Name :Harsh Kadu   Roll No : 33

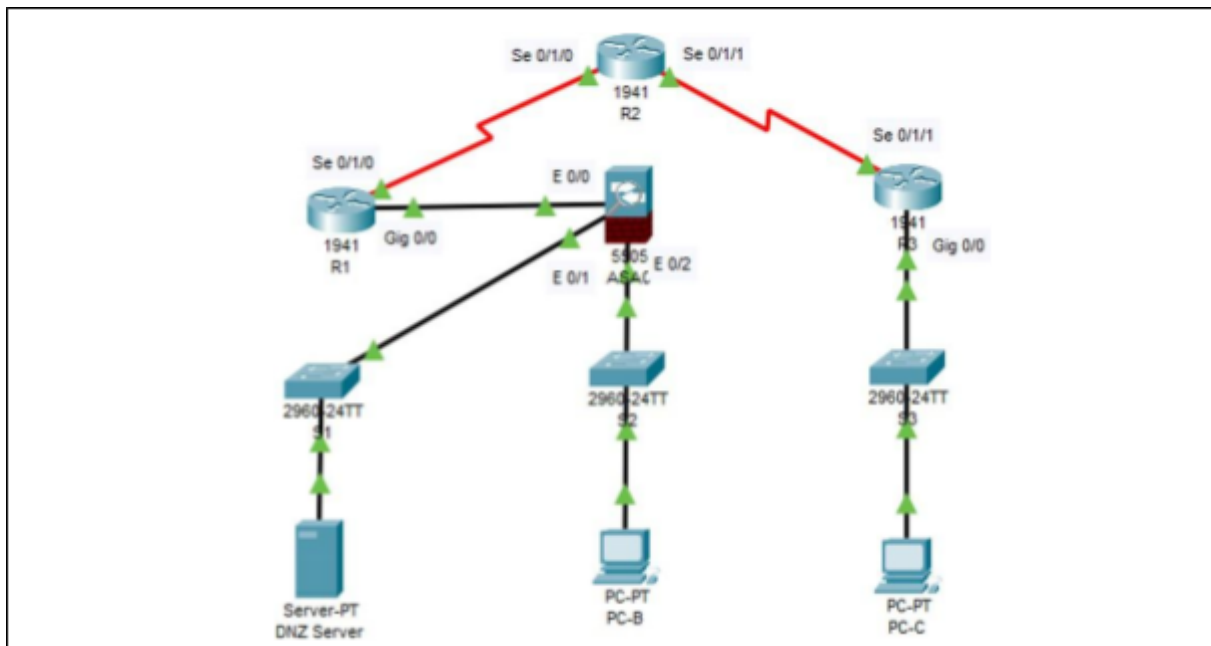## Practical 10

Configure ASA Basic Settings and Firewall using CLI

## Topology:

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router1 (R1)	GigabitEthernet 0/0	209.165.200.225	255.255.255.248	
	Serial 0/1/0	10.1.1.1	255.255.255.252	
Router2 (R2)	Serial 0/1/0	10.1.1.2	255.255.255.252	
	Serial 0/1/1	10.2.2.2	255.255.255.252	
Router3 (R3)	GigabitEthernet 0/0	172.16.3.1	255.255.255.0	
	Serial 0/1/1	10.2.2.1	255.255.255.252	
DNZ Server	FastEthernet0	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	FastEthernet0	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	FastEthernet0	172.16.3.3	255.255.0.0	172.16.3.1

Name :Harsh Kadu   Roll No : 33

Procedure:

Step 1: Add Serial Interface to each Router before connecting component:

i) Click on Router1 (R1) ➜ Physical Tab ➜ Switch off the switch first ➜ Select H2WIC-2T
➜   Drag it and place it on Interface ➜ Make Switch On.

Repeat the same procedure on Router2 (R2) and Router3

(R3).
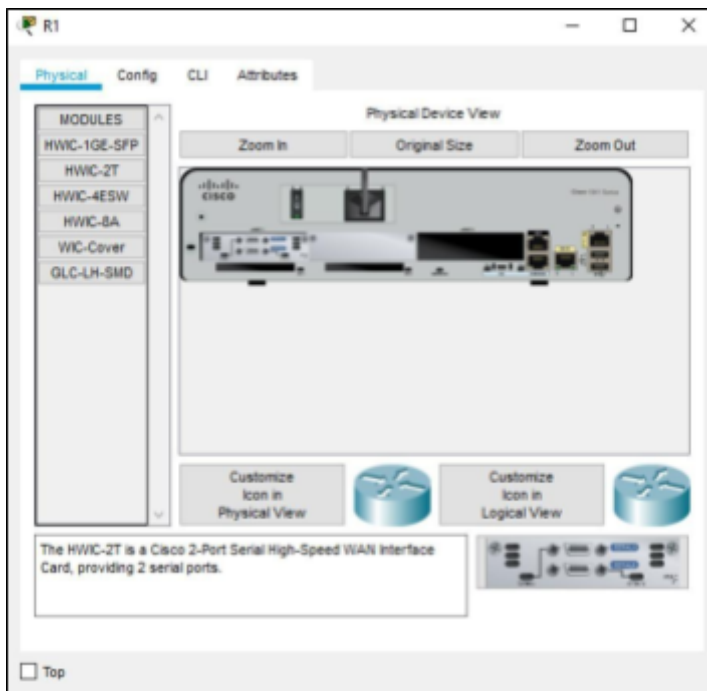
Step 2: Configure Commands on all Routers:

i) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

```
R1>enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable secret enpa55
R1(config)#line console 0
R1(config-line)#password conpa55
R1(config-line)#login
R1(config-line)#exit
R1(config)#ip domain-name ccnasecurity.com
R1(config)#username admin secret adminpa55
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Name :Harsh Kadu   Roll No : 33

ii) Click on Router2 (R2) ➜ CLI Tab ➜ Type the following Commands:

```
R2>enable
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#enable secret enpa55
R2(config)#line console 0
R2(config-line)#password conpa55
R2(config-line)#login
R2(config-line)#exit
R2(config)#ip domain-name ccnasecurity.com
R2(config)#username admin secret adminpa55
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#exit
R2(config)#crypto key generate rsa
The name for the keys will be: R2.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

iii) Click on Router3 (R3) ➜ CLI Tab ➜ Type the following Commands:

```
R3>enable
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable secret enpa55
R3(config)#line console 0
R3(config-line)#password conpa55
R3(config-line)#login
R3(config-line)#exit
R3(config)#ip domain-name ccnasecurity.com
R3(config)#username admin secret adminpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#exit
R3(config)#crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Step 3: Configure OSPF on Routers:

i) Click on Router1 (R1) ➜ CLI Tab ➜ Type the following Commands:

```
R1>enable
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 209.165.200.0 0.0.0.7 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#exit
R1(config)#
```

Name :Harsh Kadu   Roll No : 33

ii) Click on Router2 (R2) ➜ CLI Tab ➜ Type the following Commands:

```
R2>enable
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#
00:38:34: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/1/0 from LOADING to FULL, Loading Done
router ospf 1
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#exit
```

iii) Click on Router3 (R3) ➜ CLI Tab ➜ Type the following Commands:

```
R3>enable
Password:
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 172.16.3.0 0.0.0.255 area 0
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
R3(config-router)#exit
R3(config)#
00:40:42: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/1/1 from
LOADING to FULL, Loading Done
```

Step 4: **Configure ASA Settings on DMZ Server:**

i) Click on DMZ Server ➜ CLI Tab ➜ Type the following Commands:

```
CCNAS-ASA#show version

Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)

Compiled on Wed 15-Jun-11 18:17 by mnguyen
System image file is "disk0:/asa842-k8.bin
Config file at boot was "startup-config"

CCNAS-ASA up 48 minutes 54 seconds

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB
```

Name :Harsh Kadu   Roll No : 33

```
Encryption hardware device : Cisco ASA-5505 on-board accelerator
(revision 0x0)
                              Boot microcode          : CN1000-MC-
BOOT-2.00
                              SSL/IKE microcode       : CNLite-MC-SSLm-
PLUS-2.03
                              IPSec microcode         : CNlite-MC-
IPSECm-MAIN-2.06
                              Number of accelerators: 1

  0: Int: Internal-Data0/0   : address is 44d3.caef.1e22, irq 11
  1: Ext: Ethernet0/0        : address is 0002.4A9C.5D01, irq 255
  2: Ext: Ethernet0/1        : address is 0002.4A9C.5D02, irq 255
  3: Ext: Ethernet0/2        : address is 0002.4A9C.5D03, irq 255
  4: Ext: Ethernet0/3        : address is 0002.4A9C.5D04, irq 255
  5: Ext: Ethernet0/4        : address is 0002.4A9C.5D05, irq 255
  6: Ext: Ethernet0/5        : address is 0002.4A9C.5D06, irq 255
  7: Ext: Ethernet0/6        : address is 0002.4A9C.5D07, irq 255
  8: Ext: Ethernet0/7        : address is 0002.4A9C.5D08, irq 255
  9: Int: Internal-Data0/1   : address is 0000.0003.0002, irq 255
 10: Int: Not used           : irq 255
 11: Int: Not used           : irq 255

Licensed features for this platform:
Maximum Physical Interfaces   : 8            perpetual
VLANs                         : 3            DMZ Restricted
Dual ISPs                     : Disabled     perpetual
VLAN Trunk Ports              : 0            perpetual
Inside Hosts                  : 10           perpetual
Failover                      : Disabled     perpetual
VPN-DES                       : Enabled      perpetual
VPN-3DES-AES                  : Enabled      perpetual
AnyConnect Premium Peers      : 2            perpetual
AnyConnect Essentials         : Disabled     perpetual
Other VPN Peers               : 10           perpetual
Total VPN Peers               : 25           perpetual
Shared License                : Disabled     perpetual
AnyConnect for Mobile         : Disabled     perpetual
AnyConnect for Cisco VPN Phone : Disabled    perpetual
Advanced Endpoint Assessment  : Disabled     perpetual
UC Phone Proxy Sessions       : 2            perpetual
Total UC Proxy Sessions       : 2            perpetual
Botnet Traffic Filter         : Disabled     perpetual
Intercompany Media Engine     : Disabled     perpetual

This platform has a Base license.

Serial Number: JMX1536E4XO-
Running Permanent Activation Key: 0x8901148A 0x3EEDBB32 0x5C8DD2C6
0x2C91D06E 0x3CADA275
Configuration register is 0x1
Configuration has not been modified since last system restart.


CCNAS-ASA#show file system

File Systems:

     Size(b)       Free(b)       Type  Flags  Prefixes
*    128573440     123001856     disk  rw     disk0: flash:
```

```
CCNAS-ASA#show flash:
--#--  --length--  -----date/time------  path
   1   5571584                           asa842-k8.bin

128573440 bytes total (123001856 bytes free)
```

Name :Harsh Kadu   Roll No : 33

```
CCNAS-ASA#config t
CCNAS-ASA(config)#domain-name ccnasecurity.com
CCNAS-ASA(config)#enable password enpa55
CCNAS-ASA(config)#clock set 08:36:00 7 feb 2025
CCNAS-ASA(config)#int vlan 1
CCNAS-ASA(config-if)#nameif inside
CCNAS-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#security-level 100
CCNAS-ASA(config-if)#int vlan 2
CCNAS-ASA(config-if)#nameif outside
CCNAS-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)#security-level 0
CCNAS-ASA(config-if)#exit
CCNAS-ASA(config)#exit
```

```
CCNAS-ASA#show int ip brief
Interface            IP-Address       OK? Method Status            Protocol

Ethernet0/0          unassigned       YES unset  up                up

Ethernet0/1          unassigned       YES unset  up                up

Ethernet0/2          unassigned       YES unset  up                up

Ethernet0/3          unassigned       YES unset  down              down

Ethernet0/4          unassigned       YES unset  down              down

Ethernet0/5          unassigned       YES unset  down              down

Ethernet0/6          unassigned       YES unset  down              down

Ethernet0/7          unassigned       YES unset  down              down

Vlan1                192.168.1.1      YES CONFIG up                up

Vlan2                209.165.200.226 YES manual up                 up
CCNAS-ASA#
```

```
CCNAS-ASA#show ip address
System IP Addresses:
Interface            Name             IP address       Subnet mask       Method
Vlan1                inside           192.168.1.1      255.255.255.0     CONFIG
Vlan2                outside          209.165.200.226 255.255.255.248   manual

Current IP Addresses:
Interface            Name             IP address       Subnet mask       Method
Vlan1                inside           192.168.1.1      255.255.255.0     CONFIG
Vlan2                outside          209.165.200.226 255.255.255.248   manual
```

```
CCNAS-ASA#show switch vlan

VLAN Name                                 Status    Ports
---- -------------------------------      --------- -------------------------------
1    inside                               up        Et0/1, Et0/2, Et0/3, Et0/4
                                                    Et0/5, Et0/6, Et0/7
2    outside                              up        Et0/0
CCNAS-ASA#
```

Name :Harsh Kadu   Roll No : 33

```
CCNAS-ASA#show route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
     209.165.200.0/29 is subnetted, 2 subnets
C       209.165.200.0 255.255.255.248 is directly connected, outside, Vlan2
C       209.165.200.224 255.255.255.248 is directly connected, outside, Vlan2
CCNAS-ASA#
```

Step 5: **Configure Address Translation:**

i) Click on DMZ Server ➜ CLI Tab ➜ Type the following Commands:

```
CCNAS-ASA#config t
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA(config)#exit
```

```
CCNAS-ASA#config t
CCNAS-ASA(config)#object network inside-net
CCNAS-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)#nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)#end
CCNAS-ASA#
```

```
CCNAS-ASA#show run
: Saved
:
ASA Version 8.4(2)
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password DzaLrtot/vx63hrf encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
```

Name :Harsh Kadu
Roll No : 33

```
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
!
!
object network inside-net
 nat (inside,outside) dynamic interface
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
!
!
CCNAS-ASA#
```

```
CCNAS-ASA#config t
CCNAS-ASA(config)#class-map inspection_default
CCNAS-ASA(config-cmap)#match default-inspection-traffic
CCNAS-ASA(config-cmap)#exit
CCNAS-ASA(config)#policy-map global_policy
CCNAS-ASA(config-pmap)#class inspection_default
CCNAS-ASA(config-pmap-c)#inspect icmp
CCNAS-ASA(config-pmap-c)#exit
CCNAS-ASA(config)#service-policy global_policy global
CCNAS-ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
CCNAS-ASA(config)#dhcpd dns 209.165.201.2 interface inside
CCNAS-ASA(config)#dhcpd enable inside
```

ii) Click on PC-B ➜ Desktop Tab ➜ IP Configuration ➜ Change Radio button to DHCP.

Name :Harsh Kadu   Roll No : 33
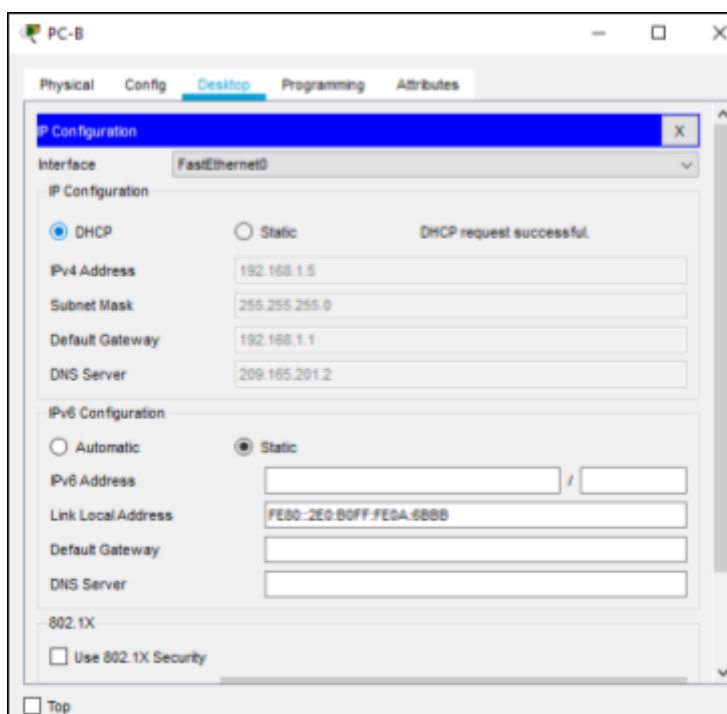
iii) Click on DMZ Server ➔ CLI Tab ➔ Type the following Commands:

```
CCNAS-ASA(config)#username admin password adminpa55
CCNAS-ASA(config)#aaa authentication ssh console LOCAL
CCNAS-ASA(config)#crypto key generate rsa modulu 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

```
CCNAS-ASA(config)#
CCNAS-ASA(config)#ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)#ssh timeout 10
```

Step 6: Verify SSH on PC-B:

i) Click on PC-B ➔ Desktop ➔ Command Prompt ➔ Type the following Command:

```
Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.1.1

Password:



CCNAS-ASA>
```

Step 7: Configure VLAN 3 on DMZ Server:

i) Click on DMZ Server ➔ CLI Tab ➔ Type the following Commands:

```
CCNAS-ASA(config)#int vlan 3
CCNAS-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)#no forward interface vlan 1
CCNAS-ASA(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
CCNAS-ASA(config-if)#security-level 70
CCNAS-ASA(config-if)#int et 0/2
CCNAS-ASA(config-if)#switchport access vlan 3
CCNAS-ASA(config-if)#exit
CCNAS-ASA(config)#exit
```

Name :Harsh Kadu   Roll No : 33

```
CCNAS-ASA#show int ip brief
Interface              IP-Address      OK? Method Status              Protocol

Ethernet0/0            unassigned      YES unset  up                  up

Ethernet0/1            unassigned      YES unset  up                  up

Ethernet0/2            unassigned      YES unset  up                  up

Ethernet0/3            unassigned      YES unset  down                down

Ethernet0/4            unassigned      YES unset  down                down

Ethernet0/5            unassigned      YES unset  down                down

Ethernet0/6            unassigned      YES unset  down                down

Ethernet0/7            unassigned      YES unset  down                down

Vlan1                  192.168.1.1     YES CONFIG up                  up

Vlan2                  209.165.200.226 YES manual up                  up

Vlan3                  192.168.2.1     YES manual up                  up
CCNAS-ASA#
```

```
CCNAS-ASA#show ip address
System IP Addresses:
Interface          Name          IP address        Subnet mask      Method
Vlan1              inside        192.168.1.1       255.255.255.0    CONFIG
Vlan2              outside       209.165.200.226 255.255.255.248 manual
Vlan3              dmz           192.168.2.1       255.255.255.0    manual

Current IP Addresses:
Interface          Name          IP address        Subnet mask      Method
Vlan1              inside        192.168.1.1       255.255.255.0    CONFIG
Vlan2              outside       209.165.200.226 255.255.255.248 manual
Vlan3              dmz           192.168.2.1       255.255.255.0    manual
```

```
CCNAS-ASA#show switch vlan

VLAN Name                                  Status      Ports
---- ------------------------------------- ---------   ----------------------------
1    inside                                up          Et0/1, Et0/3, Et0/4, Et0/5
                                                       Et0/6, Et0/7
2    outside                               up          Et0/0
3    dmz                                   up          Et0/2
CCNAS-ASA#
```

```
CCNAS-ASA#config t
CCNAS-ASA(config)#object network dmz-server
CCNAS-ASA(config-network-object)#host 192.168.2.3
CCNAS-ASA(config-network-object)#nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)#exit
CCNAS-ASA#
```

```
CCNAS-ASA#config t
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNAS-ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNAS-ASA(config)#access-group OUTSIDE-DMZ in interface outside
CCNAS-ASA(config)#exit
CCNAS-ASA#
```