

Índice:

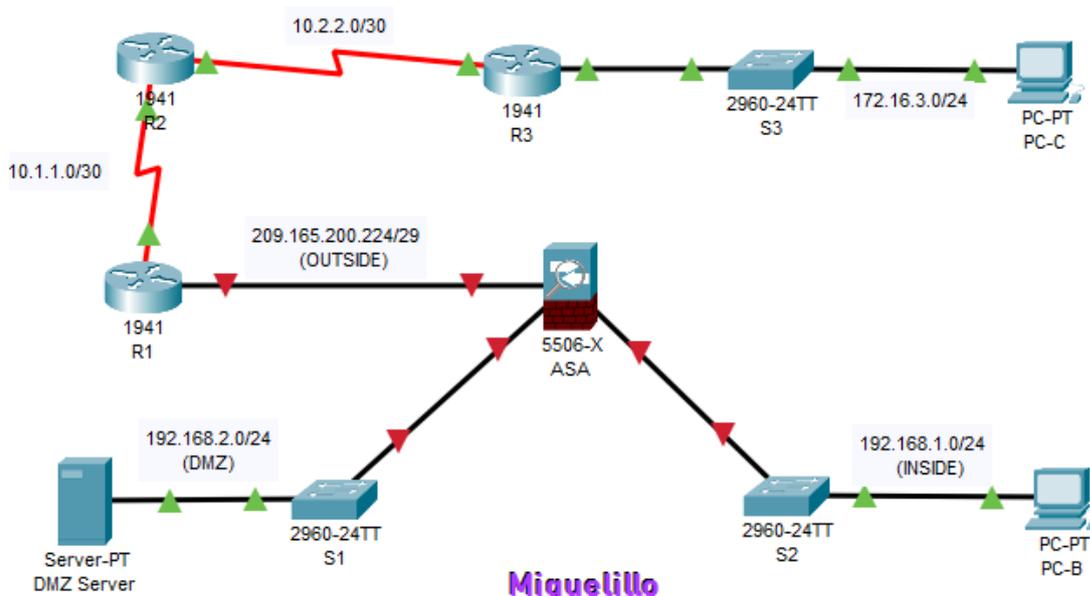
Ejercicio 1	2
a) Configure un ASA CISCO (servicios de red, enrutamiento y DMZ) mediante CLI en Packet Tracer. Laboratorio 21.7.5 del curso CISCO Network Security.	2

Ejercicio 1

a) Configure un ASA CISCO (servicios de red, enrutamiento y DMZ) mediante CLI en Packet Tracer. Laboratorio 21.7.5 del curso CISCO Network Security.

Solución:

Escenario:



Miguelillo

Parte 1: Verificar la conectividad y explorar la ASA

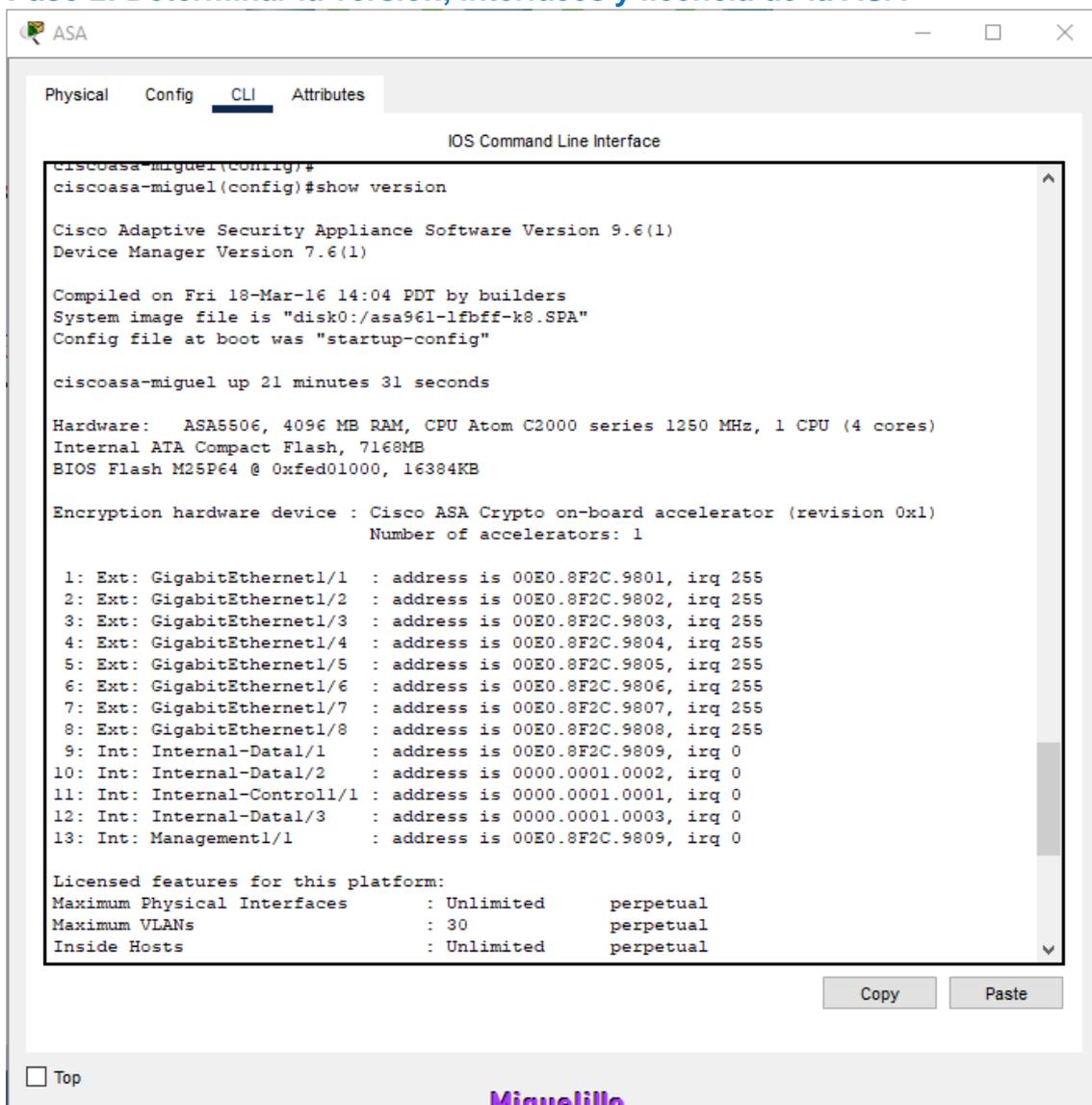
Paso 1: Verificar la conectividad

Pruebo conectividad Entre PC C y los rúters y pruebo con PC B no conecta ya que no está configurado el ASA

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-C	R3	ICMP	Green	0.000	N	0	(edit)	(delete)
	Successful	PC-C	R1	ICMP	Yellow	0.000	N	1	(edit)	(delete)
	Successful	PC-C	R2	ICMP	Green	0.000	N	2	(edit)	(delete)
	Failed	PC-B	R1	ICMP	Purple	0.000	N	3	(edit)	(delete)

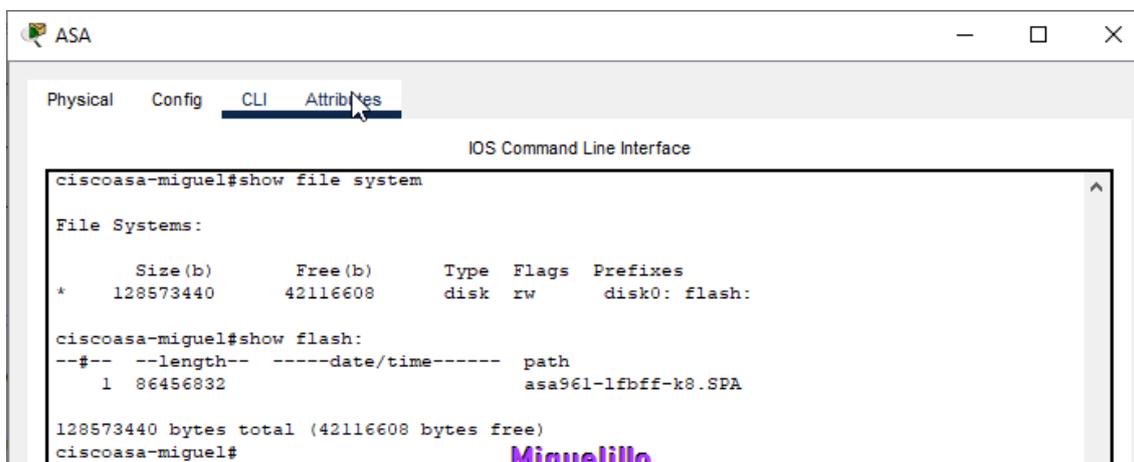
Miguelillo

Paso 2: Determinar la versión, interfaces y licencia de la ASA



Miguelillo

Paso 3: Determinar el sistema de archivos y el contenido de la memoria flash



Miguelillo

Parte 2: Configurar la configuración básica y niveles de seguridad de la interfaz de la ASA

Paso 1: Configurar el nombre de host y el nombre de dominio



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface
ciscoasa-miguel#configure terminal
ciscoasa-miguel(config)#hostname ASA-Miguel-SRI
ASA-Miguel-SRI(config)#domain-name netsec.com
ASA-Miguel-SRI(config)#
```

Miauelillo

Paso 2: Configurar la contraseña de modo privilegiado



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface
ASA-Miguel-SRI(config)#enable password inves
ASA-Miguel-SRI(config)#
```

Miauelillo

Paso 3: Establecer la fecha y la hora



```
ASA
Physical Config CLI Attributes
IOS Command Line Interface
ASA-Miguel-SRI(config)#clock set 17:56:10 March 08 2024
ASA-Miguel-SRI(config)#
```

Miauelillo

Paso 4: Configurar las interfaces INSIDE y OUTSIDE de la ASA

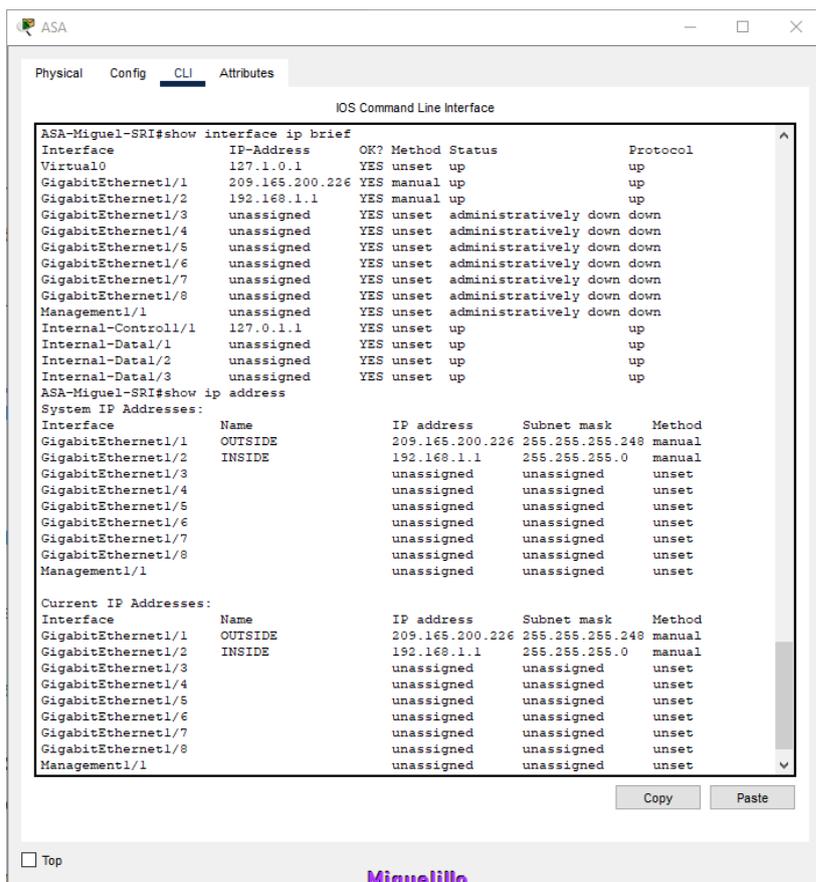


```
ASA
Physical Config CLI Attributes
IOS Command Line Interface
ASA-Miguel-SRI(config)#interface g1/1
ASA-Miguel-SRI(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
ASA-Miguel-SRI(config-if)#ip address 209.165.200.226 255.255.255.248
ASA-Miguel-SRI(config-if)#security-level 0
ASA-Miguel-SRI(config-if)#no shutdown

ASA-Miguel-SRI(config-if)#interface g1/2
ASA-Miguel-SRI(config-if)#nameif INSIDE
INFO: Security level for "INSIDE" set to 0 by default.
ASA-Miguel-SRI(config-if)#ip address 192.168.1.1 255.255.255.0
ASA-Miguel-SRI(config-if)#security-level 100
ASA-Miguel-SRI(config-if)#no shutdown
```

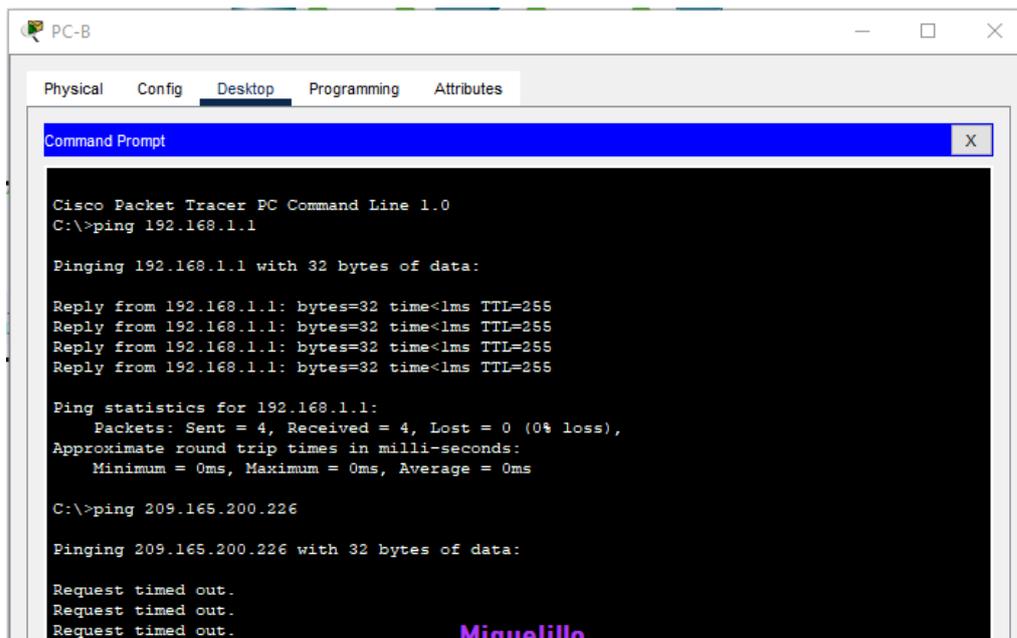
Miauelillo

Verificamos la configuración



Paso 5: Probar la conectividad a la ASA

A la interfaz G1/1(externo) y G1/2 (interior)



Parte 3: Configurar enrutamiento, traducción de direcciones e inspección de políticas usando la CLI

Paso 1: Configurar una ruta estática predeterminedada para la ASA

```

ASA-Miguel-SRI(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
ASA-Miguel-SRI(config)#
    
```

Paso 2: Configurar la traducción de direcciones utilizando PAT y objetos de red

```

ASA-Miguel-SRI(config)#object network INSIDE-NET
ASA-Miguel-SRI(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA-Miguel-SRI(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
ASA-Miguel-SRI(config-network-object)#exit
ASA-Miguel-SRI#
    
```

Podemos ver la configuración del nat con show runing

```

!
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface
!
route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225 1
!
    
```

Hacemos un de PC-B a R1 (tiene que fallar)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC-B	R1	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC-B	R1	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC-B	R1	ICMP		0.000	N	2	(edit)	(delete)
	Failed	PC-B	R1	ICMP		0.000	N	3	(edit)	(delete)

Vemos las traducciones del nat

```

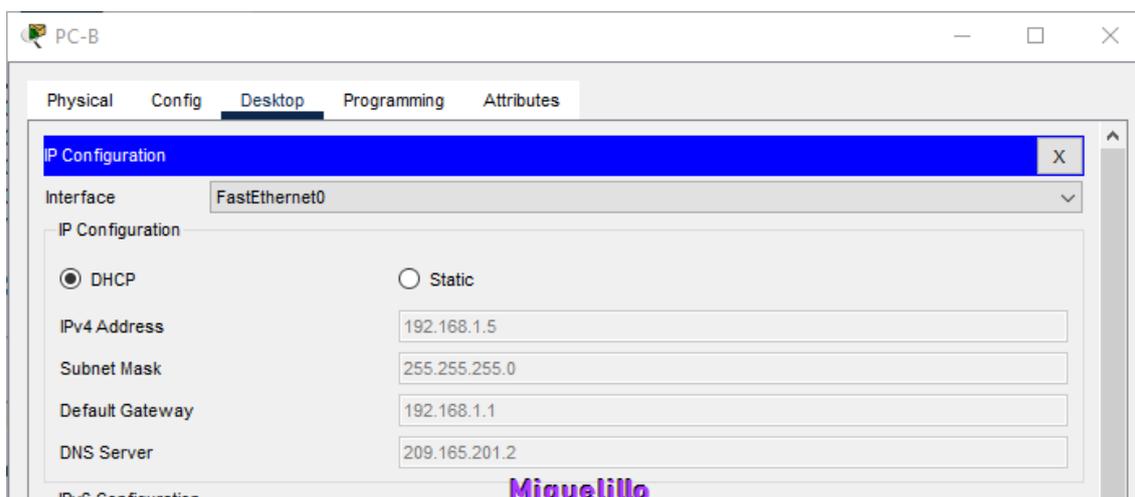
ASA-Miguel-SRI#show nat
Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
 translate_hits = 4, untranslate_hits = 3
    
```

Parte 4: Configurar DHCP, AAA y SSH

Paso 1: Configurar la ASA como servidor DHCP.



Probamos el cliente en DHCP

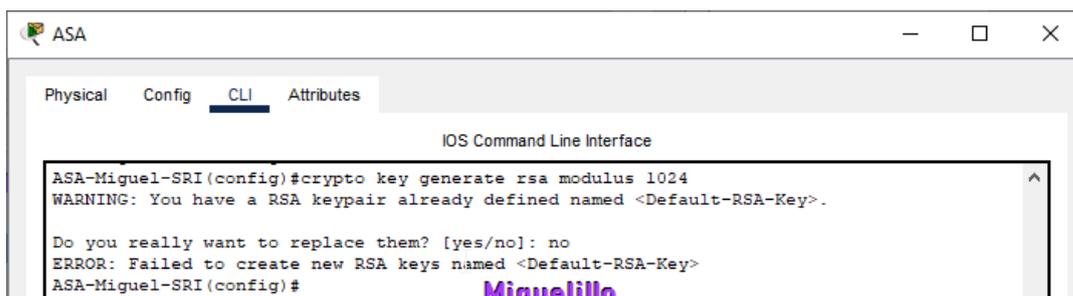


Paso 2: Configurar AAA para usar la base de datos local para la autenticación.



Paso 3: Configurar el acceso remoto a la ASA.

a. Generar un par de claves RSA, que se requiere para admitir conexiones SSH. Dado que el dispositivo ASA ya tiene claves RSA en su lugar, ingresar "no" cuando se le pregunte si se desean reemplazar.



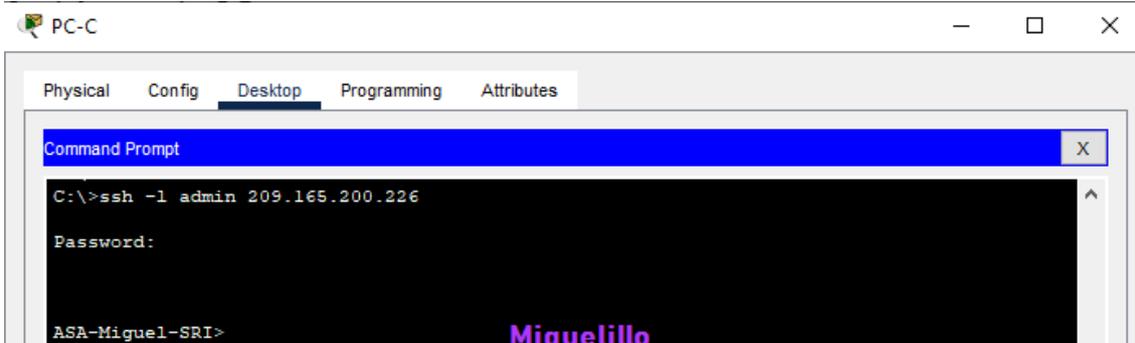
b. Configurar la ASA para permitir conexiones SSH desde cualquier host en la red INSIDE (192.168.1.0/24) y desde el host de administración remoto en la sucursal (172.16.3.3) en la red OUTSIDE. Establecer el tiempo de espera de SSH en 10 minutos



```

ASA-Miguel-SRI(config)#ssh 192.168.1.0 255.255.255.0 INSIDE
ASA-Miguel-SRI(config)#ssh 172.16.3.3 255.255.255.255 OUTSIDE
ASA-Miguel-SRI(config)#ssh timeout 10
ASA-Miguel-SRI(config)#
  
```

Prueba establecer una sesión SSH desde PC-C a la ASA (209.165.200.226)



```

C:\>ssh -l admin 209.165.200.226
Password:
ASA-Miguel-SRI>
  
```

Prueba establecer una sesión SSH desde PC-B a la ASA (192.168.1.1)



```

C:\>ssh -l admin 192.168.1.1
Password:
ASA-Miguel-SRI>
  
```

Parte 5: Configurar una DMZ, NAT estática y ACLs

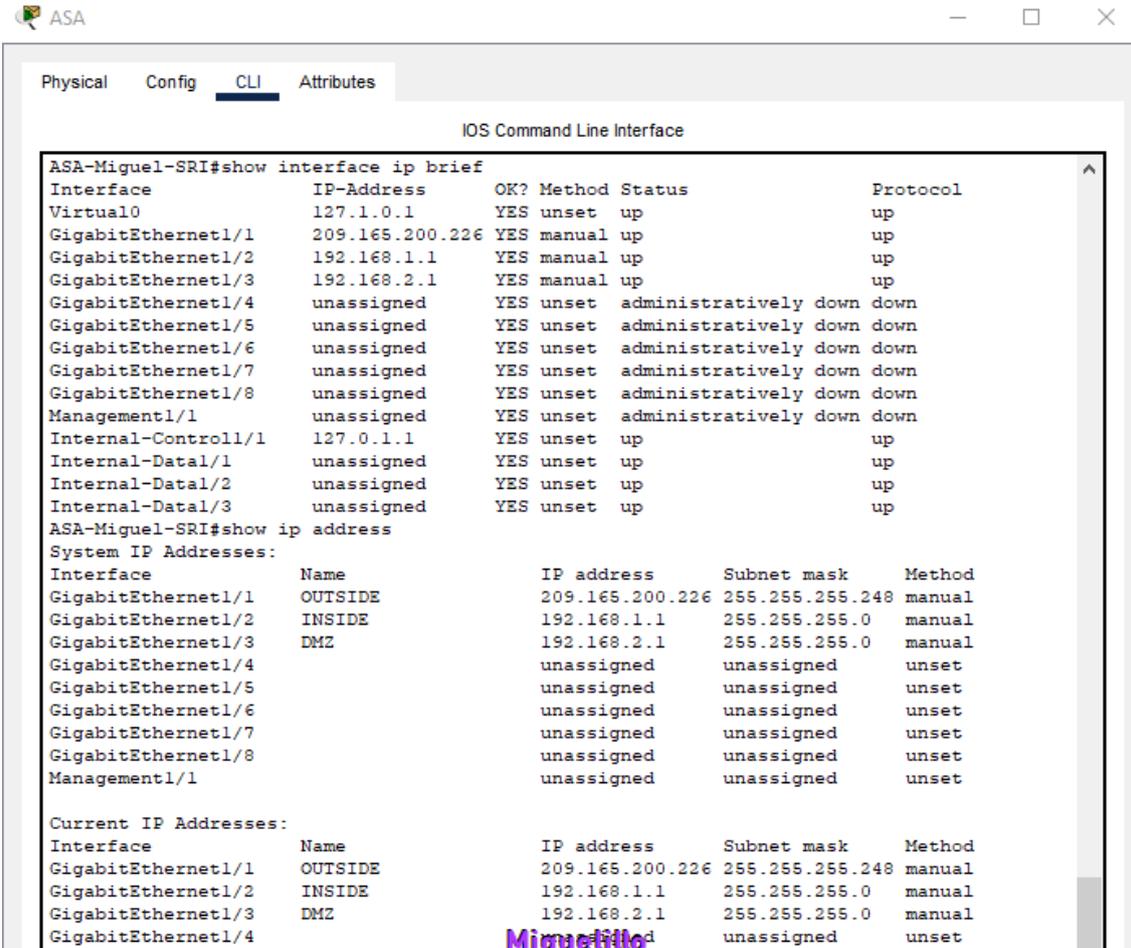
Paso 1: Configurar la interfaz DMZ VLAN 3 en la ASA.



```

ASA-Miguel-SRI(config)#interface g1/3
ASA-Miguel-SRI(config-if)#ip address 192.168.2.1 255.255.255.0
ASA-Miguel-SRI(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
ASA-Miguel-SRI(config-if)#security-level 70
ASA-Miguel-SRI(config-if)#no shutdown
  
```

Verificar la configuración



ASA-Miguel-SRI#show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Virtual0	127.1.0.1	YES	unset	up	up
GigabitEthernet1/1	209.165.200.226	YES	manual	up	up
GigabitEthernet1/2	192.168.1.1	YES	manual	up	up
GigabitEthernet1/3	192.168.2.1	YES	manual	up	up
GigabitEthernet1/4	unassigned	YES	unset	administratively down	down
GigabitEthernet1/5	unassigned	YES	unset	administratively down	down
GigabitEthernet1/6	unassigned	YES	unset	administratively down	down
GigabitEthernet1/7	unassigned	YES	unset	administratively down	down
GigabitEthernet1/8	unassigned	YES	unset	administratively down	down
Management1/1	unassigned	YES	unset	administratively down	down
Internal-Controll1/1	127.0.1.1	YES	unset	up	up
Internal-Datal1	unassigned	YES	unset	up	up
Internal-Datal2	unassigned	YES	unset	up	up
Internal-Datal3	unassigned	YES	unset	up	up

ASA-Miguel-SRI#show ip address

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet1/1	OUTSIDE	209.165.200.226	255.255.255.248	manual
GigabitEthernet1/2	INSIDE	192.168.1.1	255.255.255.0	manual
GigabitEthernet1/3	DMZ	192.168.2.1	255.255.255.0	manual
GigabitEthernet1/4		unassigned	unassigned	unset
GigabitEthernet1/5		unassigned	unassigned	unset
GigabitEthernet1/6		unassigned	unassigned	unset
GigabitEthernet1/7		unassigned	unassigned	unset
GigabitEthernet1/8		unassigned	unassigned	unset
Management1/1		unassigned	unassigned	unset

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet1/1	OUTSIDE	209.165.200.226	255.255.255.248	manual
GigabitEthernet1/2	INSIDE	192.168.1.1	255.255.255.0	manual
GigabitEthernet1/3	DMZ	192.168.2.1	255.255.255.0	manual
GigabitEthernet1/4		unassigned	unassigned	unset

Paso 2: Configurar NAT estática para el servidor DMZ usando un objeto de red.



ASA-Miguel-SRI(config)#object network DMZ-SERVER

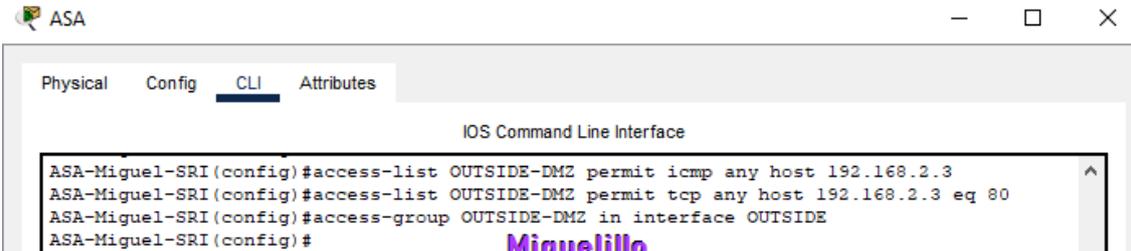
ASA-Miguel-SRI(config-network-object)#host 192.168.2.3

ASA-Miguel-SRI(config-network-object)#nat (DMZ,OUTSIDE) static 209.165.200.227

ASA-Miguel-SRI(config-network-object)#exit

ASA-Miguel-SRI#

Paso 3: Configurar una ACL para permitir el acceso al servidor DMZ desde Internet.



ASA-Miguel-SRI(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3

ASA-Miguel-SRI(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80

ASA-Miguel-SRI(config)#access-group OUTSIDE-DMZ in interface OUTSIDE

ASA-Miguel-SRI(config)#

Paso 4: Probar el acceso al servidor DMZ.

Desde un navegador web en PC-C, acceder al servidor DMZ

