

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

Para esto realizamos:

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

```
RA#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  172.16.5.1      YES NVRAM  up          up
GigabitEthernet0/1  172.16.10.1     YES NVRAM  up          up
GigabitEthernet0/2  unassigned      YES NVRAM  administratively down down
Serial0/0/0         172.16.100.1    YES NVRAM  up          up
```

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

Tenemos un ejemplo de la aplicación en RA:

```
RA#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.5.0 0.0.0.255 area 0
    172.16.10.0 0.0.0.255 area 0
    172.16.100.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:13:21
    2.2.2.2          110          00:13:21
    3.3.3.3          110          00:13:21
  Distance: (default is 110)
```

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

```
Neighbor count is 1 / Adjacent neighbor count
  Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
  Youngest key id is 1
RA#
```

2. Requerimiento 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.

Se apagaron las interfaces que no se estaba utilizando y se pasaron todas a la vlan99

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

La implementación de estos puntos lo podemos ver en la siguiente captura:

```
SWB#show run | section interface FastEthernet0/10
interface FastEthernet0/10
  switchport access vlan 99
  ip dhcp snooping limit rate 2
  switchport mode access
  switchport port-security
  switchport port-security maximum 2
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0004.9A12.057D
  spanning-tree portfast
  spanning-tree bpduguard enable
SWB#
```

Las interfaces que se conectan a los routers se configuraron como trust:

```
SWB#show run | section interface FastEthernet0/20
interface FastEthernet0/20
  switchport access vlan 99
  ip dhcp snooping trust
```

3. Requerimiento 3 Realiza la implementación de Seguridad, confi gurando fi rewall 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

Inside:

```
ciscoasa#show run interface GigabitEthernet1/1
interface GigabitEthernet1/1
  nameif inside
  security-level 100
  ip address 172.16.15.1 255.255.255.0
```

Dmz:

```
ciscoasa#show run interface GigabitEthernet1/5
interface GigabitEthernet1/5
 nameif dmz
 security-level 40
 ip address 172.16.20.1 255.255.255.0
```

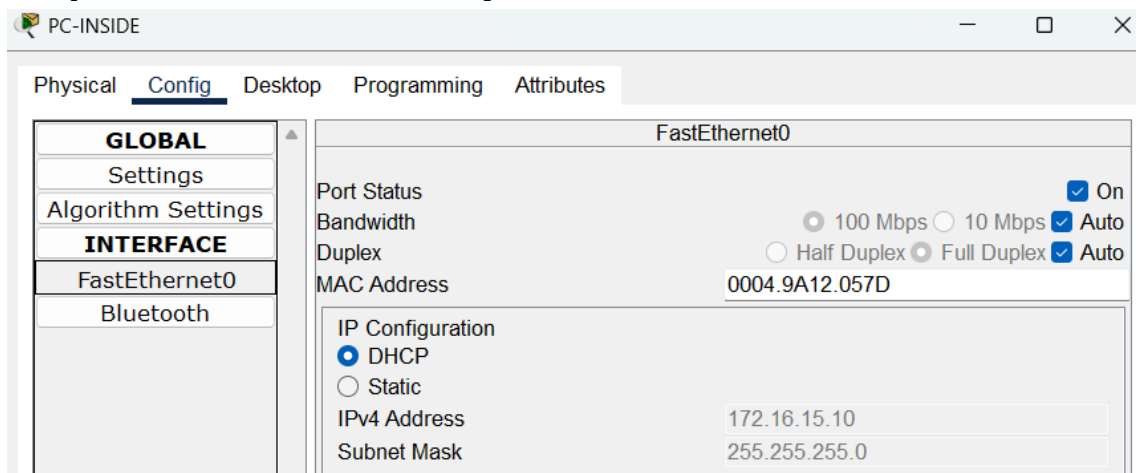
Outside:

```
ciscoasa#show run interface GigabitEthernet1/3
interface GigabitEthernet1/3
 nameif outside
 security-level 20
 ip address 172.16.5.2 255.255.255.0
```

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

```
ciscoasa#show run | include dhcpd
dhcpd option 3 ip 172.16.15.1
dhcpd address 172.16.15.10-172.16.15.25 inside
dhcpd enable inside
ciscoasa#
```

y vemos que la PC-INSIDE obtiene su IP por DHCP:



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

Vemos las traducciones de inside a outside

```
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static DMZ_PC 172.16.5.100
   translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic INSIDE_NET interface
   translate_hits = 8, untranslate_hits = 8
```

Vemos que se modifico el MPF para incluir el ICMP:

```
ciscoasa#show run | section policy-map
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect icmp
    inspect tftp
```

Conectividad de inside a outside desde PC-INSIDE:

```
C:\>ping 172.16.250.3

Pinging 172.16.250.3 with 32 bytes of data:

Reply from 172.16.250.3: bytes=32 time=21ms TTL=124
Reply from 172.16.250.3: bytes=32 time=2ms TTL=124
Reply from 172.16.250.3: bytes=32 time=2ms TTL=124
Reply from 172.16.250.3: bytes=32 time=27ms TTL=124

Ping statistics for 172.16.250.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 27ms, Average = 13ms
```

- 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.

Se ve el ping desde zona outside a la dirección pública de PC-DMZ

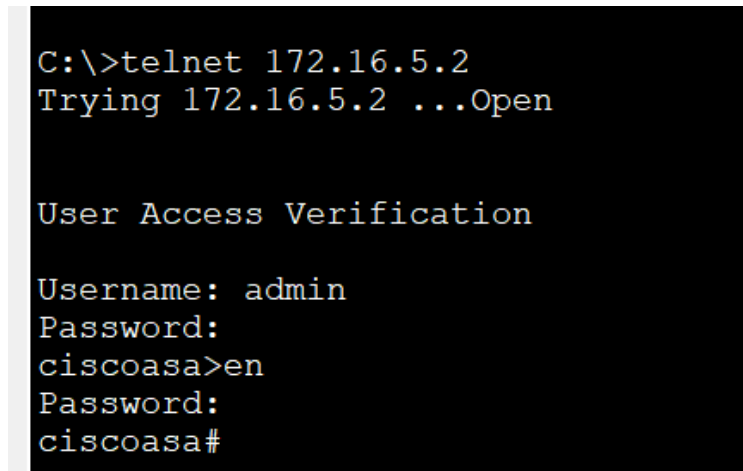
```
RA#ping 172.16.5.100
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.100, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

la imagen es la prueba de que el NAT Estático que se configuró para que la PC-DMZ pueda salir a la zona **outside** está funcionando.

```
ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T - twice, N - net-to-net
NAT from dmz:172.16.20.3/32 to outside:172.16.5.100/32 flags s idle 04:49:06, timeout 0:00:00
```

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



```
C:\>telnet 172.16.5.2
Trying 172.16.5.2 ...Open

User Access Verification

Username: admin
Password:
ciscoasa>en
Password:
ciscoasa#
```

- Implementar VPN Site to Site entre RA y RC

```
RA#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
172.16.200.1 172.16.100.1 QM_IDLE        1089      0 ACTIVE

IPv6 Crypto ISAKMP SA

RA#show crypto ipsec sa
interface: Serial0/0/0
  Crypto map tag: VPN-MAP, local addr 172.16.100.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (172.16.250.0/255.255.255.0/0/0)
  current_peer 172.16.200.1 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 18, #pkts encrypt: 18, #pkts digest: 0
    #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
```

4. Implementa una política de control de acceso para la red de la empresa Desafío Latam en donde este relacionado con el uso eficiente de la VPN site to site entre RA y RC respectivamente.

Política: Política de Uso Eficiente de la VPN Desafío Latam

- **Objetivo:** Asegurar que el túnel VPN Site-to-Site se utilice exclusivamente para el tráfico que requiere cifrado y acceso a recursos internos de la red remota. Esto garantiza un uso eficiente del ancho de banda y mantiene la seguridad de la información sensible.
- **Alcance:**
 - Todo el personal de la empresa que requiera acceder a recursos en la red remota.
- **Lineamientos:**
 - **Tráfico Permitido por la VPN:** Solo se permitirá que el tráfico de la red 172.16.10.0/24 acceda a la red 172.16.250.0/24 a través del túnel VPN. Este tráfico se considerará "interesante" y será cifrado.
 - **Tráfico No Permitido por la VPN:** Todo el tráfico que no cumpla con la condición anterior (por ejemplo, acceso a internet, tráfico de la red 172.16.15.0/24 a la 172.16.250.0/24) no utilizará el túnel VPN y se enrutará de manera normal a través de la red pública.
 - **Configuración de ACL:** La implementación técnica de esta política se realizará mediante listas de control de acceso (ACL) en los routers RA y RC, que definirán de manera explícita el tráfico que debe pasar por el túnel VPN.
 - **Uso de Protocolos:** Se dará prioridad al uso de protocolos seguros para la transmisión de datos, y se limitará el uso de protocolos no esenciales a través del túnel.
 - **Monitoreo:** Se implementarán herramientas para monitorear el uso de la VPN y asegurar que no se utilice para fines no autorizados.

