



Lab 13

Configuring ASA Basic Settings and Firewall

Name: Syed Asghar Abbas Zaidi	Student ID: 07201
-------------------------------	-------------------

13.1 Objective

The Objectives of this lab are:

- 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

13.2 Background/Scenario

Your company has one location connected to an ISP. R1 represents a CPE (Customer Premises Equipment) 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 lab: 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**

13.3 Topology

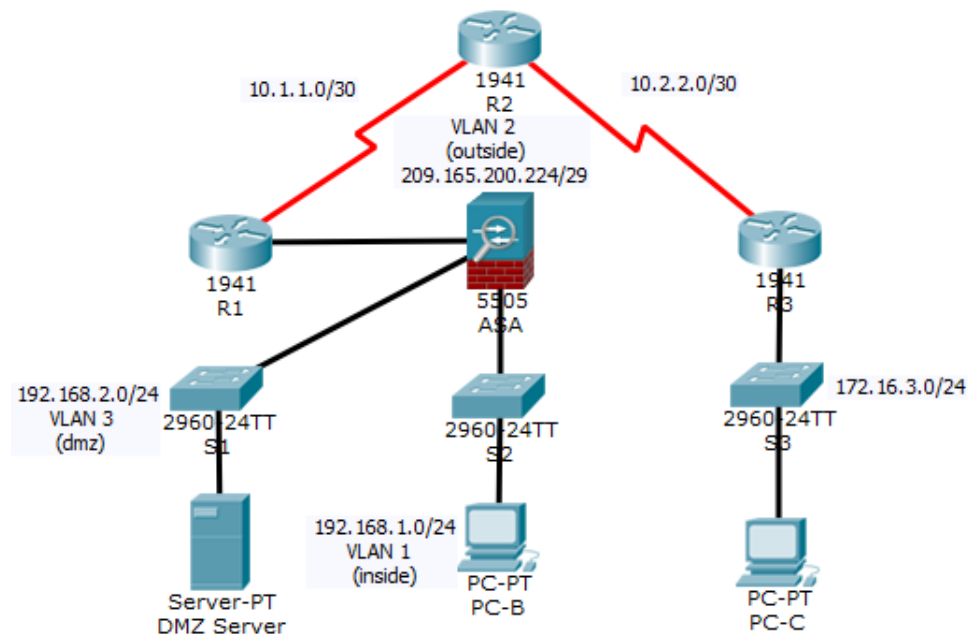


Figure 1: Topology

13.4 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

Figure 2: Addressing Table

Task 1: Verify Connectivity and Explore the ASA

Note: This Packet Tracer lab starts with 16% of the assessment items marked as complete. This is to ensure that you do not inadvertently change some ASA default values. For example, the default name of the inside interface is “inside” and should not be changed. Click Check Results to see which assessment items are already scored as correct.

1. Test 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.

Proof that I can ping all of my routers from PC-C

```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
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=14ms TTL=253
Reply from 10.1.1.1: bytes=32 time=10ms TTL=253
Reply from 10.1.1.1: bytes=32 time=7ms TTL=253
Reply from 10.1.1.1: bytes=32 time=10ms TTL=253

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 14ms, Average = 10ms

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=2ms TTL=255
Reply from 172.16.3.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=10ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
Reply from 10.1.1.2: bytes=32 time=9ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254

Ping statistics for 10.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 5ms
```

Proof that I can't ping my ASA, PC-B, DMZ



```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
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),

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.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3

Pinging 192.168.1.3 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.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

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



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface

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 8 minutes 52 seconds

Hardware: ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

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 000A.F30A.0601, irq 255
2: Ext: Ethernet0/1 : address is 000A.F30A.0602, irq 255
3: Ext: Ethernet0/2 : address is 000A.F30A.0603, irq 255
4: Ext: Ethernet0/3 : address is 000A.F30A.0604, irq 255
5: Ext: Ethernet0/4 : address is 000A.F30A.0605, irq 255
6: Ext: Ethernet0/5 : address is 000A.F30A.0606, irq 255
7: Ext: Ethernet0/6 : address is 000A.F30A.0607, irq 255
8: Ext: Ethernet0/7 : address is 000A.F30A.0608, 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
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual

This platform has a Base license.

Serial Number: JMX15361OFM
Running Permanent Activation Key: 0xENR31SHB 0xCOW63112 0xD9N7RDM6 0xN23CNH00 0x2Y1HETOV
Configuration register is 0x1
Configuration has not been modified since last system restart.
```

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.

a)

```
ciscoasa>en
Password:
Invalid password
Password:
Invalid password
Password:
ciscoasa#show file system
```

b)

```
ciscoasa#show file system

File Systems:

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

c)

```
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

128573440 bytes total (123001856 bytes free)
```

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

Tip: Many ASA CLI commands are similar to, if not the same, as those used with the Cisco IOS CLI. In addition, the process of moving between configuration modes and sub modes is essentially the same.

1. Configure the hostname and domain name
 - a. Configure the ASA hostname as **CCNAS-ASA**.
 - b. Configure the domain name as **ccnasecurity.com**.

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

2. Configure the enable mode password.



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

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

3. Set the date and time.

Use the **clock set** command to manually set the date and time (this step is not scored).

```
CCNAS-ASA(config)#clock set 10:48:00 Nov 14 2024
```

```
CCNAS-ASA(config)#show running-config
: Saved
:
ASA Version 8.4(2)
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password 57n/mTd4HwB/bqHS 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
 no ip address
!
interface Vlan2
 nameif outside
 security-level 0
 ip address dhcp
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
```



```
ssh timeout 5
!  
dhcpd auto_config outside  
!  
dhcpd enable inside
```

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 Task 5 of the lab.

- 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
```

```
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
```

```
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:
- i. Use the **show interface ip brief** command to display the status for all ASA interfaces. **Note:** This command is different from the IOS command **show ip interface brief**. If any of the physical or logical interfaces previously



configured are not up/up, troubleshoot as necessary before continuing. **Tip:** Most ASA **show** commands, including **ping**, **copy**, and others, can be issued from within any configuration mode prompt without the **do** command.

```
CCNAS-ASA(config)#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

- ii. Use the **show ip address** command to display the information for the Layer 3 VLAN interfaces

```
CCNAS-ASA(config)#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

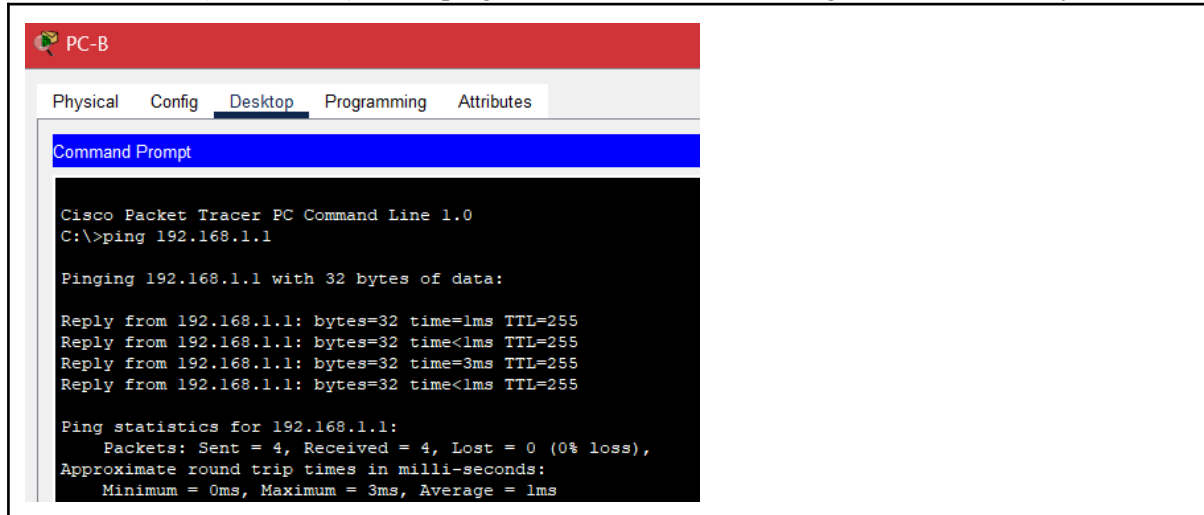
- iii. Use the **show switch vlan** command to display the inside and outside VLANs configured on the ASA and to display the assigned ports.

```
CCNAS-ASA(config)#show switch vlan
```

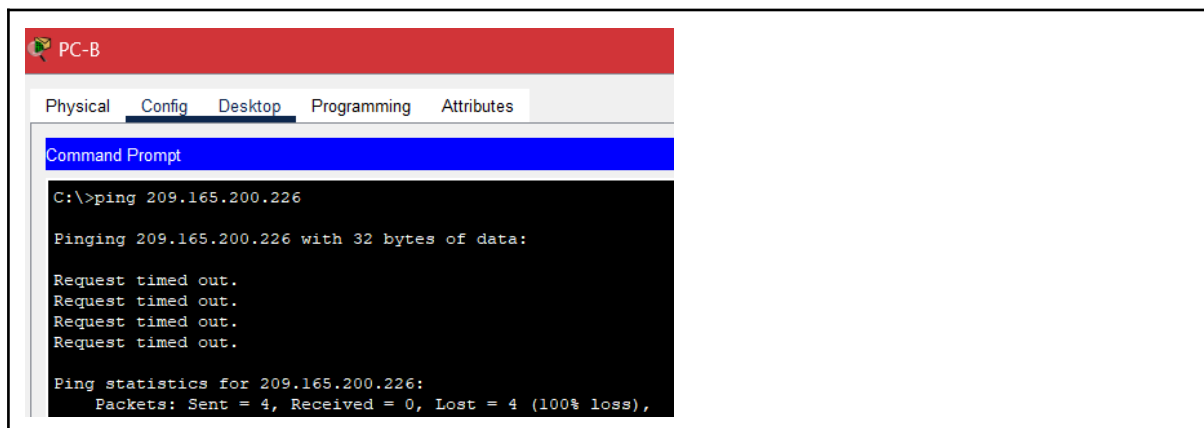
VLAN	Name	Status	Ports
1	inside	up	Et0/1, Et0/2, Et0/3, Et0/4 Et0/5, Et0/6, Et0/7
2	outside	up	Et0/0



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.



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

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
```



```
CCNAS-ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.255
```

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

```
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 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 209.165.200.255 to network 0.0.0.0

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
S*   0.0.0.0/0 [1/0] via 209.165.200.255
```

- c. Verify that the ASA can ping the R1 S0/0/0 IP address 10.1.1.1. If the ping is unsuccessful, troubleshoot as necessary.

```
CCNAS-ASA(config)#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 100 percent (5/5), round-trip min/avg/max = 0/4/8 ms
Verified.
```

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
```

```
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.

```
CCNAS-ASA#show run
: Saved
:
ASA Version 8.4(2)
!
hostname CCNAS-ASA
domain-name ccnasecurity.com
enable password 57n/mTd4HwB/bqHS 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
!
object network inside-net
  subnet 192.168.1.0 255.255.255.0
  nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 209.165.200.255 1
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd enable inside
!
!
!
!
```

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



```
PC-B
C:\>ping 209.165.200.255

Pinging 209.165.200.255 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.255:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- 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 task of the lab.

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

After one more ping testing:

```
CCNAS-ASA#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
   translate_hits = 8, untranslate_hits = 7
```

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
```

```
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. If the pings fail, troubleshoot your configurations.

```
PC-B
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<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=6ms TTL=254
Reply from 209.165.200.225: bytes=32 time<1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Task 4: Configure DHCP, AAA, and SSH

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=
```

```
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
```

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

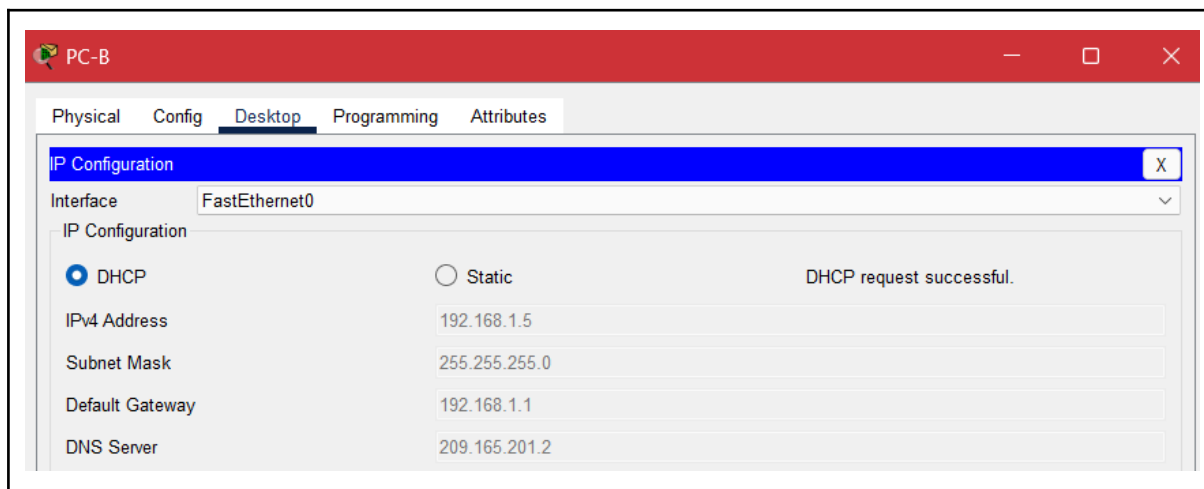


- c. Enable the DHCP daemon within the ASA to listen for DHCP client requests on the enabled interface (inside).

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

```
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.



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
```

```
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
```

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

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>
```

```
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
```

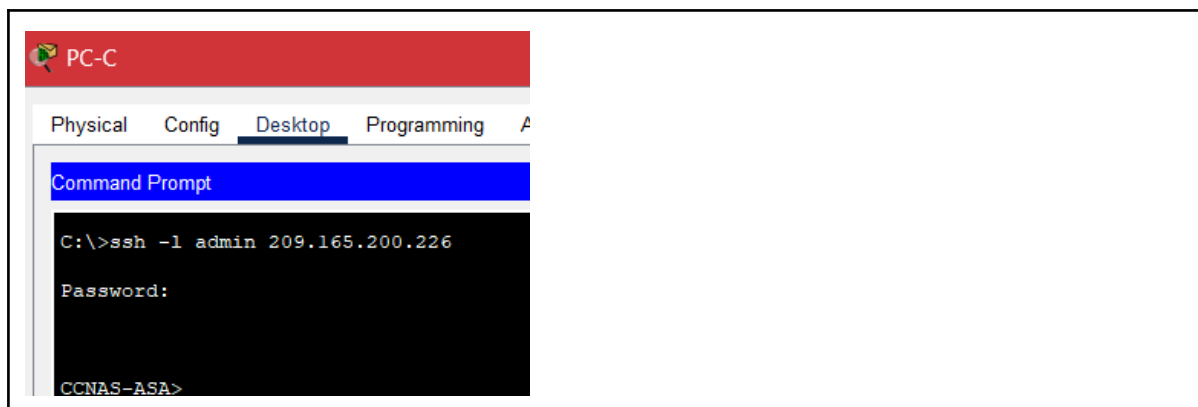
```
CCNAS-ASA(config)#ssh 192.168.1.0 255.255.255.0 inside
```

```
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). Troubleshoot if it is not successful

```
PC> ssh -l admin 209.165.200.226
```



- d. Establish an SSH session from PC-B to the ASA (192.168.1.1). Troubleshoot if it is not successful.

```
PC> ssh -l admin 192.168.1.1
```




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

Password:
% Login invalid

Password:

CCNAS-ASA>
```

Task 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.

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
```

```
CCNAS-ASA(config)#interface vlan 3
CCNAS-ASA(config-if)#ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)#nameif dmz
ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.
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
```

```
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:
- Use the **show interface ip brief** command to display the status for all ASA interfaces.

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

- Use the **show ip address** command to display the information for the Layer 3 VLAN interfaces.

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

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

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



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
```

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

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.

```
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
```

4. Test access to the DMZ server.

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

(As this was optional, I chose to not do it)

PROOF OF COMPLETION



Time Elapsed: 01:30:34

Score : 42/43

Item Count : 42/43

Component	Items/Total	Score
ACL	3/3	3/3
Ip	11/12	11/12
Other	24/24	24/24
Routing	1/1	1/1
Switching	3/3	3/3

PT Activity: 01:31:02

Packet Tracer - Configuring ASA Basic Settings and Firewall Using CLI

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

Time Elapsed: 01:31:02

Completion: 100%

☐ Top ☐ Dock [Check Results](#) [Back](#) 1/1 [Next](#)



Assessment Rubric

Lab 13

Configuring ASA Basic Settings and Firewall

Name: Syed Asghar Abbas Zaidi	Student ID: 07201
--------------------------------------	--------------------------

Points Distribution

Task No.	LR 2 Simulation	LR5 Results/Plots	LR9 Report
Task 1	10	10	
Task 2	10	5	
Task 3	10	5	
Task 4	10	5	
Task 5	10	5	
Total	/50	/30	/10
CLO Mapped	CLO 4	CLO 4	CLO4

Affective Domain Rubric		Points	CLO Mapped
AR 7	Report Submission	/10	CLO 4

CLO	Total Points	Points Obtained
4	90	
4	10	
Total	100	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.



Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3: Good Points 3	Level 4: Exemplary Points 4
LR2	Program/Code / Simulation Model/ Network Model	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR5	Results & Plots	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	Report	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.