SPI=0xcc23a5c7)
12	5.214565	220.0.0.4	100.0.0.2	ESP	134 ESP (SPI=0xbb1a7309)
13	6.243615	100.0.0.2	220.0.0.4	ESP	134 ESP (SPI=0xcc23a5c7)
14	6.251881	220.0.0.4	100.0.0.2	ESP	134 ESP (SPI=0xbb1a7309)
15	7.247090	100.0.0.2	220.0.0.4	ESP	134 ESP (SPI=0xcc23a5c7)
16	7.251872	220.0.0.4	100.0.0.2	ESP	134 ESP (SPI=0xbb1a7309)

```
> Frame 6: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
> Ethernet II, Src: aa:bb:cc:00:20:00 (aa:bb:cc:00:20:00), Dst: 50:00:00:03:00:01 (50:00:00:03:00:01)
v Internet Protocol Version 4, Src: 220.0.0.4, Dst: 100.0.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x7395 (29589)
  v Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 63
    Protocol: Encap Security Payload (50)
    Header checksum: 0xc7b8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 220.0.0.4
    Destination: 100.0.0.2
v Encapsulating Security Payload
    ESP SPI: 0xbb1a7309 (3139072777)
    ESP Sequence: 116
```

```
0000  50 00 00 03 00 01 aa bb  cc 00 20 00 08 00 45 00   P······ ·· ···E·
0010  00 78 73 95 00 00 3f 32  c7 b8 dc 00 00 04 64 00   ·xs···?2 ·····d·
0020  00 02 bb 1a 73 09 00 00  00 74 9c fc 7b b7 a2 0b   ··  ··s··· ·t··{···
0030  a0 a7 2d a4 c7 40 9a f3  97 05 a2 e9 20 67 9b 8b   ··-··@·· ···· g··
0040  97 2f 6d e5 5e e7 d5 3a  2b 73 a0 3f 78 bf 35 00   ·/m·^··: +s·?x·5·
0050  e7 cc 2c 10 04 f5 b6 b7  18 ce ff 48 8d 6c 93 b6   ··,····· ···H·l··
0060  0d 23 99 8b bd 92 52 51  eb e5 87 e0 52 f3 01 60   ·#····RQ ····R··`
0070  30 1f 65 52 10 6d b9 18  d3 b9 a6 04 73 9a d8 e8   0·eR·m·· ····s···
0080  ba 42 5e 84 1f 9a                                 ·B^···
```

Như ta đã quan sát ở trên, gói ICMP chúng ta gửi đi (khi ping từ máy tính 192.168.2.10 sang 172.16.2.10) đã được đóng gói an toàn qua giao thức IPSEC bảo mật ESP . Mode IPSEC VPN ở đây là Tunnel (đường hầm) vì gói tin đã được đóng gói lại một IP header mới (Ip source và dest) chính là ip public của 2 cổng outside1 của ASA3 và outside của ASA4 thay vì source 192.168.2.10 và dest 172.16.2.10.