Documentación Prueba Modulo 6

Estudiante: Sebastián Díaz San Martín

1. Realiza la implementación de Capa 3 según los requerimientos solicitados.

✓ La topología y equipos finales correspondiente se encuentran direccionado con IPv4.

✓ Implementar Protocolo de Enrutamiento de Estado de Enlace, usando área de backbone. Configurar interfaces pasivas correspondiente.

✓ Implementar autenticación de protocolo de enrutamiento a nivel de interfaz.

OSPF	
AREA	0
Authentication Key	Cisco.2025
Passive Interfaces	RB (Gig0/0) RC (Gig0/0)
Router-ID	RA 1.1.1.1 RB 2.2.2.2 RC 3.3.3.3
Cifrado	MD5

2. Realiza la implementación de Capa 2, además de los requerimientos de seguridad requeridos.

✓ Realizar configuración correspondiente para que las interfaces de los SW no queden asignadas en la VLAN1, además que estas estén apagadas.

✓ En interfaces correspondientes implementar seguridad de puerto por aprendizaje con un máximo de 2 direcciones MAC, además que en caso de exceder la interfaz debe desactivarse.

✓ En interfaces correspondientes, implementar mecanismos de estabilización de STP.

✓ En interfaces correspondiente, implementar control de tormenta para permitir solo el 15% de tráfico broadcast.

✓ En equipo apropiado implementar DHCP Snooping y mecanismo para evitar el ataque de hambruna, permitiendo solo 2 IP por minuto.

✓ Se aplica port-security máximo de aprendizaje 2 MAC y violation restric en los puertos de los switches con equipos finales.

Port-Security	
Equipo	Interfaz(ces)
SWA	Fa0/10
SWB	Fa0/10
SWC	Fa0/1

Mecanismos Estabilización STP	
Equipo	Interfaz(ces)
SWA	Fa0/10
SWB	Fa0/10
SWC	Fa0/1

Storm-Control	
Equipo	Interfaz(ces)
SWA	G0/2
SWB	G0/2
SWC	Fa0/20

DHCP Snooping limit rate	
Equipo	Interfaz(ces)
SWB	Fa0/10

3. Realiza la implementación de Seguridad, configurando firewall ASA y VPN de Acceso remoto según requerimientos.

✓ En Firewall ASA, definir los nombres de las zonas. Los niveles de seguridad serán los siguientes: Para la Zona Inside el nivel de seguridad será el máximo permitido, para la DMZ será el 40% de la zona Inside, y para la zona Outside será la mitad de la DMZ.

Zonas ASA	
Interfaz	Configuracion
Gig 1/1	Zona Outside Security Level 20.0
Gig 1/2	Zona DMZ Security Level 40.0
Gig 1/3	Zona Inside Security Level 100.0

- ✓ Implementar pool de DHCP para proporcionar IP de forma dinámica a zona inside. El número máximo de IPv4 serán 16.

DHCP INSIDE	
Gig 1/3 Zona INSIDE	DHCP entregando las IP's 172.16.15.5-172.16.15.20

- ✓ Implementar PAT para que Inside pueda salir por zona Outside, no olvidando implementar MPF para permitir el paso del ICMP.

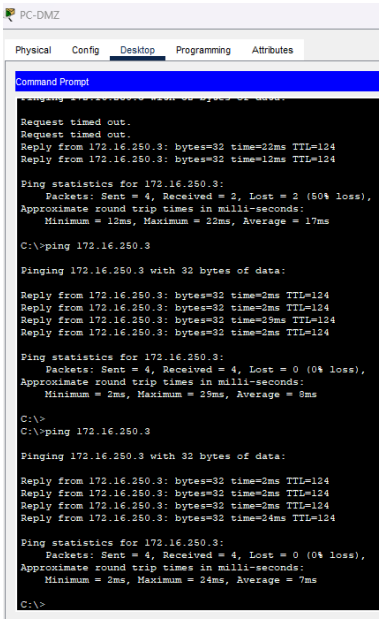
Se aplica NAT dinámico en interfaz INSIDE

```
object network INSIDE-NET
 subnet 172.16.15.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface
!
```

- ✓ Permitir que en PC-DMZ pueda salir por NAT Estático hacia Outside. Utilizar IP a elección de dicho segmento de red. Realizar configuraciones pertinentes para permitir el retorno del ICMP hacia la DMZ.

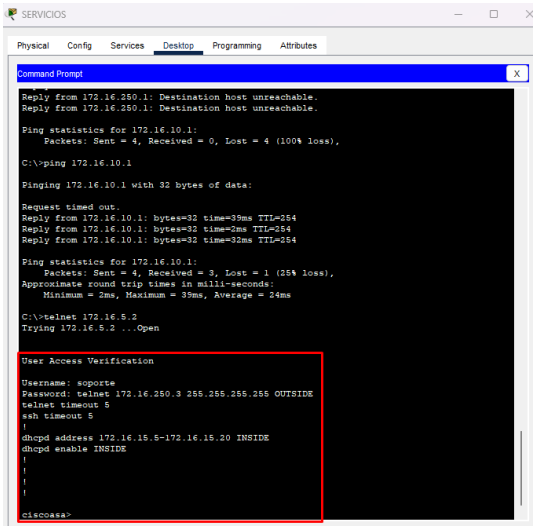
NAT Estático PC DMZ a OUTSIDE	
PC-DMZ	172.16.20.3 se traduce en 172.16.5.3

```
object network DMZ-SERVER
 host 172.16.20.3
 nat (DMZ,OUTSIDE) static 172.16.5.3
```



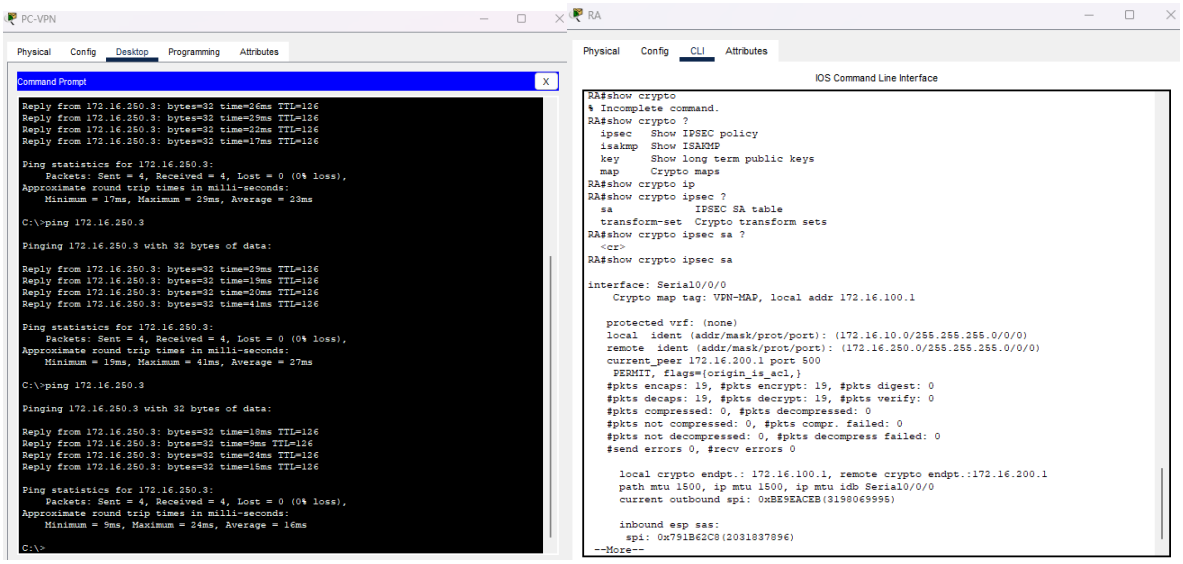
✓ Permitir que el servidor SERVICIOS pueda acceder por Telnet hacia ASA.

```
telnet 172.16.250.3 255.255.255.255 OUTSIDE
telnet timeout 5
```



✓ Implementar VPN S2S para que PC pueda llegar al servidor SERVICIOS mediante VPN. Debe comprobar que el PC establezca conexión por VPN y la conectividad sea mediante la VPN y no por el protocolo de enrutamiento.

VPN S2S	
Fase 1	
Encryption	AES-256
Authentication	Pre-share
Diffie-Hellman Group	5
PSK	vpnpc
Fase 2	
Match addres	ACL extended 110
Transform-Set	Esp-aes esp-sha-hmac



4. Implementa una política de control de acceso para la red de la empresa Desafio Latam en donde esté relacionado con el uso eficiente de la VPN de Acceso Remoto, así como la conectividad limitada que existirá desde Internet hacia la red de la empresa a través del firewall ASA.

```
access-list OUTSIDE-DMZ extended permit tcp any host 172.16.20.3 eq www
access-list OUTSIDE-DMZ extended permit icmp any host 172.16.20.3
access-list OUTSIDE-INSIDE extended permit icmp any 172.16.15.0 255.255.255.0
```