Prueba de módulo 6

Informe de configuración realizada en topología

Elaborado por Esteban Aranda, para el módulo Soluciones de Seguridad en redes corporativas

Bootcamp Especialidad Seguridad en Redes de Datos, G1 – BOTIC-SOFOF-24-28-05-0006

27 de agosto de 2025

El presente informe tiene como finalidad resumir toda la configuración realizada en la topología propuesta por la empresa Desafío Latam, siguiendo los requisitos solicitados, poniendo especial atención en la conectividad y la seguridad de la red.

Para ciertos requisitos se modificó el cumplimiento del objetivo debido a distintos percances que se encontraron, que se informarán a continuación:

- **Cambio de Firewall modelo 5505 por modelo 5506-X**:

Se realiza el cambio del Firewall de la topología debido a que presentaba limitaciones al momento de definir las zonas INSIDE, OUTSIDE y DMZ; solo permite el uso de dos VLANs a las cuales se les puede configurar un *nameif*, quedando una que no se puede configurar (DMZ Restricted). Si bien la topología se realizó con el modelo 5506-X, se puede quitar la restricción del modelo 5505 aplicando una llave de activación, que se puede obtener aplicando el siguiente comando en CLI:

```
ciscoasa#show version
```

La llave de activación tiene el siguiente formato:

```
0x1321CF73 0xFCB68F7E 0x801111DC 0xB554E4A4 0x0F3E008D
```

Luego, para aplicar la configuración se aplica el siguiente comando:

```
ciscoasa#activation-key 0x1321CF73 0xFCB68F7E 0x801111DC 0xB554E4A4 0x0F3E008D
```

Con esta configuración el Firewall ASA 5505 permite utilizar 20 VLANs, sin restricción de DMZ.

- **Cambio de routers RA y RC por modelo 2811**:

Se cambian los modelos de la topología (2911) por el modelo 2811 debido a que los originales no permitían la configuración de VPN. Si bien la topología se configuró con RA y RC con el modelo 2811, se puede activar la configuración de seguridad mediante la activación de una licencia de seguridad. El comando para 2911 es el siguiente:

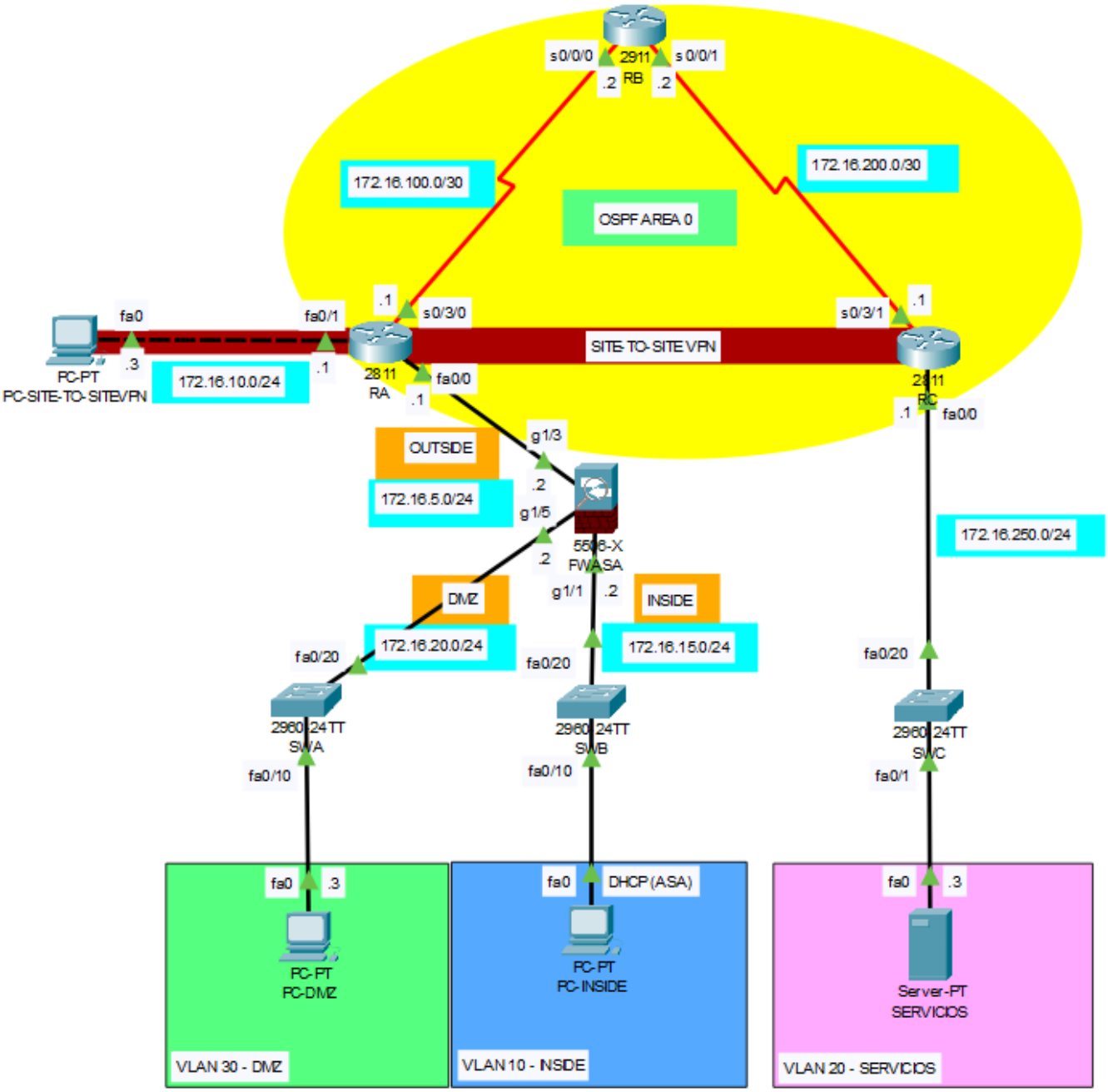
```
Router(config)#license boot module c2900 technology-package securityk9
```

1. Resumen de la topología

1.1 Direccionamiento IP

Dispositivo	Interface	Identificador de red	IP address	Máscara	Gateway	Conectado a
PC-DMZ	fa0	172.16.20.0	.3	/24	.2	SWA
PC-INSIDE	fa0	172.16.15.0	DHCP	/24	.2	SWB
SERVICIOS	fa0	172.16.250.0	.3	/24	.1	SWC
PC-Site-To-Site-VPN	fa0	172.16.10.0	.3	/24	.1	RA
SWA	fa0/10	n/a	n/a	n/a	n/a	PC-DMZ
	fa0/20	n/a	n/a	n/a	n/a	FWASA
SWB	fa0/10	n/a	n/a	n/a	n/a	PC-INSIDE
	fa0/20	n/a	n/a	n/a	n/a	FWASA
SWC	fa0/1	n/a	n/a	n/a	n/a	SERVICIOS
	fa0/20	n/a	n/a	n/a	n/a	RC
FWASA	g1/1	172.16.15.0	.2	/24	n/a	SWB
	g1/3	172.16.5.0	.2 (**NAT-DMZ: .7**)	/24	n/a	RA
	g1/5	172.16.20.0	.2	/24	n/a	SWA
RA	fa0/0	172.16.5.0	.1	/24	n/a	FWASA
	fa0/1	172.16.10.0	.1	/24	n/a	PC-Site-To-Site-VPN
	s0/3/0	172.16.100.0	.1	/30	n/a	RB
RB	s0/0/0	172.16.100.0	.2	/30	n/a	RA
	s0/0/1	172.16.200.0	.2	/30	n/a	RC
RC	s0/3/1	172.16.200.0	.1	/30	n/a	RB
	fa0/0	172.16.250.0	.1	/24	n/a	SWC

1.2 Topología configurada



2. Configuraciones realizadas en la red

2.1 Configuración switches capa 2 (SWA, SWB, SWC):

En cada switch se configuraron:

- VLANs correspondientes a la red LAN que gestionan.
- Medidas de seguridad y estabilización (VLAN BlackHole, apagado de puertos en desuso, BPDUGuard, STP, Storm-control).

2.1.1 SWA

```
   #Creación de VLAN y definición de nombre:
SWA(config)#vlan 30
SWA(config-vlan)#name DMZ
…
   #Tránsito de la VLAN por las interfaces de interés:
SWA(config)#inter fa0/10
SWA(config-if)#switchport mode access
SWA(config-if)#switchport access vlan 30
SWA(config-if)#switchport nonegotiate
…
SWA(config)#inter fa0/20
SWA(config-if)#switchport mode access
SWA(config-if)#switchport access vlan 30
…
   #Configuración de VLAN Blackhole, apagado de puertos, estabilización y seguridad:
SWA(config)#vlan 999
SWA(config-vlan)#name BLACKHOLE
…
SWA(config)#inter range fa0/1-9, fa0/11-19, fa0/21-24
SWA(config-if-range)#switchport mode access
SWA(config-if-range)#switchport access vlan 999
SWA(config-if-range)#switchport nonegotiate
SWA(config-if-range)#shutdown
…
SWA(config)#inter range fa0/1-19, fa0/21-24
SWA(config-if-range)#spanning-tree bpduguard enable
…
SWA(config)#inter fa0/10
SWA(config-if)#spanning-tree portfast
…
SWA(config)#inter fa0/10
SWA(config-if)#switchport port-security
SWA(config-if)#switchport port-security maximum 2
SWA(config-if)#switchport port-security violation shutdown
SWA(config-if)#switchport port-security mac-address sticky
…
SWA(config)#inter fa0/10
SWA(config-if)#storm-control broadcast level 15
```

2.1.2 SWB

```
   #Creación de VLAN y definición de nombre:
SWB(config)#vlan 10
SWB(config-vlan)#name INSIDE
…
   #Tránsito de la VLAN por las interfaces de interés:
SWB(config)#inter fa0/10
SWB(config-if)#switchport mode access
SWB(config-if)#switchport access vlan 10
SWB(config-if)#switchport nonegotiate
…
SWB(config)#inter fa0/20
SWB(config-if)#switchport mode access
SWB(config-if)#switchport access vlan 10
…
   #Configuración de VLAN Blackhole, apagado de puertos, estabilización y seguridad:
SWB(config)#vlan 999
SWB(config-vlan)#name BLACKHOLE
SWB(config)#inter range fa0/1-9, fa0/11-19, fa0/21-24
SWB(config-if-range)#switchport mode access
SWB(config-if-range)#switchport access vlan 999
SWB(config-if-range)#switchport nonegotiate
SWB(config-if-range)#shutdown
…
SWB(config)#inter range fa0/1-19, fa0/21-24
SWB(config-if-range)#spanning-tree bpduguard enable
…
SWB(config)#inter fa0/10
SWB(config-if)#spanning-tree portfast
…
SWB(config)#inter fa0/10
SWB(config-if)#switchport port-security
SWB(config-if)#switchport port-security maximum 2
SWB(config-if)#switchport port-security violation shutdown
SWB(config-if)#switchport port-security mac-address sticky
…
SWB(config)#inter fa0/10
SWB(config-if)#storm-control broadcast level 15
…
   #DHCP Snooping:
SWB(config)#ip dhcp snooping
SWB(config)#ip dhcp snooping vlan 10
SWB(config)#inter fa0/20
SWB(config-if)#ip dhcp snooping trust
SWB(config)#inter fa0/10
SWB(config-if)#ip dhcp snooping limit rate 2
```

2.1.3 SWC

```
   #Creación de VLAN y definición de nombre:
SWC(config)#vlan 20
SWC(config-vlan)#name SERVICIOS
…
   #Tránsito de la VLAN por las interfaces de interés:
SWC(config)#inter fa0/1
SWC(config-if)#switchport mode access
SWC(config-if)#switchport access vlan 20
SWC(config-if)#switchport nonegotiate
…
SWC(config)#inter fa0/20
SWC(config-if)#switchport mode access
SWC(config-if)#switchport access vlan 20
…
   #Configuración de VLAN Blackhole, apagado de puertos, estabilización y seguridad:
SWC(config)#vlan 999
SWC(config-vlan)#name BLACKHOLE
…
SWC(config)#inter range fa0/2-19, fa0/21-24
SWC(config-if-range)#switchport mode access
SWC(config-if-range)#switchport access vlan 999
SWC(config-if-range)#switchport nonegotiate
SWC(config-if-range)#shutdown
…
SWC(config)#inter range fa0/1-24
SWC(config-if-range)#spanning-tree bpduguard enable
…
SWC(config)#inter fa0/1
SWC(config-if)#spanning-tree portfast
…
SWC(config)#inter fa0/1
SWC(config-if)#switchport port-security
SWC(config-if)#switchport port-security maximum 2
SWC(config-if)#switchport port-security violation shutdown
SWC(config-if)#switchport port-security mac-address sticky
…
SWC(config)#inter fa0/1
SWC(config-if)#storm-control broadcast level 15
```

Nota: Se decide activar BPDUGuard en todos los puertos (incluso el conectado con RC), ya que por efectos del ejercicio, la conexión entre SWC y RC es del tipo *access*, por lo que la configuración aplicada le dará un grado más de seguridad a la conexión. Sin embargo, si se requiere configurar más VLANs en los switches, se debe desactivar esta configuración en las interfaces objetivo para evitar problemas de conectividad.

2.2 Configuración de routers y Firewall ASA

En routers se configuró:

- Protocolo OSPFv2
- VPN Site-To-Site (entre RA y RC, para conectar “PC-Site-To-SiteVPN” con Servidor “SERVICIOS”)

2.2.1 RA

```
#Configuración OSPF:
RA(config)#router ospf 507
RA(config-router)#router-id 1.1.1.1
RA(config-router)#network 172.16.10.0 255.255.255.0 area 0
RA(config-router)#network 172.16.5.0 255.255.255.0 area 0
RA(config-router)#network 172.16.100.0 255.255.255.252 area 0
RA(config-router)#passive-interface g0/0
RA(config-router)#passive-interface g0/2
…
RA(config)#inter s0/0/0
RA(config-if)#ip ospf authentication message-digest
RA(config-if)#ip ospf message-digest-key 7 md5 OSPFPruebaM7
…
#Configuración VPN Site-To-Site:
RA(config)#access-list 107 permit ip 172.16.10.0 0.0.0.255 172.16.250.0 0.0.0.255
RA(config)#crypto isakmp policy 10
RA(config-isakmp)#encryption aes 256
RA(config-isakmp)#authentication pre-share
RA(config-isakmp)#group 5
…
RA(config)#crypto isakmp key vpn_ra_rc address 172.16.200.1
RA(config)#crypto ipsec transform-set SET-VPN esp-aes esp-sha-hmac
RA(config)#crypto map MAPA-VPN 10 ipsec-isakmp
RA(config-crypto-map)#description VPN_RA-RC
RA(config-crypto-map)#set peer 172.16.200.1
RA(config-crypto-map)#set transform-set SET-VPN
RA(config-crypto-map)#match address 107
…
RA(config)#int s0/3/0
RA(config-if)#crypto map MAPA-VPN
```

2.2.2 RB

```
#Configuración OSPF:
RB(config)#router ospf 507
RB(config-router)#router-id 2.2.2.2
RB(config-router)#network 172.16.100.0 255.255.255.252 area 0
RB(config-router)#network 172.16.200.0 255.255.255.252 area 0
…
RB(config)#inter s0/0/0
RB(config-if)#ip ospf authentication message-digest
RB(config-if)#ip ospf message-digest-key 7 md5 OSPFPruebaM7
```

2.2.3 RC

```
#Configuración OSPF:
RC(config)#router ospf 507
RC(config-router)#router-id 3.3.3.3
RC(config-router)#network 172.16.200.0 255.255.255.252 area 0
RC(config-router)#network 172.16.250.0 255.255.255.0 area 0
RC(config-router)#passive-interface g0/0
…
RC(config)#inter s0/0/1
RC(config-if)#ip ospf authentication message-digest
RC(config-if)#ip ospf message-digest-key 7 md5 OSPFPruebaM7
…
#Configuración VPN Site-To-Site:
RC(config)#access-list 107 permit ip 172.16.250.0 0.0.0.255 172.16.10.0 0.0.0.255
RC(config)#crypto isakmp policy 10
RC(config-isakmp)#encryption aes 256
RC(config-isakmp)#authentication pre-share
RC(config-isakmp)#group 5
…
RC(config)#crypto isakmp key vpn_ra_rc address 172.16.100.1
RC(config)#crypto ipsec transform-set SET-VPN esp-aes esp-sha-hmac
RC(config)#crypto map MAPA-VPN 10 ipsec-isakmp
RC(config-crypto-map)#description VPN_RC-RA
RC(config-crypto-map)#set peer 172.16.100.1
RC(config-crypto-map)#set transform-set SET-VPN
RC(config-crypto-map)#match address 107
…
RC(config)#inter s0/3/1
RC(config-if)#crypto map MAPA-VPN
```

Nota: En la topología entregada, los routers Cisco 2911 no soportan configuración de VPN. Por ello, se reemplazaron los routers RA y RC por los modelos 2811, los que sí soportan configuración de VPN del tipo Site-To-Site, para poder cumplir con los requisitos de la prueba. Más información en Página 2.

2.2.4 Firewall ASA

En el Firewall ASA se configuraron:

- Zonas: INSIDE, OUTSIDE, DMZ
- Nivel de seguridad acorde a requerimientos
- DHCP (para INSIDE)
- NAT y PAT según requerimientos
- MPF (habilitar inspecciones)
- Acceso remoto Telnet (desde Servidor SERVICIOS)

```
#Definición de nombre para ASA:
ciscoasa(config)#hostname FWASA
…
```

```
   #Creación de Zonas y direccionamiento:
FWASA(config)#inter g1/1
FWASA(config-if)#nameif INSIDE
FWASA(config-if)#security-level 100
FWASA(config-if)#ip address 172.16.15.2 255.255.255.0
FWASA(config-if)#no shutdown
…
FWASA(config)#inter g1/5
FWASA(config-if)#nameif DMZ
FWASA(config-if)#security-level 40
FWASA(config-if)#ip address 172.16.20.2 255.255.255.0
FWASA(config-if)#no shutdown
…
FWASA(config)#inter g1/3
FWASA(config-if)#nameif OUTSIDE
FWASA(config-if)#security-level 20
FWASA(config-if)#ip address 172.16.5.2 255.255.255.0
FWASA(config-if)#no shutdown
…
   #Configuración DHCP para INSIDE:
FWASA(config)#dhcpd address 172.16.15.1-172.16.15.16 INSIDE
FWASA(config)#dhcpd option 3 ip 172.16.15.2
FWASA(config)#dhcpd dns 8.8.8.8
FWASA(config)#dhcpd enable INSIDE
…
   #Configuración PAT (salida INSIDE-OUTSIDE):
FWASA(config)#object network VLAN10-OUTSIDE
FWASA(config-network-object)#subnet 172.16.15.0 255.255.255.0
FWASA(config-network-object)#nat (INSIDE,OUTSIDE) dynamic interface
…
   #Configuración NAT estático (salida DMZ-OUTSIDE):
FWASA(config)#object network NAT_DMZ-OUTSIDE
FWASA(config-network-object)#host 172.16.20.3
FWASA(config-network-object)#nat (DMZ,OUTSIDE) static 172.16.5.7
…
   #Habilitación de inspecciones (MPF):
FWASA(config)#policy-map global_policy
FWASA(config-pmap)#class inspection_default
FWASA(config-pmap-c)#inspect icmp
FWASA(config-pmap-c)#inspect dns
FWASA(config-pmap-c)#inspect ftp
FWASA(config-pmap-c)#inspect http
…
   #Configuración de Telntet (acceso remoto a ASA a través de SERVICIOS):
FWASA(config)#enable password ciscoenpa57 level 15
FWASA(config)#username Admin password PruebaM7
FWASA(config)#telnet 172.16.250.3 255.255.255.255 OUTSIDE
FWASA(config)#aaa authentication telnet console LOCAL
…
```

```
#Configuración de ACL que permite protocolo ICMP desde DMZ hacia INSIDE
FWASA(config)#access-list ICMP-DMZ-INSIDE extended permit icmp 172.16.20.3 255.255.255.255
172.16.15.0 255.255.255.0
FWASA(config)#access-group ICMP-DMZ-INSIDE in interface DMZ
```

Nota: El Firewall de la topología, modelo 5505, no tiene los permisos necesarios para poder configurar tres zonas como lo solicitan en el listado de requerimientos. Esto sucede porque el Firewall 5505 solo permite la configuración de dos zonas que tengan configurado un *nameif*; al intentar configurar un tercero, no se permite la acción. Por esta situación, se reemplaza el modelo 5505 por el 5506, con la finalidad de poder crear las zonas requeridas y cumplir con los requisitos solicitados. Más información en Página 2.

##

Fin del informe

##