VSIT

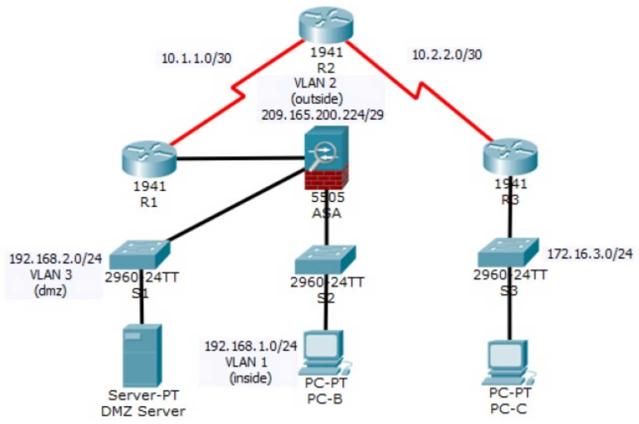
Security in Computing
Practical #8

Name	**Sanjeev Gupta**	**Roll Number**	**21302B0023**
Class	**TYBSc IT**	**Division**	**C**
Subject/Course	**Security in Computing**		
Topic	**Configuring ASA Basic Settings and Firewall Using CLI**		

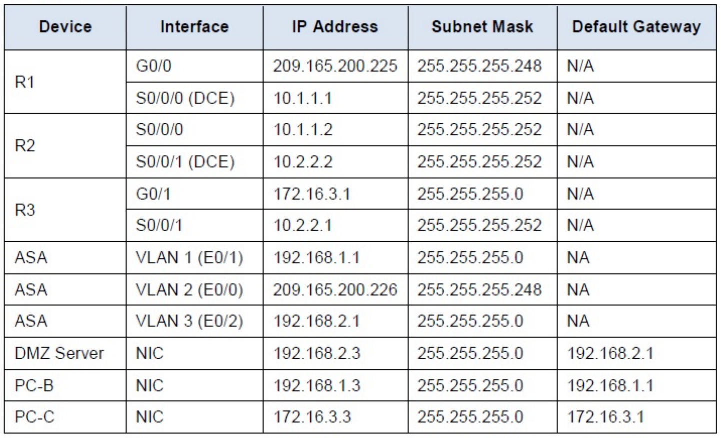
Topology and Addressing Table for IPS using CLI

Use the pre-configured topology shared as an attachment with this worksheet. Configure this topology for ASA and Firewall using CLI

Topology



IP Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Objectives

- Verify connectivity and explore the ASA
- Configure basic ASA settings and interface security levels using CLI
- Configure routing, address translation, and inspection policy using CLI
- Configure DHCP, AAA, and SSH
- Configure a DMZ, Static NAT, and ACLs

Scenario

Your company has one location connected to an ISP. R1 represents a CPE device managed by the ISP. R2 represents an intermediate Internet router. R3 represents an ISP that connects an administrator from a network management company, who has been hired to remotely manage your network. The ASA is an edge CPE security device that connects the internal corporate network and DMZ to the ISP while providing NAT and DHCP services to inside hosts. The ASA will be configured for management by an administrator on the internal network and by the remote administrator. Layer 3 VLAN interfaces provide access to the three areas created in the activity: Inside, Outside, and DMZ. The ISP assigned the public IP address space of 209.165.200.224/29, which will be used for address translation on the ASA. All router and switch devices have been preconfigured with the following:

o Enable password: ciscoenpa55
o Console password: ciscoconpa55
o Admin username and password: admin/adminpa55

Part 1 Verify Connectivity and Explore the ASA

Step 1: Verify connectivity.

The ASA is not currently configured. However, all routers, PCs, and the DMZ server are configured. Verify that PC-C can ping any router interface. PC-C is unable to ping the ASA, PC-B, or the DMZ server.

Step 2: Determine the ASA version, interfaces, and license.

Use the show version command to determine various aspects of this ASA device.

Step 3: Determine the file system and contents of flash memory.

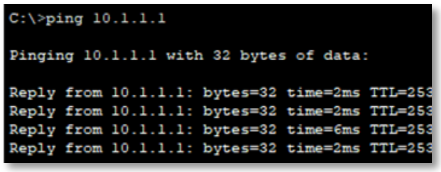
a. Enter privileged EXEC mode. A password has not been set. Press Enter when prompted for a password.

b. Use the show file system command to display the ASA file system and determine which prefixes are supported.

c. Use the show flash: or show disk0: command to display the contents of flash memory.

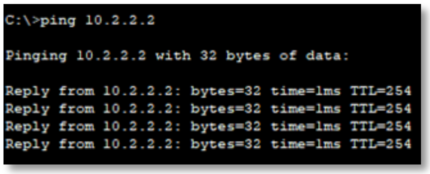
Insert screenshots here:

From PC-C to R1:



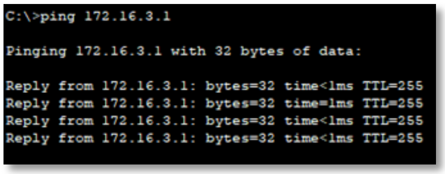
```
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=2ms TTL=253
Reply from 10.1.1.1: bytes=32 time=2ms TTL=253
Reply from 10.1.1.1: bytes=32 time=6ms TTL=253
Reply from 10.1.1.1: bytes=32 time=2ms TTL=253
```

From PC-C to R2:



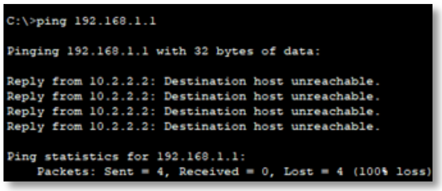
```
C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
```

From PC-C to R3:



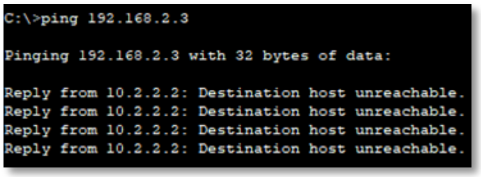
```
C:\>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:

Reply from 172.16.3.1: bytes=32 time<1ms TTL=255
Reply from 172.16.3.1: bytes=32 time=1ms TTL=255
Reply from 172.16.3.1: bytes=32 time<1ms TTL=255
Reply from 172.16.3.1: bytes=32 time<1ms TTL=255
```

From PC-C to ASA(Unsuccessful):



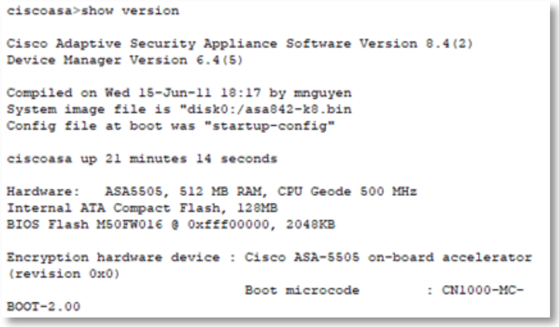
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 10.2.2.2: Destination host unreachable.
Reply from 10.2.2.2: Destination host unreachable.
Reply from 10.2.2.2: Destination host unreachable.
Reply from 10.2.2.2: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

From PC-C to DMZ:



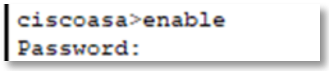
```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 10.2.2.2: Destination host unreachable.
Reply from 10.2.2.2: Destination host unreachable.
Reply from 10.2.2.2: Destination host unreachable.
Reply from 10.2.2.2: Destination host unreachable.
```

Step 2:



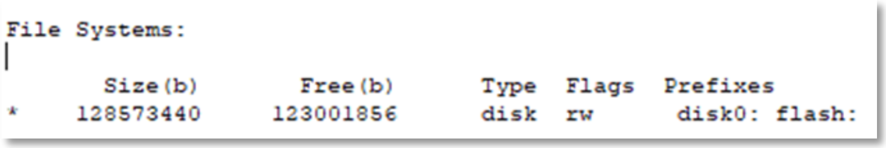
```
ciscoasa>show version

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"

ciscoasa up 21 minutes 14 seconds

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

Encryption hardware device : Cisco ASA-5505 on-board accelerator
(revision 0x0)
                             Boot microcode        : CN1000-MC-
BOOT-2.00
```

Step 3a:



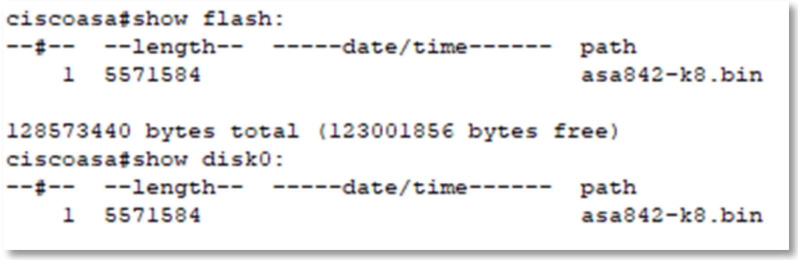
```
ciscoasa>enable
Password:
```

Step 3b:



```
File Systems:

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

Step 3c:



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

128573440 bytes total (123001856 bytes free)
ciscoasa#show disk0:
--#--  --length--  -----date/time------  path
    1  5571584                           asa842-k8.bin
```

Part 2: Configure ASA Settings and Interface Security Using the CLI

Step 1: Configure the hostname and domain name.

a. Configure the ASA hostname as CCNAS-ASA.

b. Configure the domain name as ccnasecurity.com.

Step 2: Configure the enable mode password.

Use the enable password command to change the privileged EXEC mode password to ciscoenpa55.

Step 3: Set the date and time.

Use the clock set command to manually set the date and time

Step 4: Configure the inside and outside interfaces.

You will only configure the VLAN 1 (inside) and VLAN 2 (outside) interfaces at this time. The VLAN 3 (dmz) interface will be configured in Part 5 of the activity.

a. Configure a logical VLAN 1 interface for the inside network (192.168.1.0/24) and set the security level to the highest setting of 100.

CCNAS-ASA(config)# interface 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

b. Create a logical VLAN 2 interface for the outside network (209.165.200.224/29), set the security level to the lowest setting of 0, and enable the VLAN 2 interface.

CCNAS-ASA(config-if)# interface 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

c. Use the following verification commands to check your configurations:

1) Use the show interface ip brief command to display the status for all ASA interfaces.

2) Use the show ip address command to display the information for the Layer 3 VLAN interfaces.

3) Use the show switch vlan command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

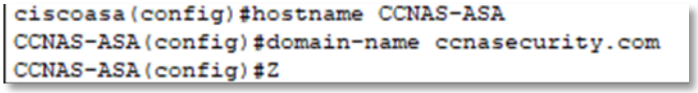
Step 5: Test connectivity to the ASA.

a. You should be able to ping from PC-B to the ASA inside interface address (192.168.1.1). If the pings fail, troubleshoot the configuration as necessary.

b. From PC-B, ping the VLAN 2 (outside) interface at IP address 209.165.200.226. You should not be able to ping this address.

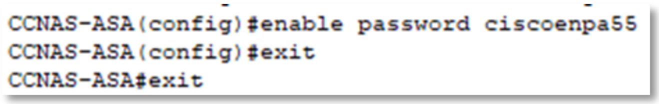
Insert screenshots here:

Step 1:



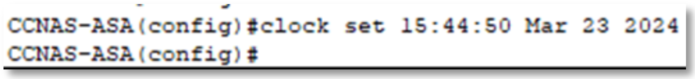
```
ciscoasa(config)#hostname CCNAS-ASA
CCNAS-ASA(config)#domain-name ccnasecurity.com
CCNAS-ASA(config)#Z
```

Step 2:



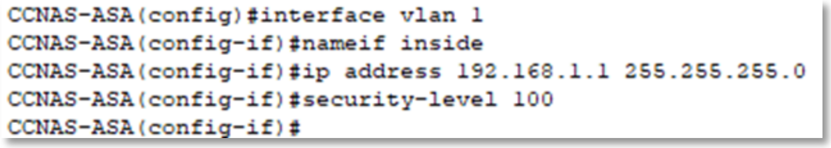
```
CCNAS-ASA(config)#enable password ciscoenpa55
CCNAS-ASA(config)#exit
CCNAS-ASA#exit
```

Step 3:



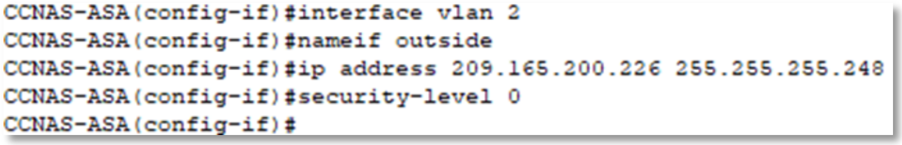
```
CCNAS-ASA(config)#clock set 15:44:50 Mar 23 2024
CCNAS-ASA(config)#
```

Step 4: VLAN-1



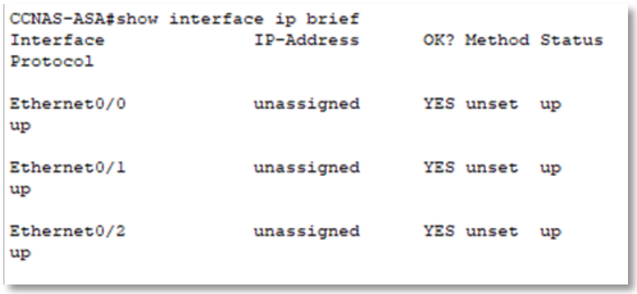
```
CCNAS-ASA(config)#interface vlan 1
CCNAS-ASA(config-if)#nameif inside
CCNAS-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)#security-level 100
CCNAS-ASA(config-if)#
```

Step 4b (VLAN-2):



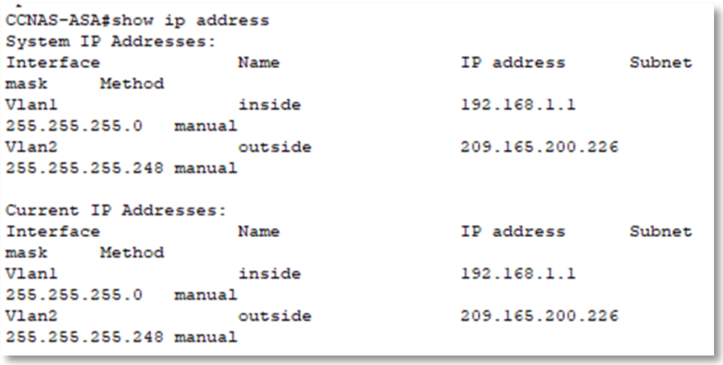
```
CCNAS-ASA(config-if)#interface vlan 2
CCNAS-ASA(config-if)#nameif outside
CCNAS-ASA(config-if)#ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)#security-level 0
CCNAS-ASA(config-if)#
```

Step 4c-1:



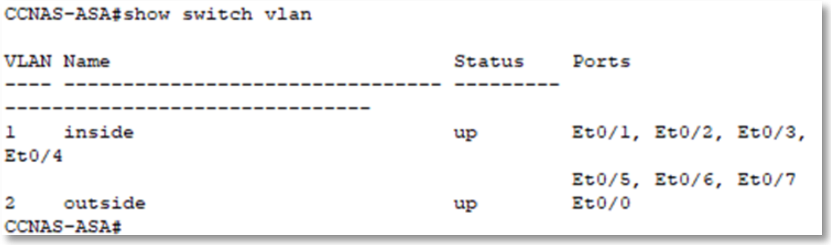
```
CCNAS-ASA#show interface ip brief
Interface                  IP-Address      OK? Method Status
Protocol

Ethernet0/0                unassigned      YES unset  up
up

Ethernet0/1                unassigned      YES unset  up
up

Ethernet0/2                unassigned      YES unset  up
up
```

Step 4c-2:



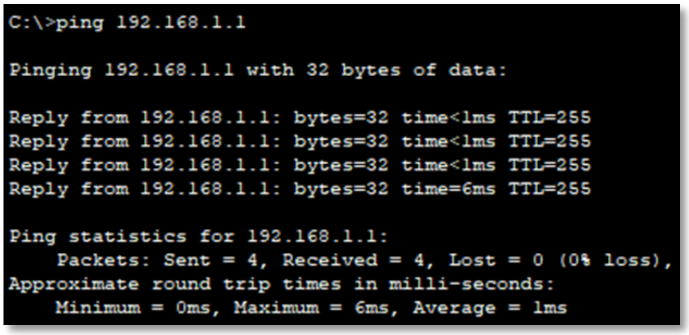
```
CCNAS-ASA#show ip address
System IP Addresses:
Interface             Name                     IP address       Subnet
mask      Method
Vlan1                 inside                   192.168.1.1
255.255.255.0    manual
Vlan2                 outside                  209.165.200.226
255.255.255.248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

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

Step 4c-3:



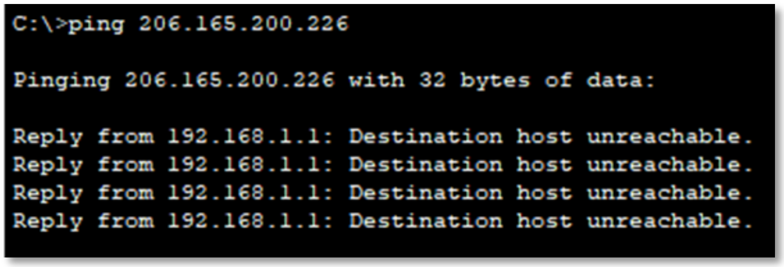
```
CCNAS-ASA#show switch vlan

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#
```

Step 5a (Pinging From PC-B to ASA):



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=6ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Step 5b (From PC-B to VLAN-2):



```
C:\>ping 206.165.200.226

Pinging 206.165.200.226 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

Part 3: Configure Routing, Address Translation, and Inspection Policy Using the CLI

Step 1: Configure a static default route for the ASA.

Configure a default static route on the ASA outside interface to enable the ASA to reach external networks.

a. Create a “quad zero” default route using the **route** command, associate it with the ASA outside interface, and point to the R1 G0/0 IP address (209.165.200.225) as the gateway of last resort.

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

b. Issue the **show route** command to verify the static default route is in the ASA routing table.

c. Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1

Step 2: Configure address translation using PAT and network objects.

a. Create network object **inside-net** and assign attributes to it using the **subnet** and **nat** commands.

```
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
```

b. The ASA splits the configuration into the object portion that defines the network to be translated and the actual **nat** command parameters. These appear in two different places in the running configuration. Display the NAT object configuration using the **show run** command.

c. From PC-B attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should fail.

d. Issue the **show nat** command on the ASA to see the translated and untranslated hits. Notice that, of the pings from PC-B, four were translated and four were not. The outgoing pings (echos) were translated and sent to the destination. The returning echo replies were blocked by the firewall policy. You will configure the default inspection policy to allow ICMP in Step 3 of this part of the activity.

Step 3: Modify the default MPF application inspection global service policy.

For application layer inspection and other advanced options, the Cisco MPF is available on ASAs.
The Packet Tracer ASA device does not have an MPF policy map in place by default. As a modification, we can create the default policy map that will perform the inspection on inside-to-outside traffic. When configured correctly only traffic initiated from the inside is allowed back in to the outside interface. You will need to add ICMP to the inspection list.

a. Create the class-map, policy-map, and service-policy. Add the inspection of ICMP traffic to the policy map list using the following commands:

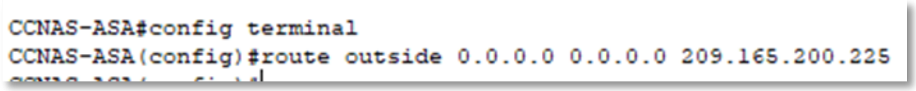
```
CCNAS-ASA(config)# class-map inspection_default
CCNAS-ASA(config-cmap)# match default-inspection-traffic
CCNAS-ASA(config-cmap)# exit
```

```
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
```

b. From PC-B, attempt to ping the R1 G0/0 interface at IP address 209.165.200.225. The pings should be successful this time because ICMP traffic is now being inspected and legitimate return traffic is being allowed.

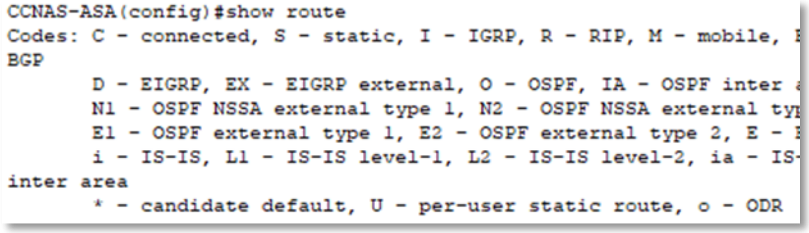
Insert screenshots here:

Step 1a:



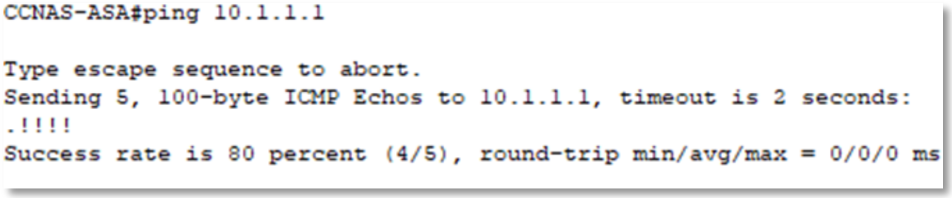
```
CCNAS-ASA#config terminal
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

Step 1b:



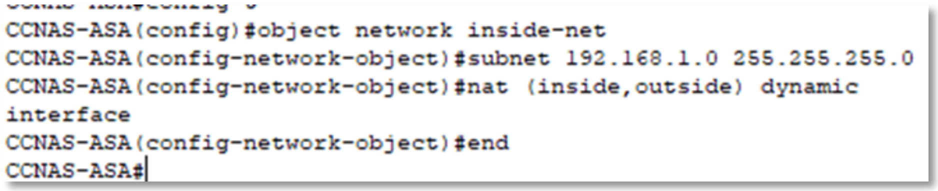
```
CCNAS-ASA(config)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter a
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external typ
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - E
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
inter area
       * - candidate default, U - per-user static route, o - ODR
```

Step 1c:



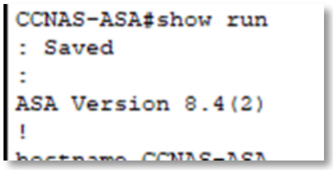
```
CCNAS-ASA#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Step 2a:

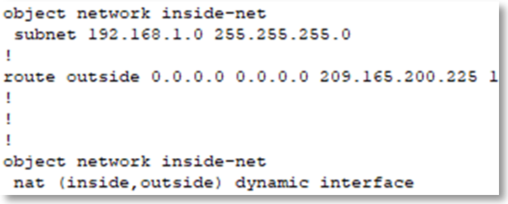


```
CCNAS-ASA(config)#object network inside-net
CCNAS-ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)#nat (inside,outside) dynamic
interface
CCNAS-ASA(config-network-object)#end
CCNAS-ASA#
```

Step 2b:

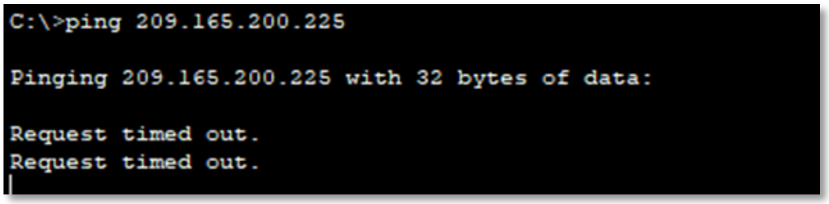


```
CCNAS-ASA#show run
: Saved
:
ASA Version 8.4(2)
!
hostname CCNAS-ASA
```



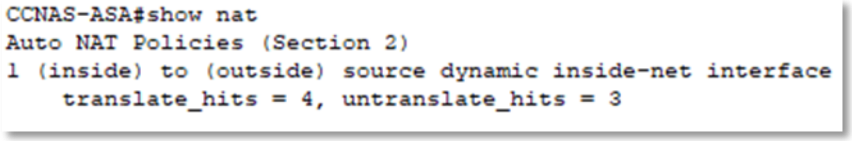
```
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
!
!
object network inside-net
 nat (inside,outside) dynamic interface
```

Step 2c:



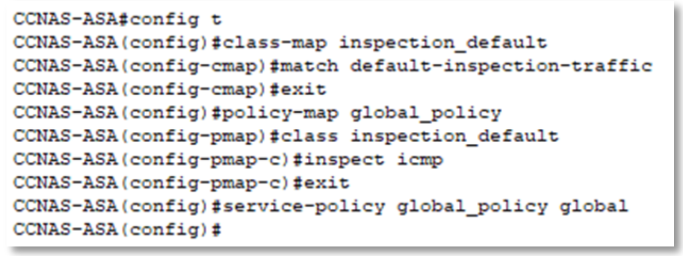
```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Request timed out.
Request timed out.
```

Step 2d:



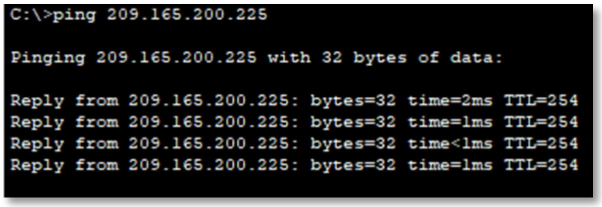
```
CCNAS-ASA#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 4, untranslate_hits = 3
```

Step 3a:



```
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)#
```

Step 3b:



```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=2ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
```

Part 4: Configure DHCP, AAA, and SSH

Step 1: Configure the ASA as a DHCP server.
a. Configure a DHCP address pool and enable it on the ASA inside interface.
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
b. (Optional) Specify the IP address of the DNS server to be given to clients.
CCNAS-ASA(config)# dhcpd dns 209.165.201.2 interface inside
c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).
CCNAS-ASA(config)# dhcpd enable inside
d. Change PC-B from a static IP address to a DHCP client, and verify that it receives IP addressing information. Troubleshoot, as necessary to resolve any problems.

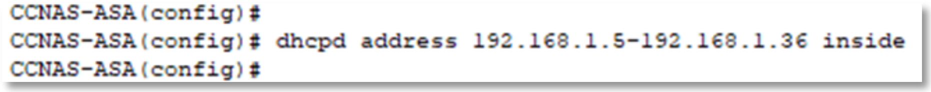
Step 2: Configure AAA to use the local database for authentication.
a. Define a local user named admin by entering the username command. Specify a password of adminpa55.
CCNAS-ASA(config)# username admin password adminpa55

b. Configure AAA to use the local ASA database for SSH user authentication.
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
Step 3: Configure remote access to the ASA.
The ASA can be configured to accept connections from a single host or a range of hosts on the inside or outside network. In this step, hosts from the outside network can only use SSH to communicate with the ASA. SSH sessions can be used to access the ASA from the inside network.

a. Generate an RSA key pair, which is required to support SSH connections. Because the ASA device has RSA keys already in place, enter no when prompted to replace them.
CCNAS-ASA(config)# crypto key generate rsa modulus 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>
b. Configure the ASA to allow SSH connections from any host on the inside network (192.168.1.0/24) and from the remote management host at the branch office (172.16.3.3) on the outside network. Set the SSH timeout to 10 minutes (the default is 5 minutes).
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
c. Establish an SSH session from PC-C to the ASA (209.165.200.226).
PC> ssh -l admin 209.165.200.226
d. Establish an SSH session from PC-B to the ASA (192.168.1.1)
PC> ssh -l admin 192.168.1.1

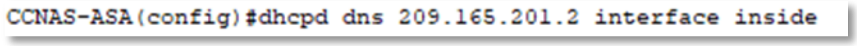
Insert screenshots here:

Step 1a:



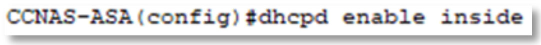
```
CCNAS-ASA(config)#
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
CCNAS-ASA(config)#
```

Step 1b:



```
CCNAS-ASA(config)#dhcpd dns 209.165.201.2 interface inside
```

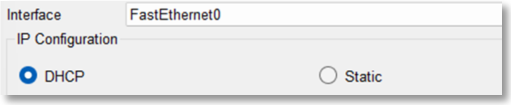
Step 1c:



```
CCNAS-ASA(config)#dhcpd enable inside
```

Step 1d:

PC-B > Desktop >

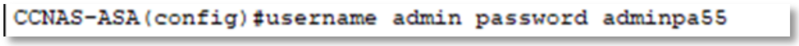


Interface: FastEthernet0

IP Configuration

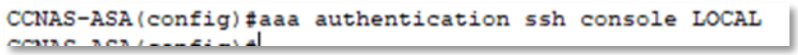
● DHCP ○ Static

Step 2a:



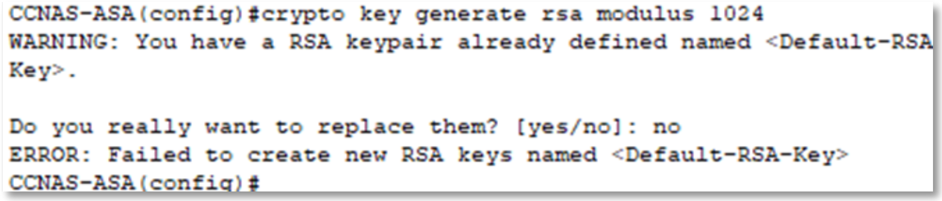
```
CCNAS-ASA(config)#username admin password adminpa55
```

Step2b:



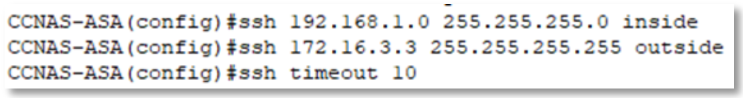
```
CCNAS-ASA(config)#aaa authentication ssh console LOCAL
```

Step 3a:



```
CCNAS-ASA(config)#crypto key generate rsa modulus 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)#
```

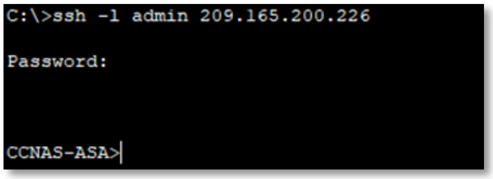
Step 3b:



```
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 3c (SSH session from PC-C to the ASA):

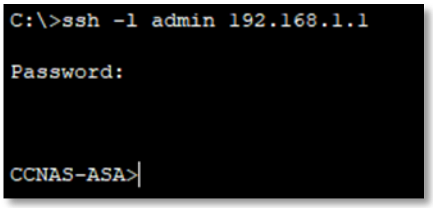
password: **adminpa55**



```
C:\>ssh -l admin 209.165.200.226

Password:


CCNAS-ASA>
```

Step 3d (SSH session from PC-B to ASA):

password: **adminpa55**



```
C:\>ssh -l admin 192.168.1.1

Password:


CCNAS-ASA>
```

Part 5: Configure a DMZ, Static NAT, and ACLs

R1 G0/0 and the ASA outside interface already use 209.165.200.225 and .226, respectively. You will use public address 209.165.200.227 and static NAT to provide address translation access to the server.

Step 1: Configure the DMZ interface VLAN 3 on the ASA.

a. Configure DMZ VLAN 3, which is where the public access web server will reside. Assign it IP address 192.168.2.1/24, name it dmz, and assign it a security level of 70. Because the server does not need to initiate communication with the inside users, disable forwarding to interface VLAN 1.

```
CCNAS-ASA(config)# interface 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
```

b. Assign ASA physical interface E0/2 to DMZ VLAN 3 and enable the interface.

```
CCNAS-ASA(config-if)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
```

c. Use the following verification commands to check your configurations:

1) Use the show interface ip brief command to display the status for all ASA interfaces.
2) Use the show ip address command to display the information for the Layer 3 VLAN interfaces.
3) Use the show switch vlan command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

Step 2: Configure static NAT to the DMZ server using a network object.

Configure a network object named dmz-server and assign it the static IP address of the DMZ server (192.168.2.3). While in object definition mode, use the nat command to specify that this object is used to translate a DMZ address to an outside address using static NAT, and specify a public translated address of 209.165.200.227.

```
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
```

Step 3: Configure an ACL to allow access to the DMZ server from the Internet.

Configure a named access list OUTSIDE-DMZ that permits the TCP protocol on port 80 from any external host to the internal IP address of the DMZ server. Apply the access list to the ASA outside interface in the "IN" direction.

```
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
```

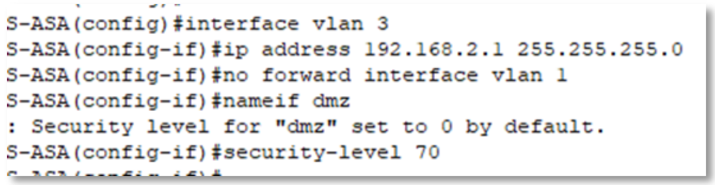
Note: Unlike IOS ACLs, the ASA ACL permit statement must permit access to the internal private DMZ address. External hosts access the server using its public static NAT address, the ASA translates it to the internal host IP address, and then applies the ACL.

Step 4: Test access to the DMZ server.

At the time this Packet Tracer activity was created, the ability to successfully test outside access to the DMZ web server was not in place; therefore, successful testing is not required

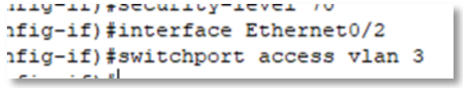
Insert screenshots here

Step 1a:



```
S-ASA(config)#interface vlan 3
S-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
S-ASA(config-if)#no forward interface vlan 1
S-ASA(config-if)#nameif dmz
: Security level for "dmz" set to 0 by default.
S-ASA(config-if)#security-level 70
```

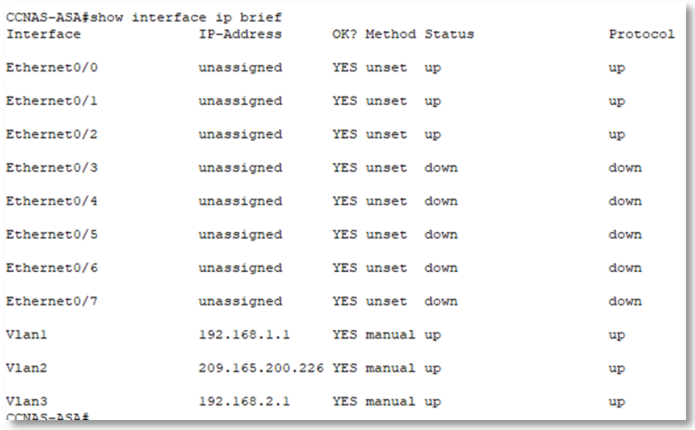
Step 1b:



```
nfig-if)#interface Ethernet0/2
nfig-if)#switchport access vlan 3
```

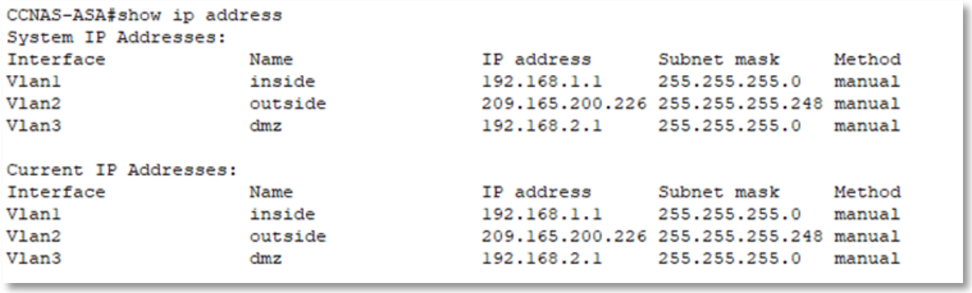
Step 1c:

1.



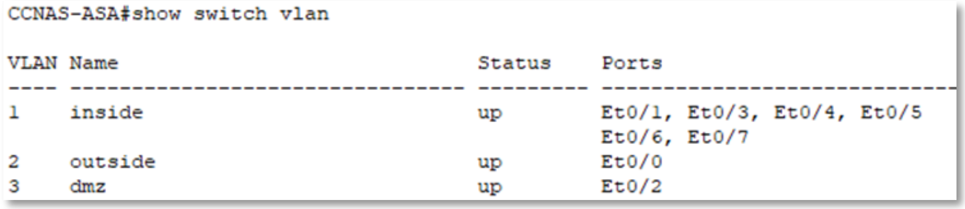
```
CCNAS-ASA#show interface ip brief
Interface              IP-Address      OK? Method Status                Protocol

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 manual up                    up

Vlan2                  209.165.200.226 YES manual up                    up

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

2.



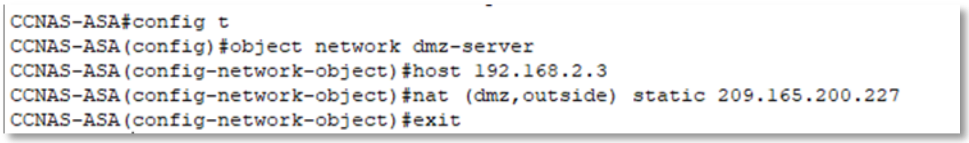
```
CCNAS-ASA#show ip address
System IP Addresses:
Interface              Name                   IP address      Subnet mask     Method
Vlan1                  inside                 192.168.1.1     255.255.255.0   manual
Vlan2                  outside                209.165.200.226 255.255.255.248 manual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

3.



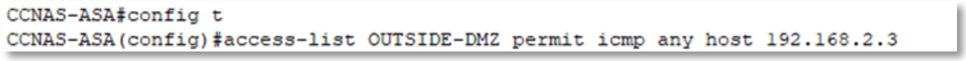
```
CCNAS-ASA#show switch vlan

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
```

Step 2:

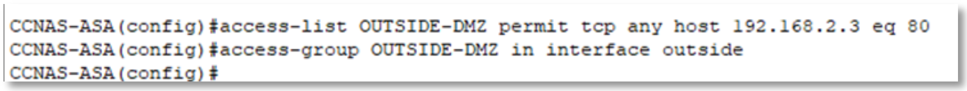


```
CCNAS-ASA#config t
CCNAS-ASA(config)#object network dmz-server
CCNAS-ASA(config-network-object)#host 192.168.2.3
CCNAS-ASA(config-network-object)#nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)#exit
```

Step 3:



```
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)#
```