Desafío/Prueba - Soluciones de seguridad en redes corporativas

Nombre: Felipe Oyanedel Beltran

<u>Descripción</u>:

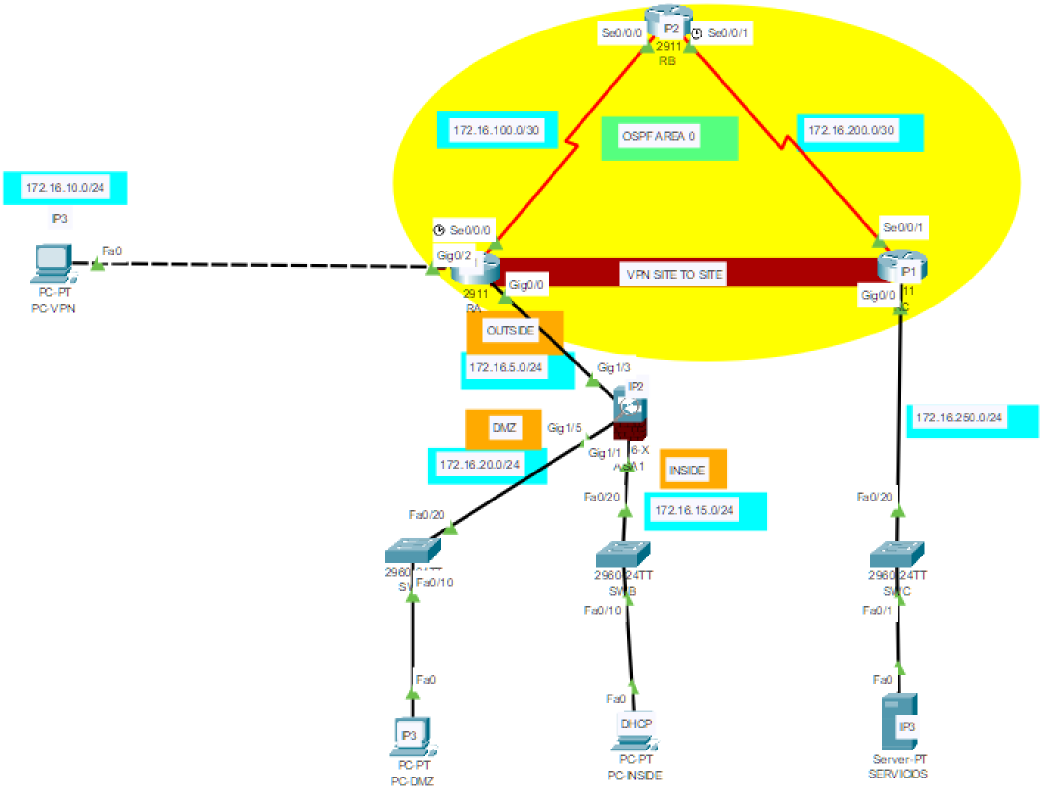
La empresa Desafío Latam ha implementado una red segura que consta de routers y switches Cisco, así como la implementación de un firewall ASA que permite el control del tráfico externo como interno en una organización. También se ha determinado que ciertos usuarios puedan tener acceso de manera segura a la red de la organización desde Internet, por lo cual implementará una VPN site to site que ir de RA a RC.

También se implementará políticas y mecanismos de control de acceso en la organización, que permitirá ir fortaleciendo la red, y el cumplimiento por parte de los usuarios de los distintos recursos, activos de información y datos que deben ser protegidos de la forma más adecuada posible.

<u>Requerimientos</u>:

1. **Realiza la implementación de Capa 3 según los requerimientos solicitados. (2 Puntos)**

Así fue el planteamiento de direccionamiento IPv4, en donde se encendieron las interfaces faltantes y se configuraron sus respectivas direcciones IP en cada segmento de red, según correspondía.

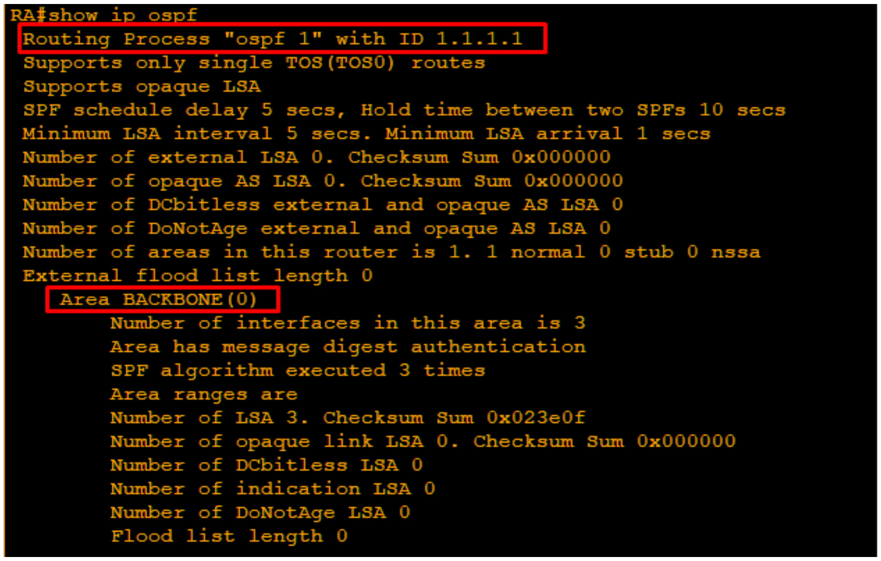


Según topología, el protocolo de enrutamiento para la comunicación entre los routers RA, RB y RC es OSPF, el cual fue configurado haciendo uso de área de Backbone, se tomaron en cuentas las interfaces que serían declaradas como pasivas en la comunicación OSPF y además la autenticación de protocolo a nivel de interfaz entre los routers.

Implementación Protocolo de Enrutamiento Dinámico OSPF

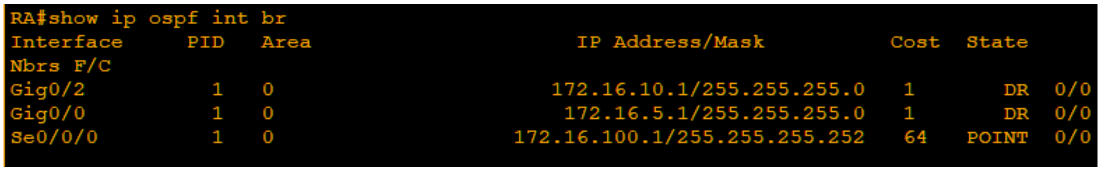
RA

En base a este comando verificamos que el protocolo OSPF se encuentra activo y el área Backbone (Área 0) correctamente configurada.



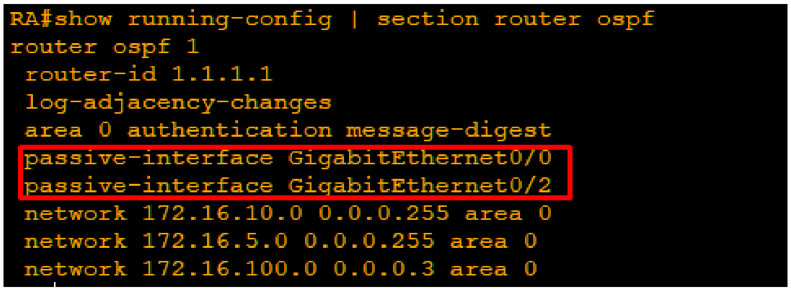
```
RA#show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has message digest authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x023e0f
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Confirmación de las interfaces participantes en enrutamiento OSPF y la validación que se encuentran configuradas en la misma área 0.



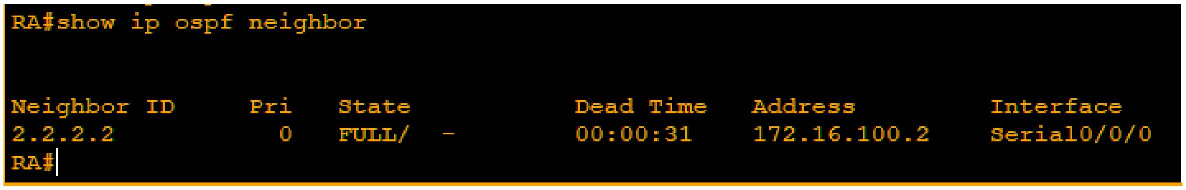
```
RA#show ip ospf int br
Interface      PID   Area                      IP Address/Mask         Cost  State
Nbrs F/C
Gig0/2           1    0                      172.16.10.1/255.255.255.0    1       DR  0/0
Gig0/0           1    0                       172.16.5.1/255.255.255.0    1       DR  0/0
Se0/0/0          1    0                   172.16.100.1/255.255.255.252   64    POINT  0/0
```

Validación que las interfaces que se encontraban conectadas a segmentos LAN se dejaron fuera de la conmutación de mensajes OSPF, quedando como interfaces pasivas. Sin embargo, estas redes LAN se declararon de igual forma, para que así fuesen conocidas por los demás routers al momento de generar adyacencia.



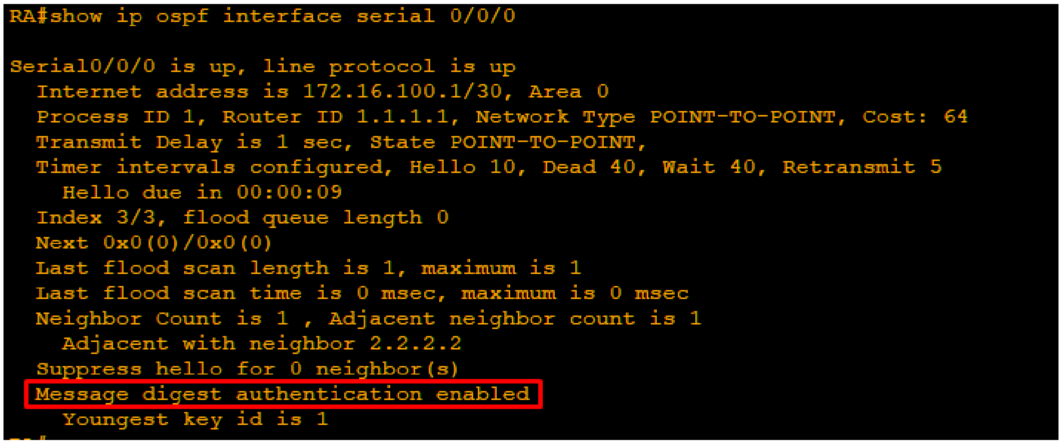
```
RA#show running-config | section router ospf
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/2
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.5.0 0.0.0.255 area 0
 network 172.16.100.0 0.0.0.3 area 0
```

Si las configuraciones no hubiesen sido realizadas con los parametros necesarios, la adyacencia no ocurriría. Sin embargo, con el comando **show ip ospf neighbors** podemos verificar los vecinos OSPF con los cuales se hizo adyacencia a través de la interfaz.



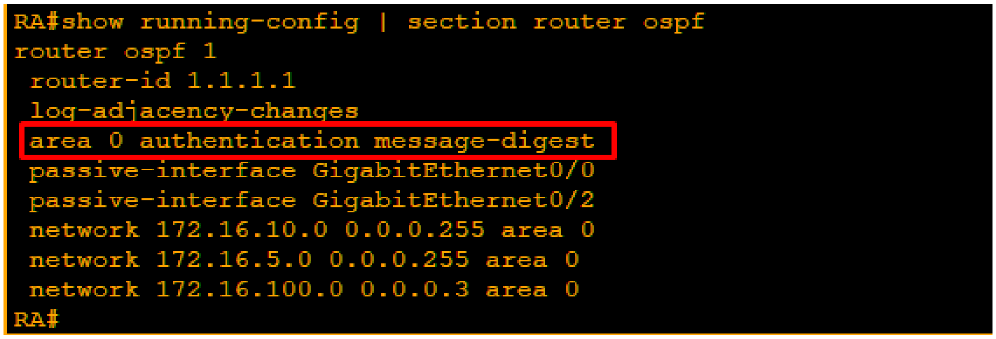
```
RA#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:31    172.16.100.2    Serial0/0/0
RA#
```

En cuanto a la autenticación a nivel de interfaz, tenemos que la interfaz Serial0/0/0 figura con la autenticación habilitada en base a MD5.



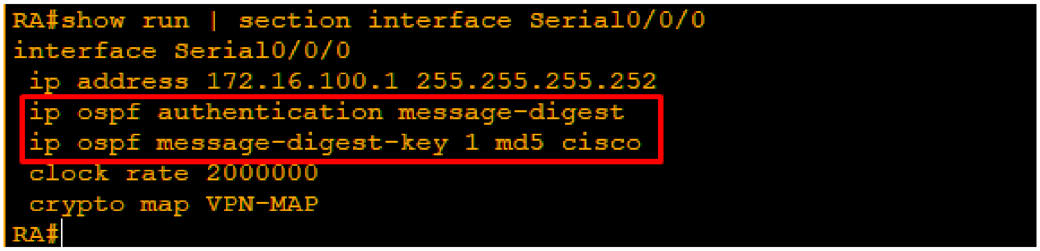
```
RA#show ip ospf interface serial 0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 172.16.100.1/30, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Verificamos a su vez que dentro de la configuración principal del OSPF se menciona la autenticación MD5 en el área BACKBONE.



```
RA#show running-config | section router ospf
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 passive-interface GigabitEthernet0/2
 network 172.16.10.0 0.0.0.255 area 0
 network 172.16.5.0 0.0.0.255 area 0
 network 172.16.100.0 0.0.0.3 area 0
RA#
```

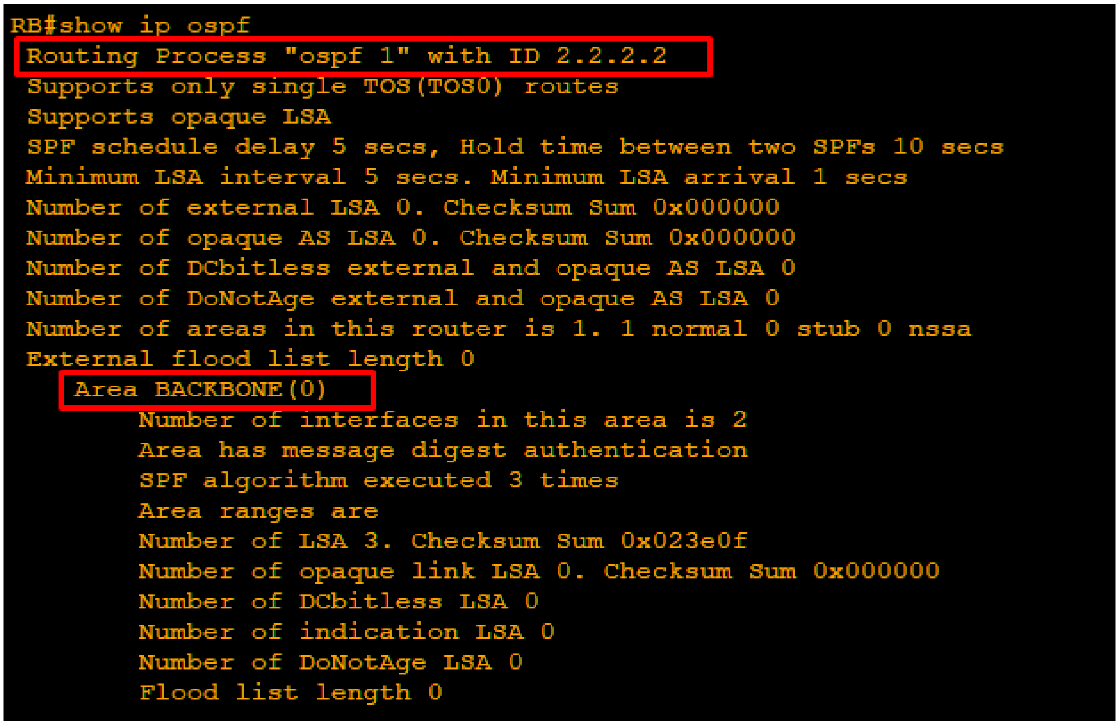
Confirmación de la configuración de autenticación en la interfaz, en donde al ser autenticación MD5 se ve de la siguiente forma:



```
RA#show run | section interface Serial0/0/0
interface Serial0/0/0
 ip address 172.16.100.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 clock rate 2000000
 crypto map VPN-MAP
RA#
```

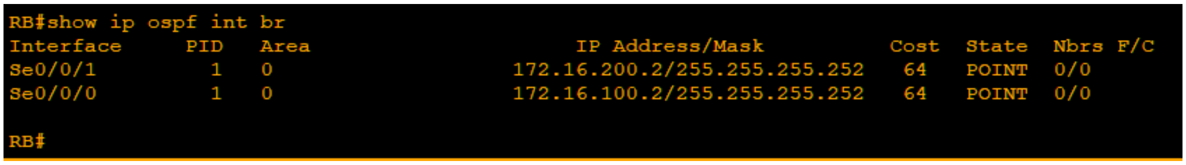
RB

En base a este comando verificamos que el protocolo OSPF se encuentra activo y el área Backbone (Área 0) correctamente configurada.



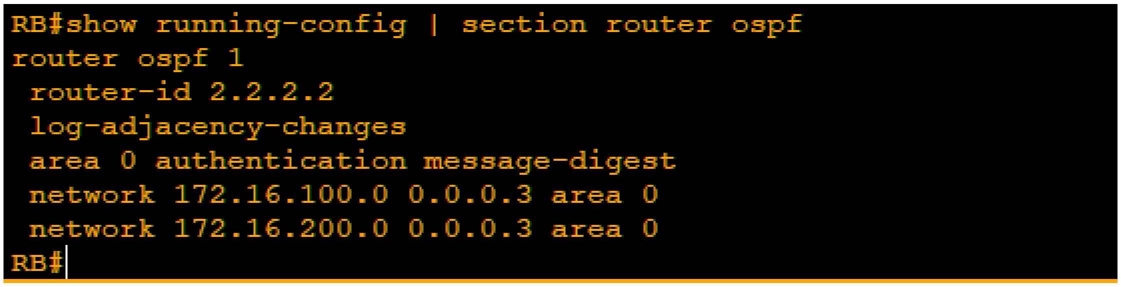
```
RB#show ip ospf
 Routing Process "ospf 1" with ID 2.2.2.2
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has message digest authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x023e0f
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Confirmación de las interfaces participantes en enrutamiento OSPF y la validación que se encuentran configuradas en la misma área 0.



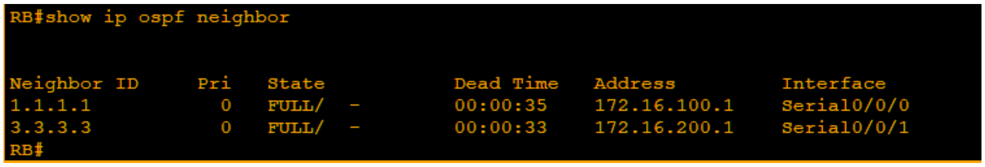
```
RB#show ip ospf int br
Interface    PID   Area            IP Address/Mask         Cost  State  Nbrs F/C
Se0/0/1        1   0          172.16.200.2/255.255.255.252   64   POINT  0/0
Se0/0/0        1   0          172.16.100.2/255.255.255.252   64   POINT  0/0

RB#
```

En este caso, el router RB no cuenta con interfaces pasivas dado que se encuentra conectado a RA y RC, entonces las interfaces deben estar activas para la conmutación de mensajes OSPF y así gestionar la esperada adyacencia.



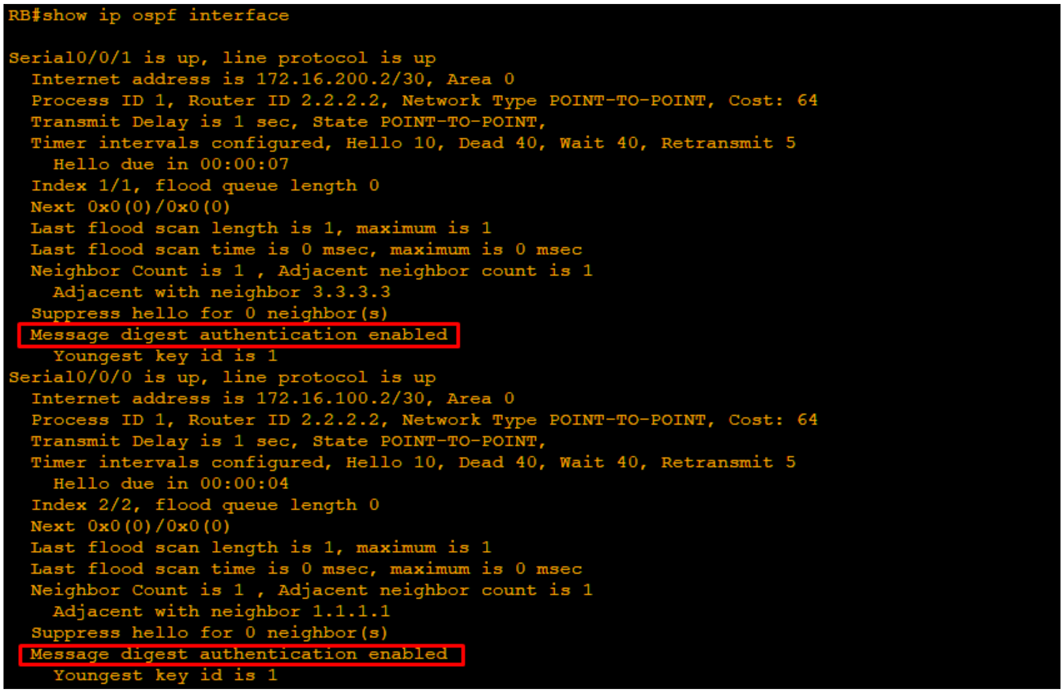
```
RB#show running-config | section router ospf
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 area 0 authentication message-digest
 network 172.16.100.0 0.0.0.3 area 0
 network 172.16.200.0 0.0.0.3 area 0
RB#
```

Si las configuraciones no hubiesen sido realizadas con los parametros necesarios, la adyacencia no ocurriría. Sin embargo, con el comando **show ip ospf neighbors** podemos verificar los vecinos OSPF con los cuales se hizo adyacencia a través de la interfaz.



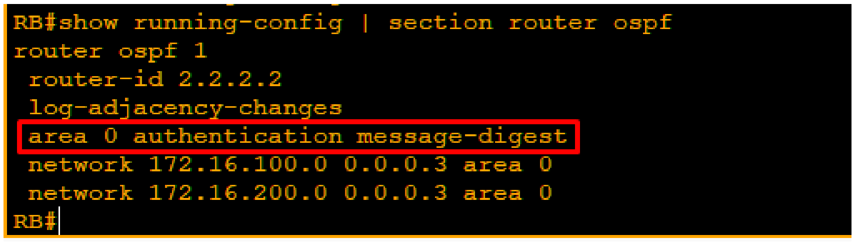
```
RB#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:35    172.16.100.1    Serial0/0/0
3.3.3.3           0   FULL/  -        00:00:33    172.16.200.1    Serial0/0/1
RB#
```

En cuanto a la autenticación a nivel de interfaz, tenemos ambas interfaces conectadas a los routers RA y RC con la autenticación MD5 habilitadas.



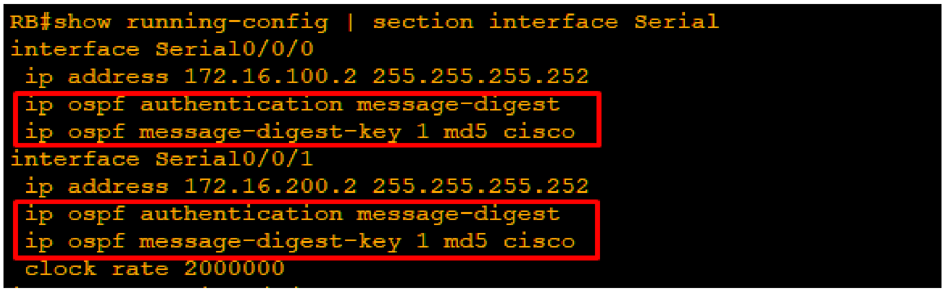
```
RB#show ip ospf interface

Serial0/0/1 is up, line protocol is up
  Internet address is 172.16.200.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Serial0/0/0 is up, line protocol is up
  Internet address is 172.16.100.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Verificamos a su vez que dentro de la configuración principal del OSPF se menciona la autenticación MD5 en el área BACKBONE.



```
RB#show running-config | section router ospf
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 area 0 authentication message-digest
 network 172.16.100.0 0.0.0.3 area 0
 network 172.16.200.0 0.0.0.3 area 0
RB#
```

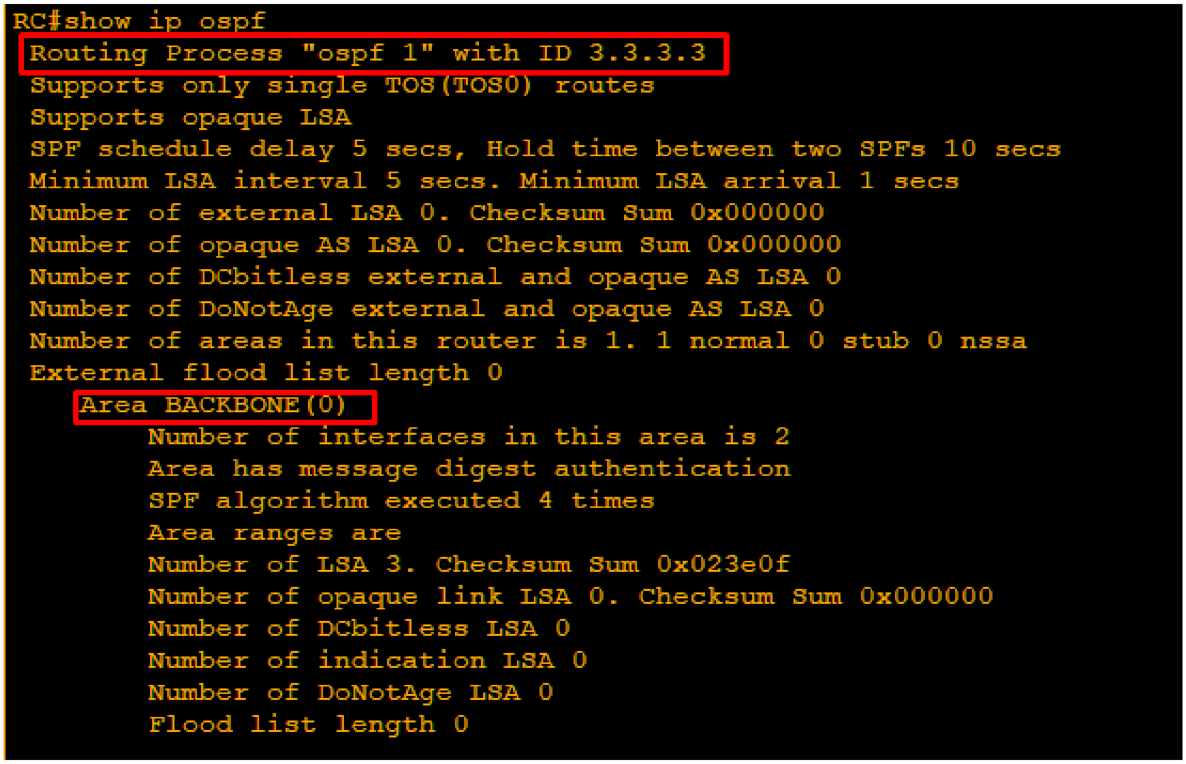
Confirmación de la configuración de autenticación en las interfaces, en donde al ser autenticación MD5 se ve de la siguiente forma:



```
RB#show running-config | section interface Serial
interface Serial0/0/0
 ip address 172.16.100.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
interface Serial0/0/1
 ip address 172.16.200.2 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 clock rate 2000000
```

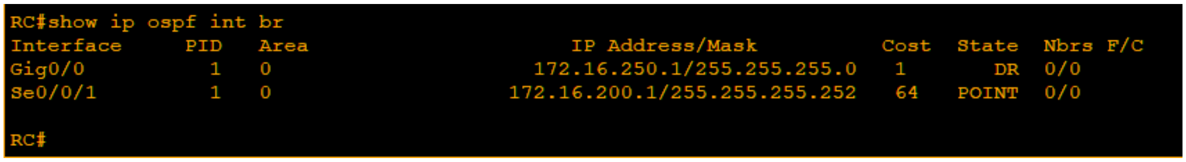
RC

En base a este comando verificamos que el protocolo OSPF se encuentra activo y el área Backbone (Área 0) correctamente configurada.



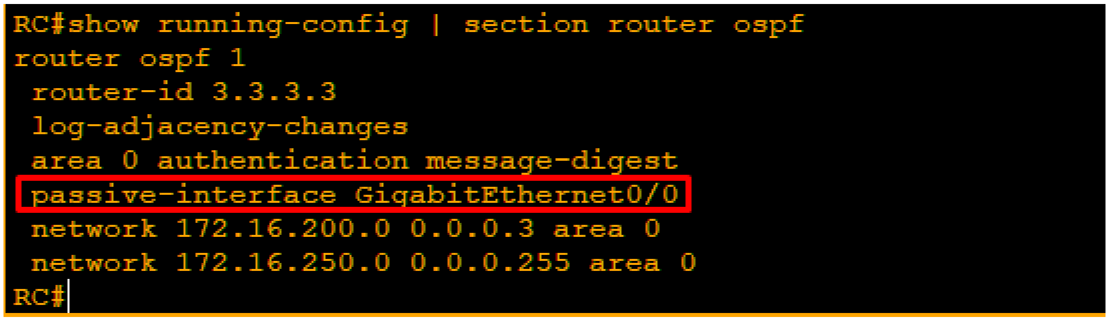
```
RC#show ip ospf
 Routing Process "ospf 1" with ID 3.3.3.3
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has message digest authentication
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x023e0f
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Confirmación de las interfaces participantes en enrutamiento OSPF y la validación que se encuentran configuradas en la misma área 0.



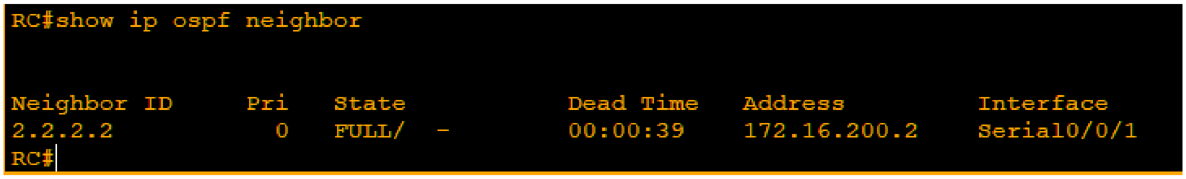
```
RC#show ip ospf int br
Interface      PID   Area                    IP Address/Mask         Cost  State  Nbrs F/C
Gig0/0           1   0                     172.16.250.1/255.255.255.0   1      DR  0/0
Se0/0/1          1   0                   172.16.200.1/255.255.255.252   64  POINT  0/0

RC#
```

Validación que las interfaces que se encontraban conectadas a segmentos LAN se dejaron fuera de la conmutación de mensajes OSPF, quedando como interfaces pasivas. Sin embargo, estas redes LAN se declararon de igual forma, para que así fuesen conocidas por los demás routers al momento de generar adyacencia.



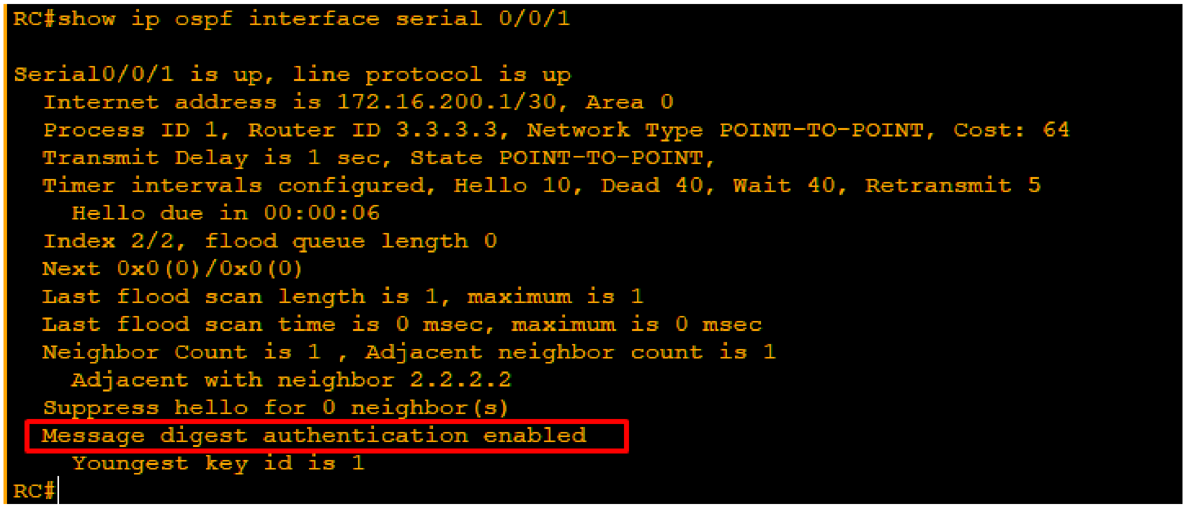
```
RC#show running-config | section router ospf
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 network 172.16.200.0 0.0.0.3 area 0
 network 172.16.250.0 0.0.0.255 area 0
RC#
```

Si las configuraciones no hubiesen sido realizadas con los parametros necesarios, la adyacencia no ocurriría. Sin embargo, con el comando **show ip ospf neighbors** podemos verificar los vecinos OSPF con los cuales se hizo adyacencia a través de la interfaz.



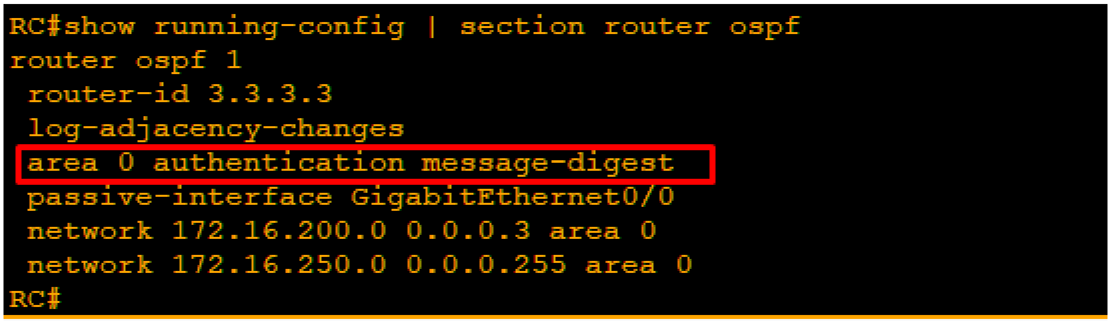
```
RC#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:39    172.16.200.2    Serial0/0/1
RC#
```

En cuanto a la autenticación a nivel de interfaz, tenemos que la interfaz Serial0/0/1 figura con la autenticación habilitada en base a MD5.



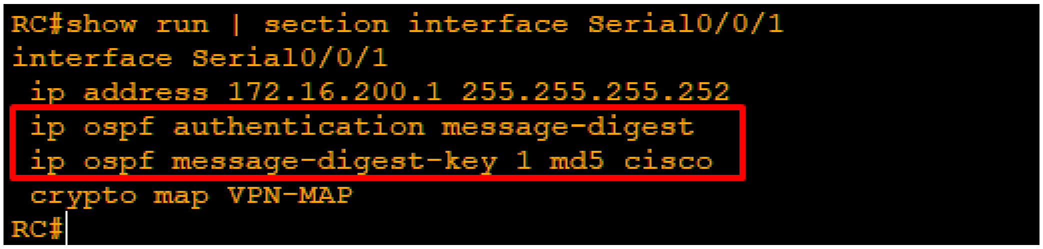
```
RC#show ip ospf interface serial 0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 172.16.200.1/30, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
RC#
```

Verificamos a su vez que dentro de la configuración principal del OSPF se menciona la autenticación MD5 en el área BACKBONE.



```
RC#show running-config | section router ospf
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 area 0 authentication message-digest
 passive-interface GigabitEthernet0/0
 network 172.16.200.0 0.0.0.3 area 0
 network 172.16.250.0 0.0.0.255 area 0
RC#
```

Confirmación de la configuración de autenticación en la interfaz, en donde al ser autenticación MD5 se ve de la siguiente forma:



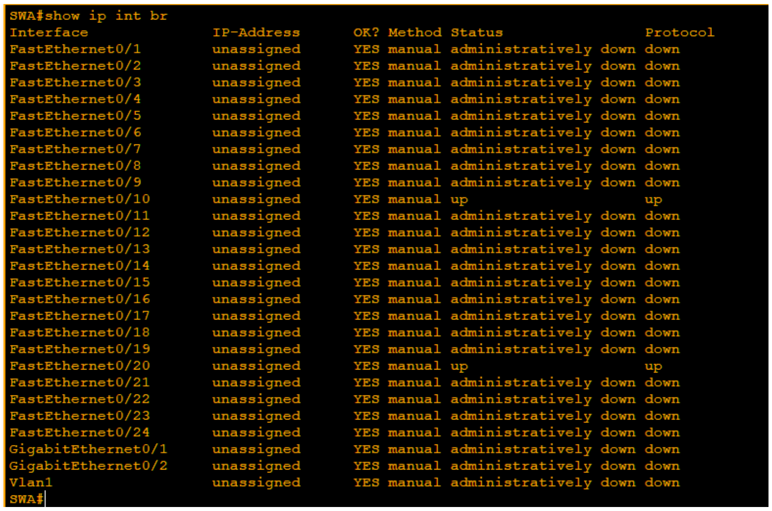
```
RC#show run | section interface Serial0/0/1
interface Serial0/0/1
 ip address 172.16.200.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 crypto map VPN-MAP
RC#
```

2. **Realiza la implementación de Capa 2, además de los requerimientos de seguridad requeridos. (2 Puntos)**

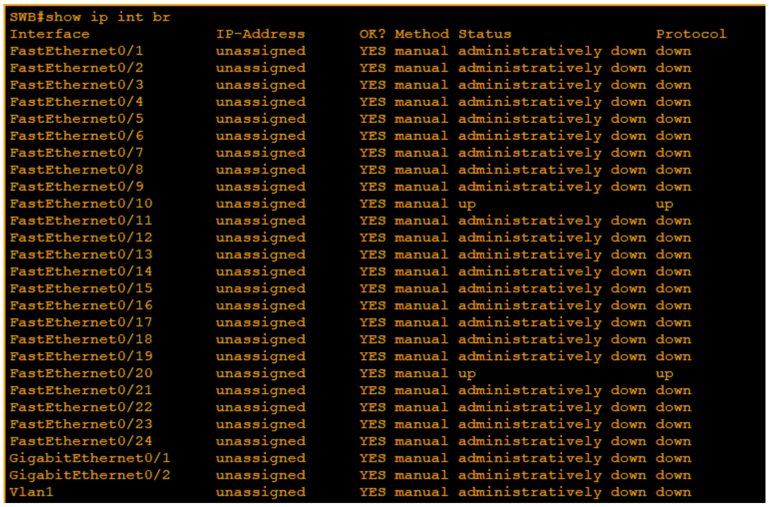
Como parte de las buenas prácticas de seguridad y optimización de la red, se implementaron configuraciones avanzadas en los switches para garantizar un entorno robusto y protegido. En primer lugar, se aseguró que las interfaces que no estuviesen en uso tuvieran una VLAN en cuarentena y separada del tráfico normal de la red, con nombre BLACKHOLE y en estado shutdown. Adicionalmente, se aplicó seguridad de puerto, limitando el aprendizaje de direcciones MAC a un máximo de 2 y configurando la desactivación automática (shutdown) en caso de exceder este límite, previniendo así posibles ataques por suplantación o saturación.

Para reforzar la estabilidad de la red, se implementaron mecanismos de protección STP (Spanning Tree Protocol), evitando bucles y ataques de manipulación de topología. Finalmente, se desplegó DHCP Snooping para bloquear servidores DHCP no autorizados, junto con un mecanismo de rate limiting que restringe las solicitudes DHCP a un máximo de dos (2) direcciones IP por minuto, mitigando eficazmente ataques de hambruna DHCP (DHCP starvation).

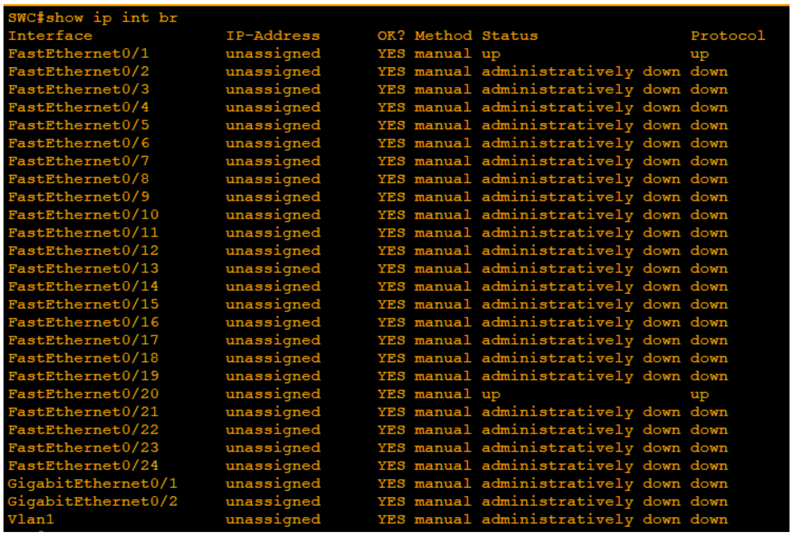
Interfaces Inactivas en Switches



```
SWA#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual administratively down down
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual up                    up
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual up                    up
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
SWA#
```

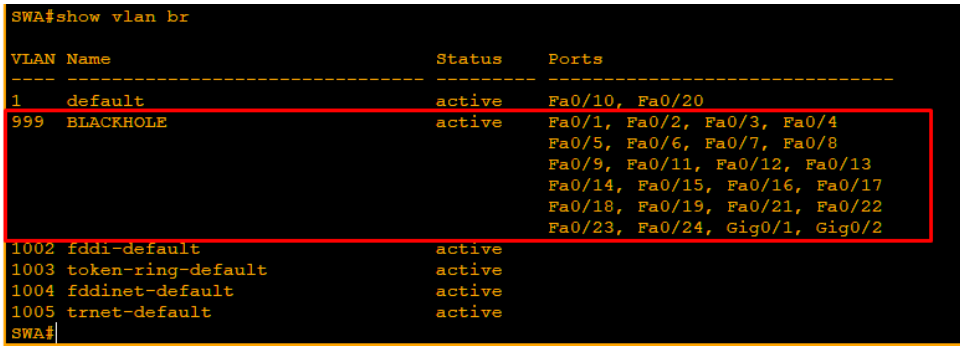


```
SWB#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual administratively down down
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual up                    up
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual up                    up
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

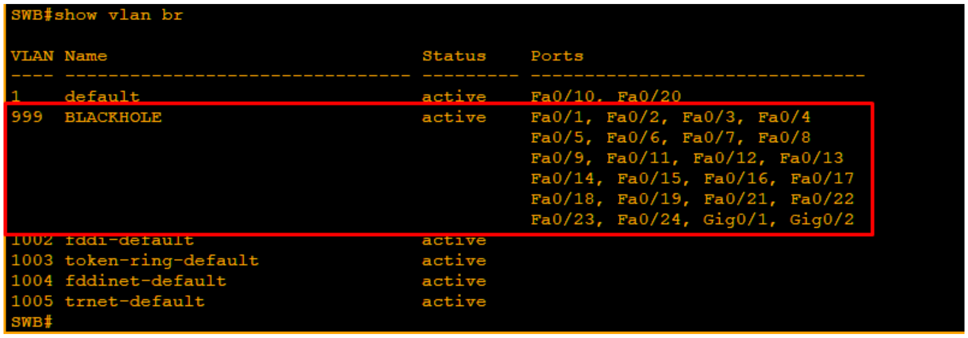


```
SWC#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual administratively down down
FastEthernet0/3        unassigned      YES manual administratively down down
FastEthernet0/4        unassigned      YES manual administratively down down
FastEthernet0/5        unassigned      YES manual administratively down down
FastEthernet0/6        unassigned      YES manual administratively down down
FastEthernet0/7        unassigned      YES manual administratively down down
FastEthernet0/8        unassigned      YES manual administratively down down
FastEthernet0/9        unassigned      YES manual administratively down down
FastEthernet0/10       unassigned      YES manual administratively down down
FastEthernet0/11       unassigned      YES manual administratively down down
FastEthernet0/12       unassigned      YES manual administratively down down
FastEthernet0/13       unassigned      YES manual administratively down down
FastEthernet0/14       unassigned      YES manual administratively down down
FastEthernet0/15       unassigned      YES manual administratively down down
FastEthernet0/16       unassigned      YES manual administratively down down
FastEthernet0/17       unassigned      YES manual administratively down down
FastEthernet0/18       unassigned      YES manual administratively down down
FastEthernet0/19       unassigned      YES manual administratively down down
FastEthernet0/20       unassigned      YES manual up                    up
FastEthernet0/21       unassigned      YES manual administratively down down
FastEthernet0/22       unassigned      YES manual administratively down down
FastEthernet0/23       unassigned      YES manual administratively down down
FastEthernet0/24       unassigned      YES manual administratively down down
GigabitEthernet0/1     unassigned      YES manual administratively down down
GigabitEthernet0/2     unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

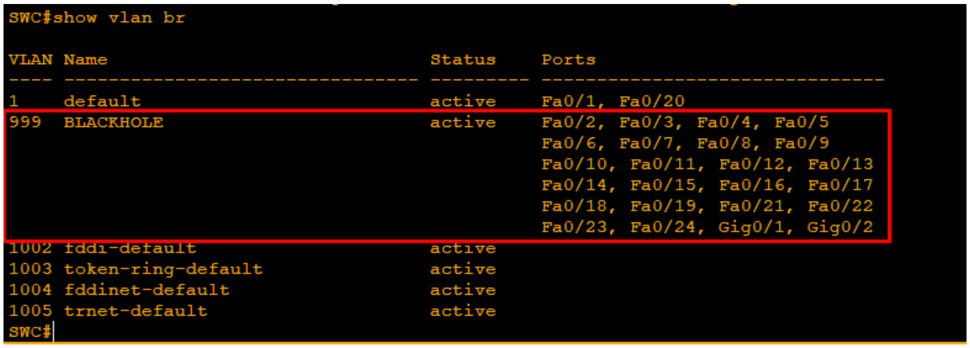
Vlan 999 BLACKHOLE



```
SWA#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/20
999  BLACKHOLE                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWA#
```



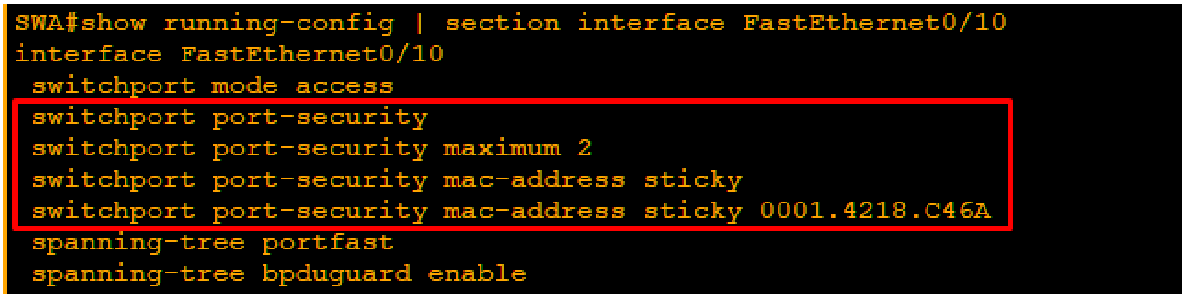
```
SWB#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/10, Fa0/20
999  BLACKHOLE                        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWB#
```



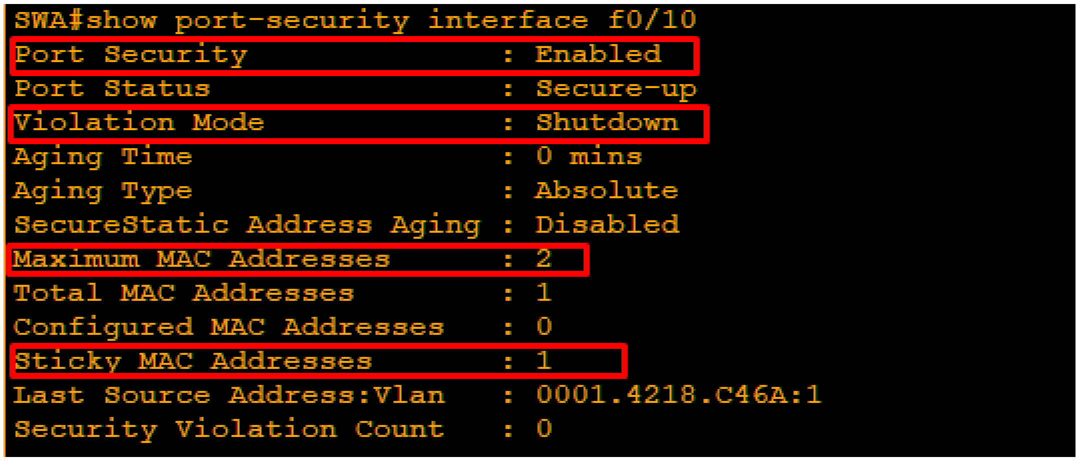
```
SWC#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/20
999  BLACKHOLE                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWC#
```

Port-Security

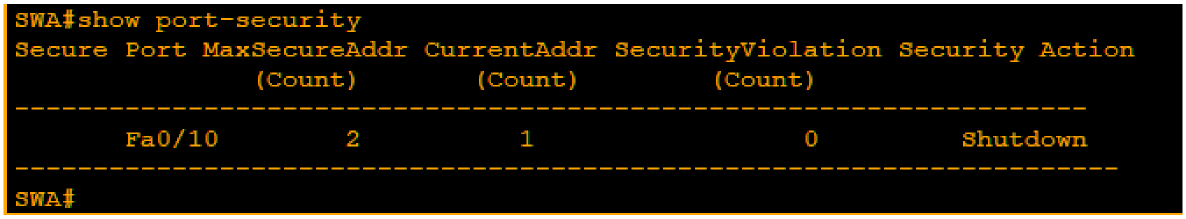
RA



```
SWA#show running-config | section interface FastEthernet0/10
interface FastEthernet0/10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.4218.C46A
 spanning-tree portfast
 spanning-tree bpduguard enable
```

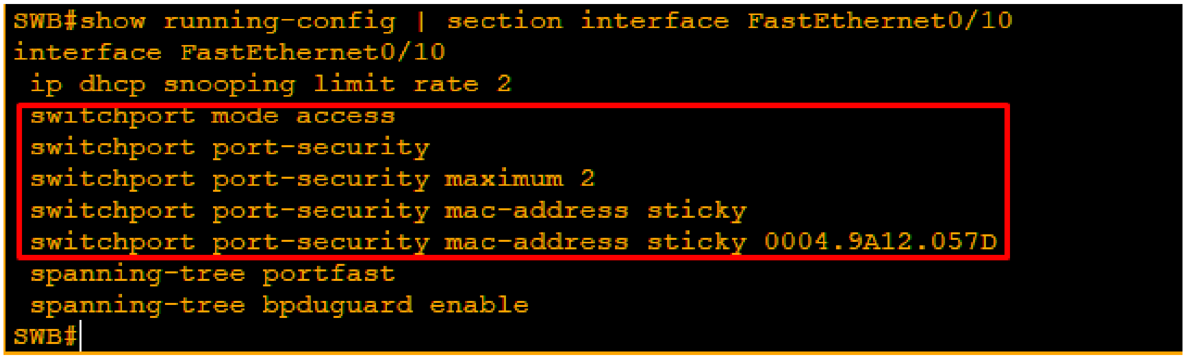


```
SWA#show port-security interface f0/10
Port Security                  : Enabled
Port Status                    : Secure-up
Violation Mode                 : Shutdown
Aging Time                     : 0 mins
Aging Type                     : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses          : 2
Total MAC Addresses            : 1
Configured MAC Addresses       : 0
Sticky MAC Addresses           : 1
Last Source Address:Vlan       : 0001.4218.C46A:1
Security Violation Count       : 0
```

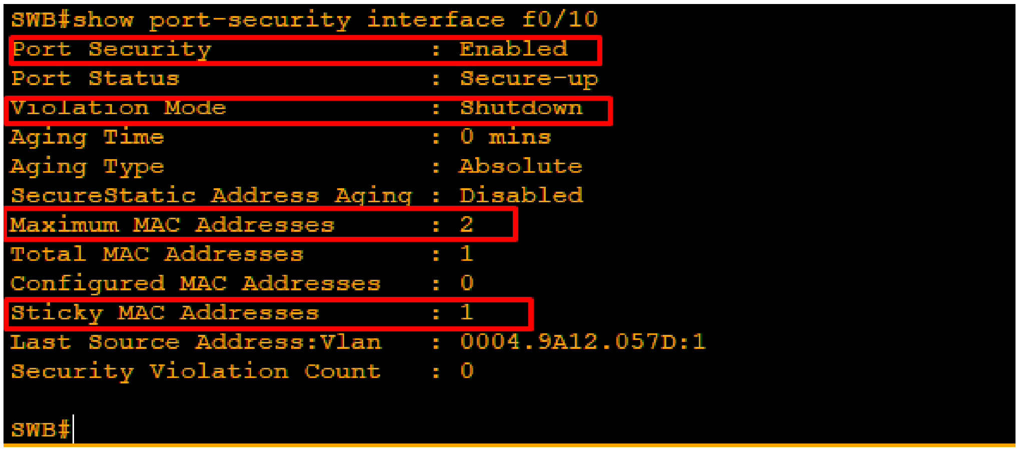


```
SWA#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)          (Count)           (Count)
----------------------------------------------------------------------
       Fa0/10           2           1                  0          Shutdown
------------------------------------------------------------------------
SWA#
```

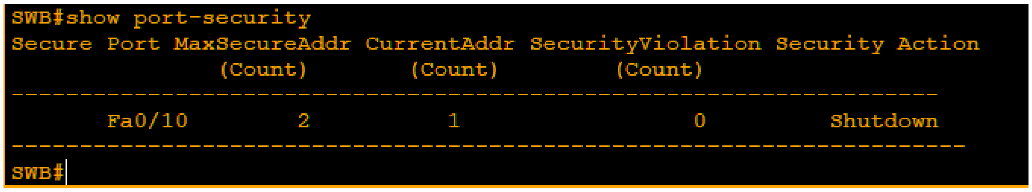
RB



```
SWB#show running-config | section interface FastEthernet0/10
interface FastEthernet0/10
 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#
```

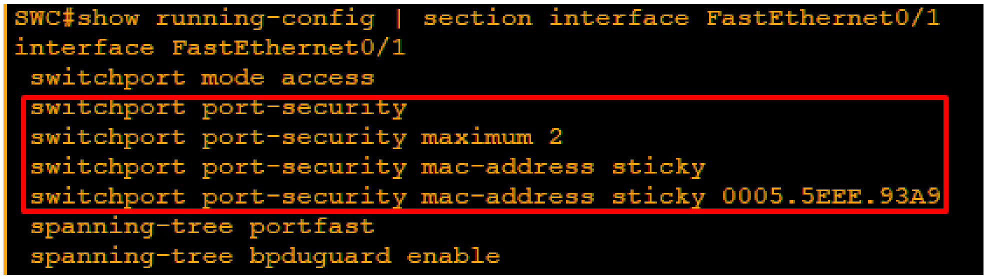


```
SWB#show port-security interface f0/10
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0004.9A12.057D:1
Security Violation Count   : 0

SWB#
```

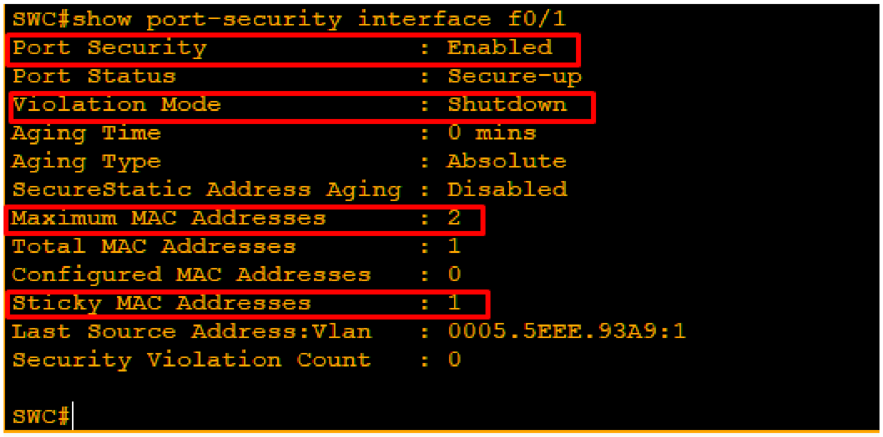


```
SWB#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
------------------------------------------------------------------------
      Fa0/10        2            1                0          Shutdown
--------------------------------------------------------------------------
SWB#
```

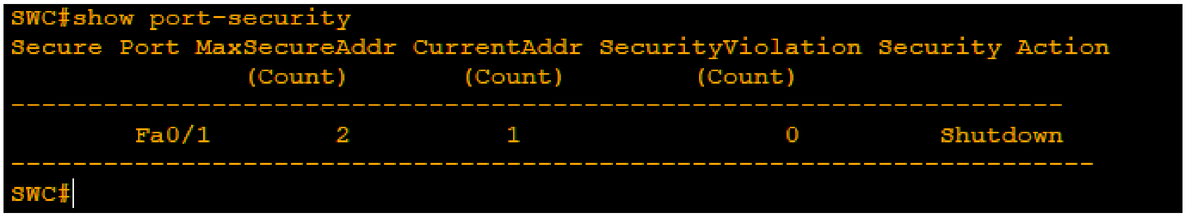
RC



```
SWC#show running-config | section interface FastEthernet0/1
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5EEE.93A9
 spanning-tree portfast
 spanning-tree bpduguard enable
```

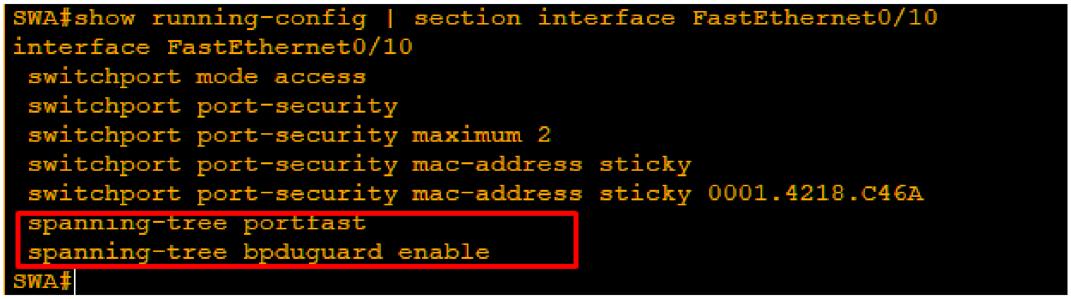


```
SWC#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0005.5EEE.93A9:1
Security Violation Count   : 0

SWC#
```

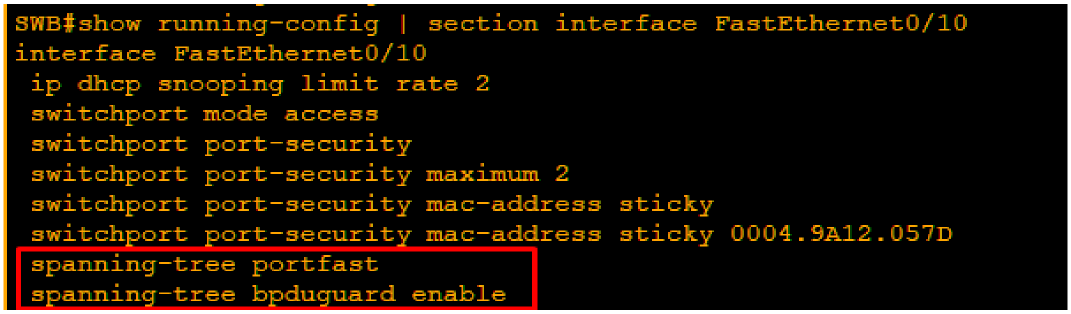


```
SWC#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
----------------------------------------------------------------------
        Fa0/1         2           1                  0         Shutdown
------------------------------------------------------------------------
SWC#
```

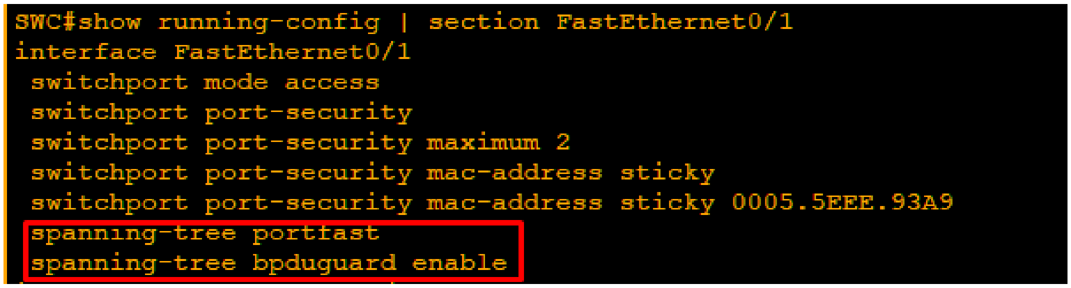
Mecanismos de estabilización de STP



```
SWA#show running-config | section interface FastEthernet0/10
interface FastEthernet0/10
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.4218.C46A
 spanning-tree portfast
 spanning-tree bpduguard enable
SWA#
```

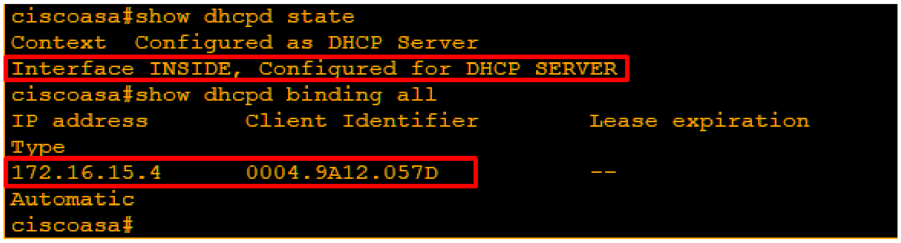


```
SWB#show running-config | section interface FastEthernet0/10
interface FastEthernet0/10
 ip dhcp snooping limit rate 2
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0004.9A12.057D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

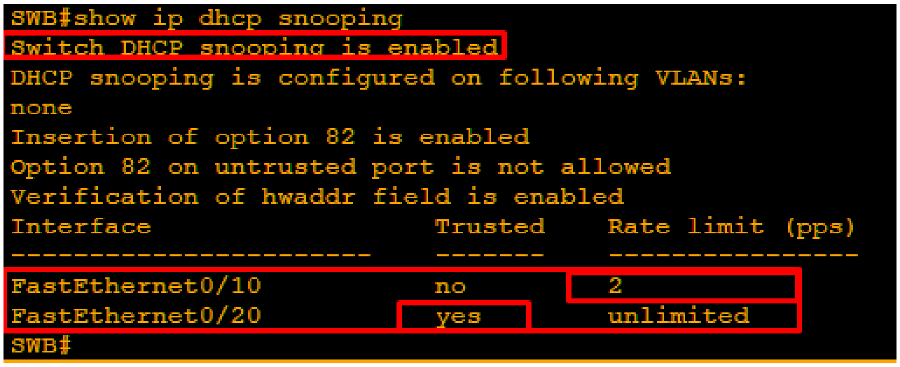


```
SWC#show running-config | section FastEthernet0/1
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0005.5EEE.93A9
 spanning-tree portfast
 spanning-tree bpduguard enable
```

DHCP Snooping



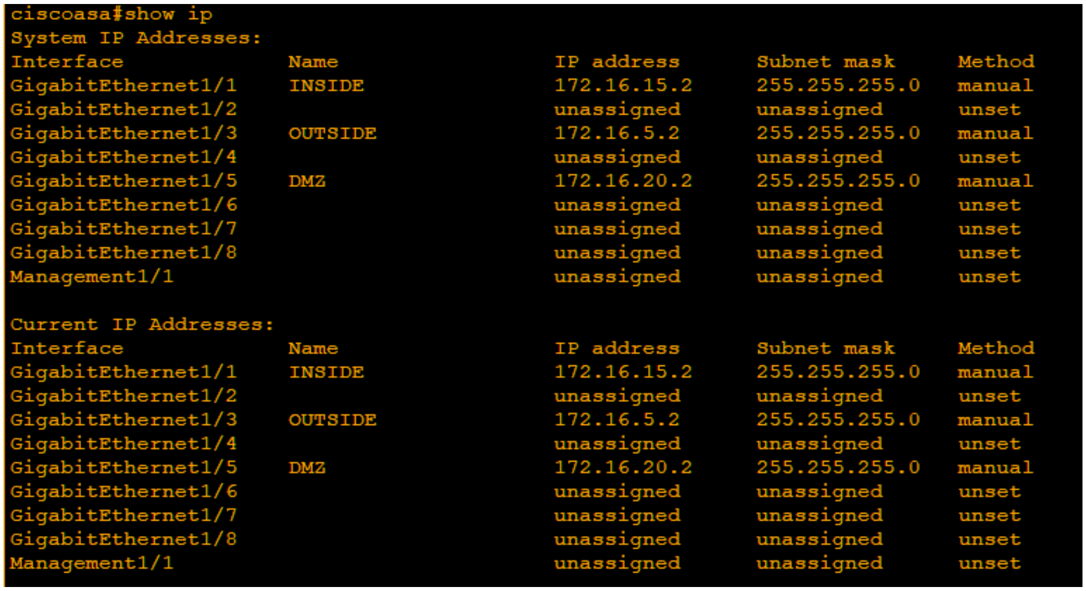
```
ciscoasa#show dhcpd state
Context  Configured as DHCP Server
Interface INSIDE, Configured for DHCP SERVER
ciscoasa#show dhcpd binding all
IP address        Client Identifier        Lease expiration
Type
172.16.15.4       0004.9A12.057D           --
Automatic
ciscoasa#
```



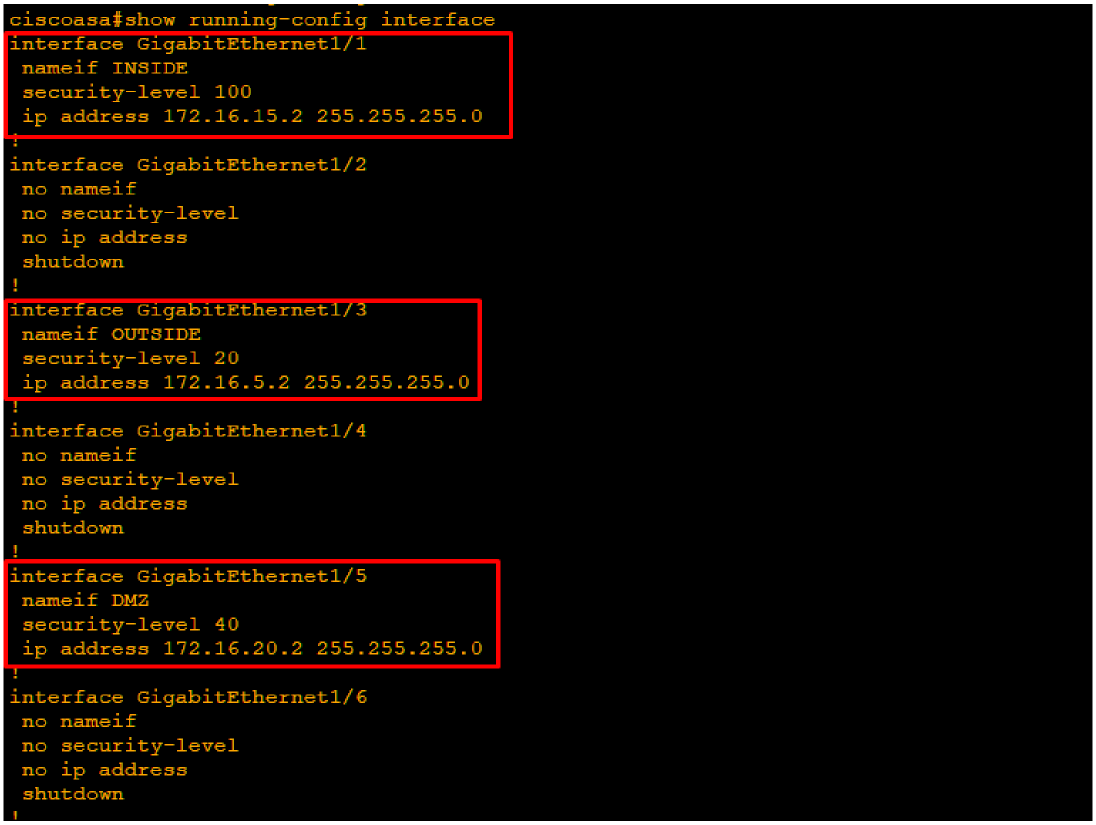
```
SWB#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    --------   ----------------
FastEthernet0/10           no         2
FastEthernet0/20           yes        unlimited
SWB#
```

3. **Realiza la implementación de Seguridad, configurando firewall ASA y VPN de Acceso Remoto según requerimientos. (2 Puntos)**

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.

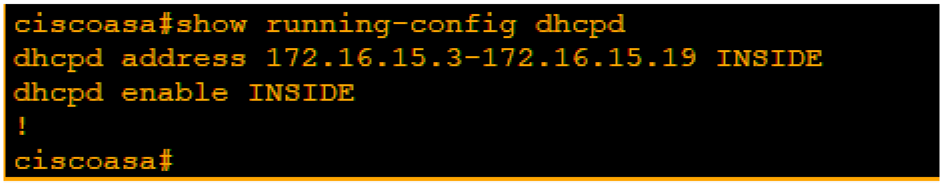


```
ciscoasa#show ip
System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet1/1       INSIDE              172.16.15.2     255.255.255.0   manual
GigabitEthernet1/2                           unassigned      unassigned      unset
GigabitEthernet1/3       OUTSIDE             172.16.5.2      255.255.255.0   manual
GigabitEthernet1/4                           unassigned      unassigned      unset
GigabitEthernet1/5       DMZ                 172.16.20.2     255.255.255.0   manual
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       INSIDE              172.16.15.2     255.255.255.0   manual
GigabitEthernet1/2                           unassigned      unassigned      unset
GigabitEthernet1/3       OUTSIDE             172.16.5.2      255.255.255.0   manual
GigabitEthernet1/4                           unassigned      unassigned      unset
GigabitEthernet1/5       DMZ                 172.16.20.2     255.255.255.0   manual
GigabitEthernet1/6                           unassigned      unassigned      unset
GigabitEthernet1/7                           unassigned      unassigned      unset
GigabitEthernet1/8                           unassigned      unassigned      unset
Management1/1                                unassigned      unassigned      unset
```

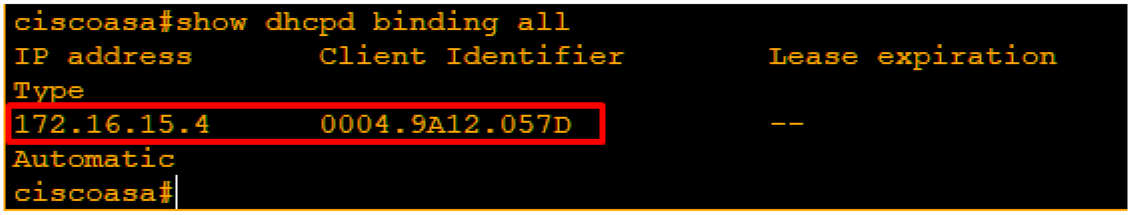


```
ciscoasa#show running-config interface
interface GigabitEthernet1/1
 nameif INSIDE
 security-level 100
 ip address 172.16.15.2 255.255.255.0
!
interface GigabitEthernet1/2
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/3
 nameif OUTSIDE
 security-level 20
 ip address 172.16.5.2 255.255.255.0
!
interface GigabitEthernet1/4
 no nameif
 no security-level
 no ip address
 shutdown
!
interface GigabitEthernet1/5
 nameif DMZ
 security-level 40
 ip address 172.16.20.2 255.255.255.0
!
interface GigabitEthernet1/6
 no nameif
 no security-level
 no ip address
 shutdown
!
```

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

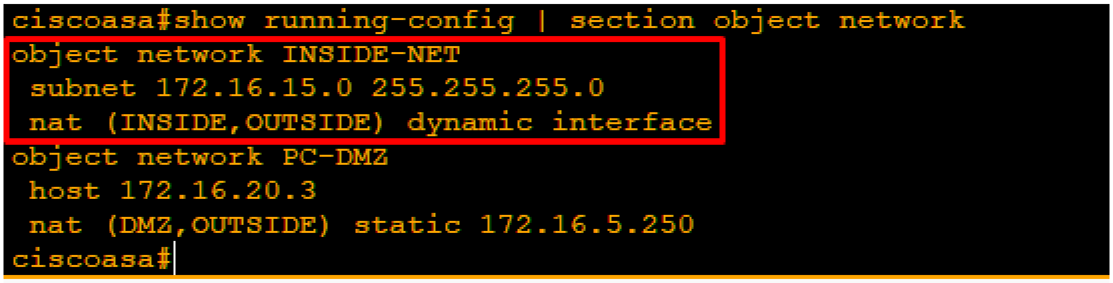


```
ciscoasa#show running-config dhcpd
dhcpd address 172.16.15.3-172.16.15.19 INSIDE
dhcpd enable INSIDE
!
ciscoasa#
```

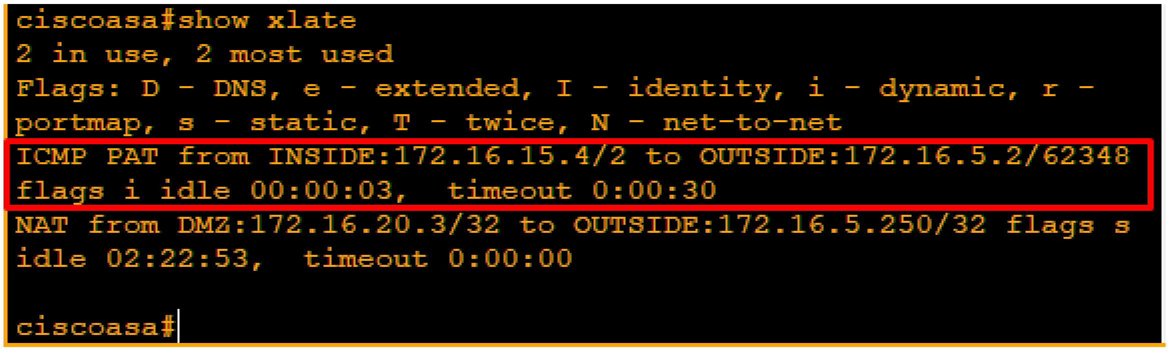


```
ciscoasa#show dhcpd binding all
IP address        Client Identifier        Lease expiration
Type
172.16.15.4       0004.9A12.057D           --
Automatic
ciscoasa#
```

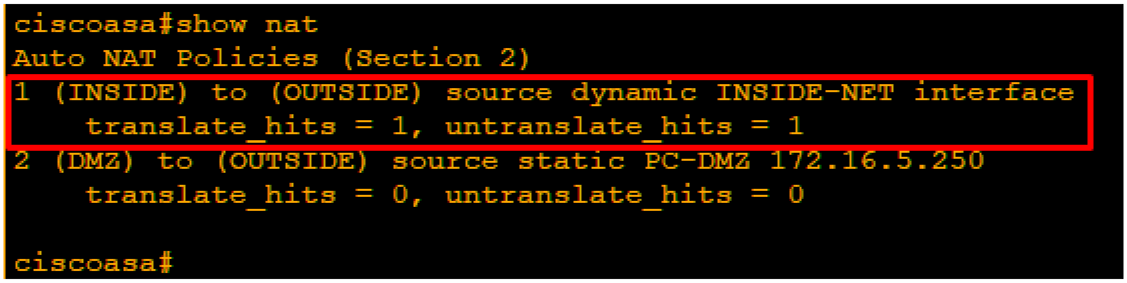
Implementar PAT para que Inside pueda salir por zona Outside, no olvidando implementar MPF para permitir el paso del ICMP.



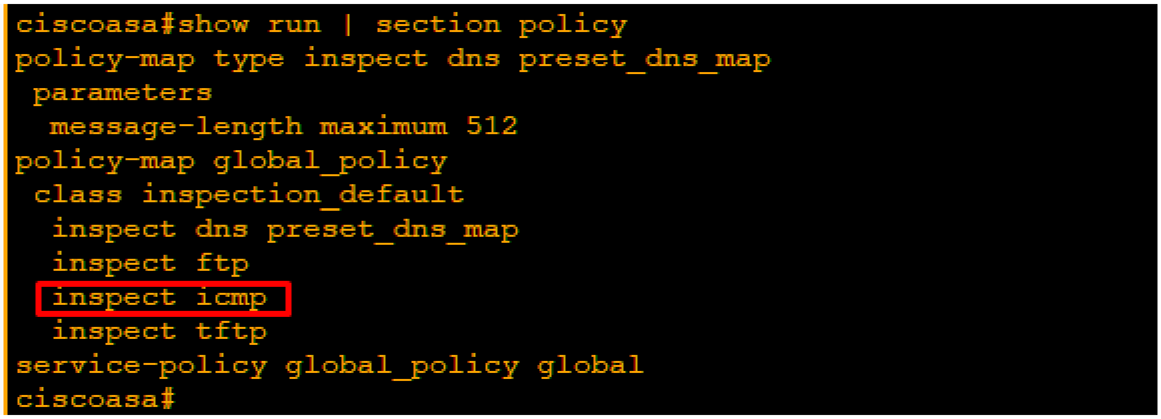
```
ciscoasa#show running-config | section object network
object network INSIDE-NET
 subnet 172.16.15.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface
object network PC-DMZ
 host 172.16.20.3
 nat (DMZ,OUTSIDE) static 172.16.5.250
ciscoasa#
```



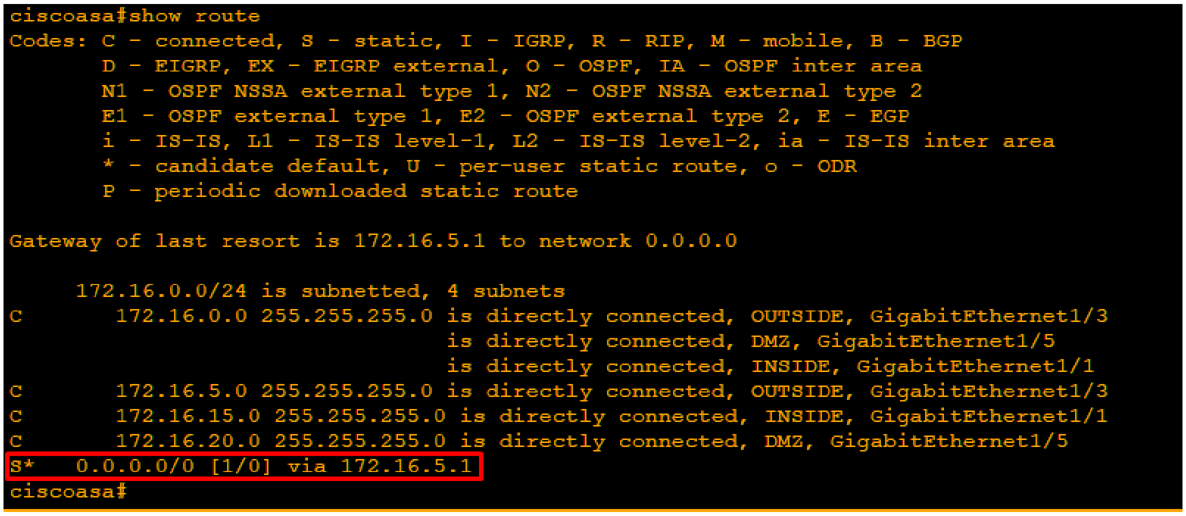
```
ciscoasa#show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r -
portmap, s - static, T - twice, N - net-to-net
ICMP PAT from INSIDE:172.16.15.4/2 to OUTSIDE:172.16.5.2/62348
flags i idle 00:00:03,  timeout 0:00:30
NAT from DMZ:172.16.20.3/32 to OUTSIDE:172.16.5.250/32 flags s
idle 02:22:53,  timeout 0:00:00

ciscoasa#
```



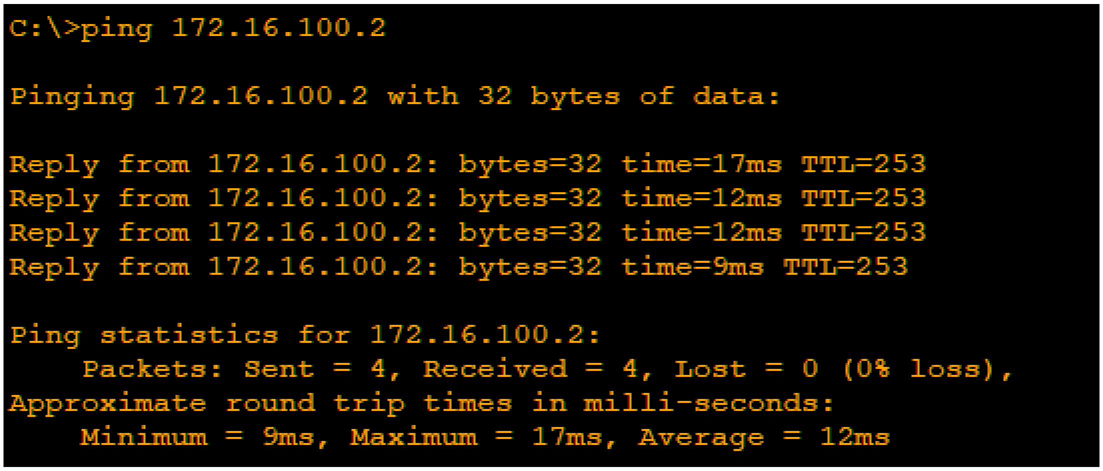
```
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
    translate_hits = 1, untranslate_hits = 1
2 (DMZ) to (OUTSIDE) source static PC-DMZ 172.16.5.250
    translate_hits = 0, untranslate_hits = 0

ciscoasa#
```



```
ciscoasa#show run | section policy
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
service-policy global_policy global
ciscoasa#
```

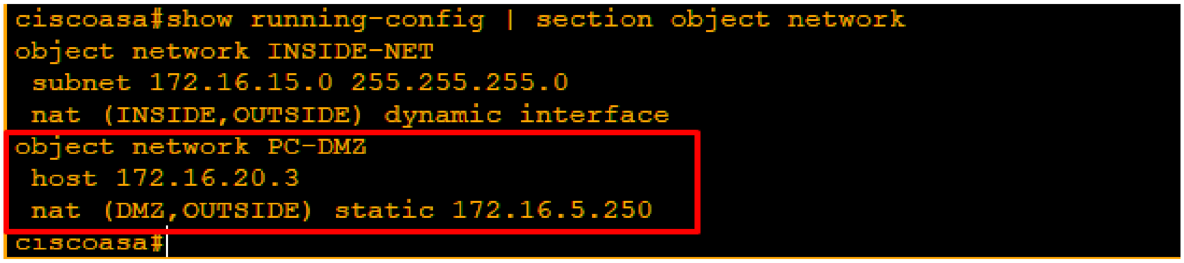


```
ciscoasa#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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 172.16.5.1 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.0.0 255.255.255.0 is directly connected, OUTSIDE, GigabitEthernet1/3
                                 is directly connected, DMZ, GigabitEthernet1/5
                                 is directly connected, INSIDE, GigabitEthernet1/1
C       172.16.5.0 255.255.255.0 is directly connected, OUTSIDE, GigabitEthernet1/3
C       172.16.15.0 255.255.255.0 is directly connected, INSIDE, GigabitEthernet1/1
C       172.16.20.0 255.255.255.0 is directly connected, DMZ, GigabitEthernet1/5
S*    0.0.0.0/0 [1/0] via 172.16.5.1
ciscoasa#
```

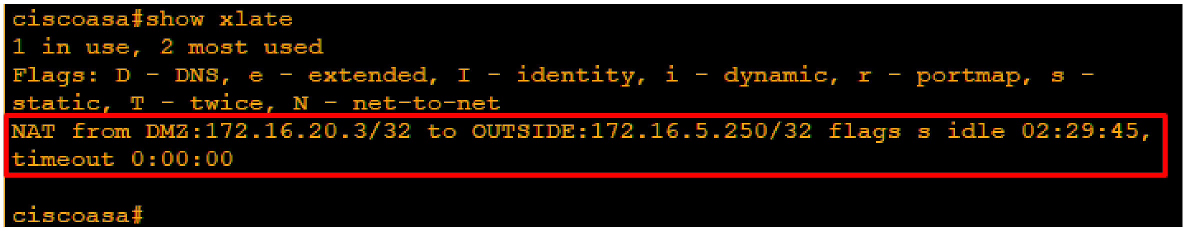


```
C:\>ping 172.16.100.2

Pinging 172.16.100.2 with 32 bytes of data:

Reply from 172.16.100.2: bytes=32 time=17ms TTL=253
Reply from 172.16.100.2: bytes=32 time=12ms TTL=253
Reply from 172.16.100.2: bytes=32 time=12ms TTL=253
Reply from 172.16.100.2: bytes=32 time=9ms TTL=253

Ping statistics for 172.16.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 17ms, Average = 12ms
```

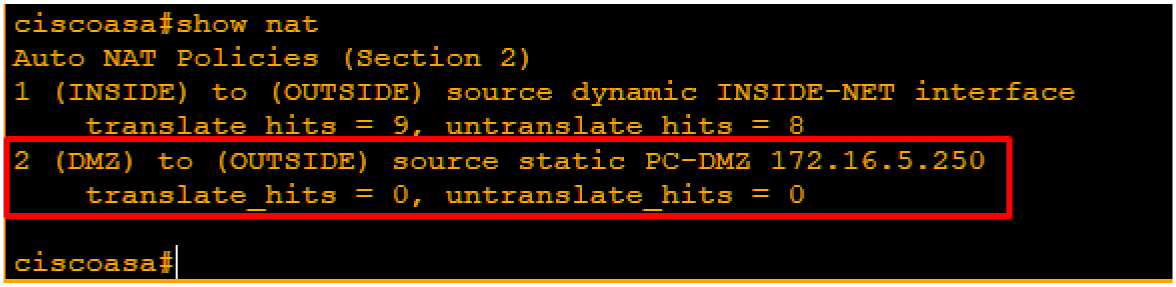
Permitir que en PC-DMZ pueda salir por NAT Estático hacia Outside. Utilizar IP a elección de dicho segmento de red. Realizar configuraciones pertinentes para permitir el retorno del ICMP hacia la DMZ.



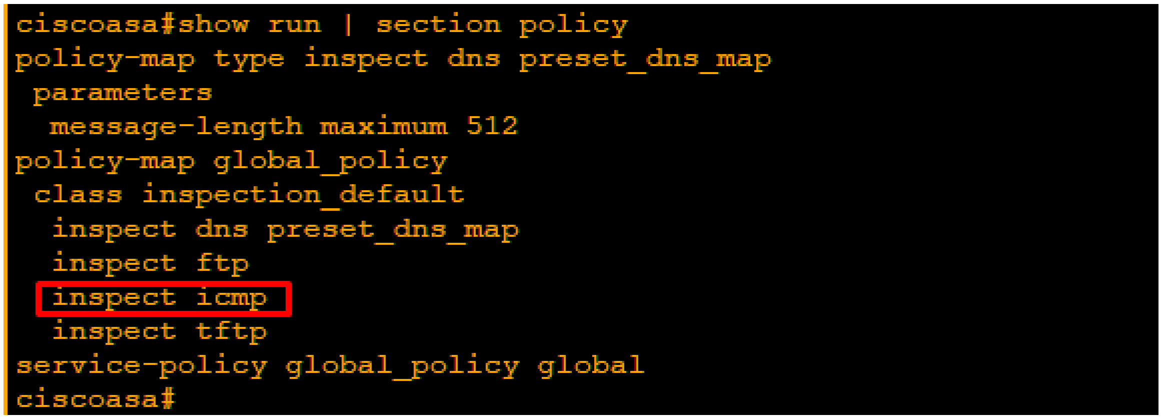
```
ciscoasa#show running-config | section object network
object network INSIDE-NET
 subnet 172.16.15.0 255.255.255.0
 nat (INSIDE,OUTSIDE) dynamic interface
object network PC-DMZ
 host 172.16.20.3
 nat (DMZ,OUTSIDE) static 172.16.5.250
ciscoasa#
```



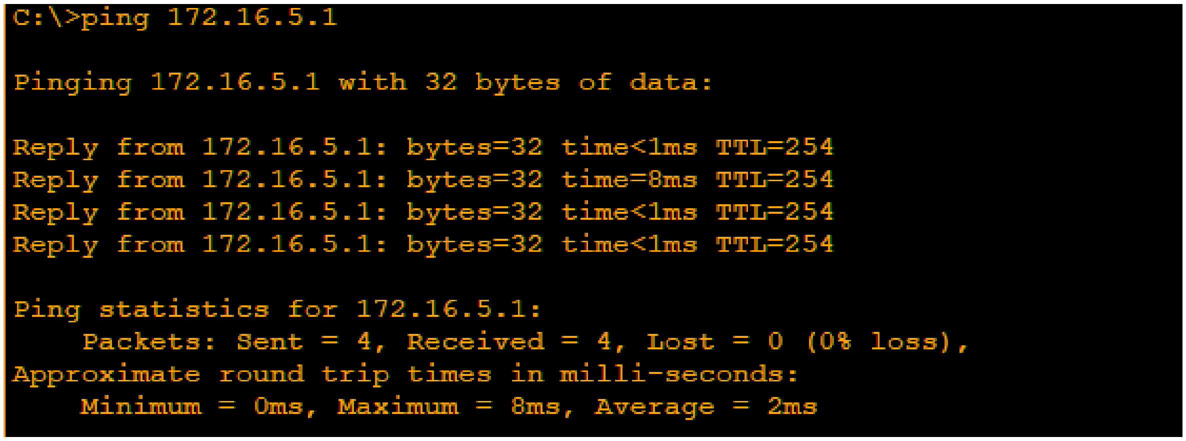
```
ciscoasa#show xlate
1 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s -
static, T - twice, N - net-to-net
NAT from DMZ:172.16.20.3/32 to OUTSIDE:172.16.5.250/32 flags s idle 02:29:45,
timeout 0:00:00

ciscoasa#
```



```
ciscoasa#show nat
Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
    translate_hits = 9, untranslate_hits = 8
2 (DMZ) to (OUTSIDE) source static PC-DMZ 172.16.5.250
    translate_hits = 0, untranslate_hits = 0

ciscoasa#
```

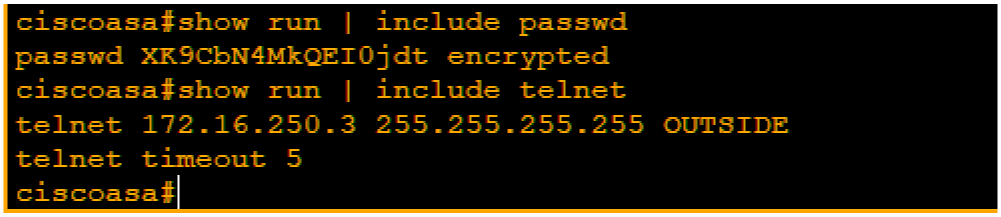


```
ciscoasa#show run | section policy
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect icmp
  inspect tftp
service-policy global_policy global
ciscoasa#
```

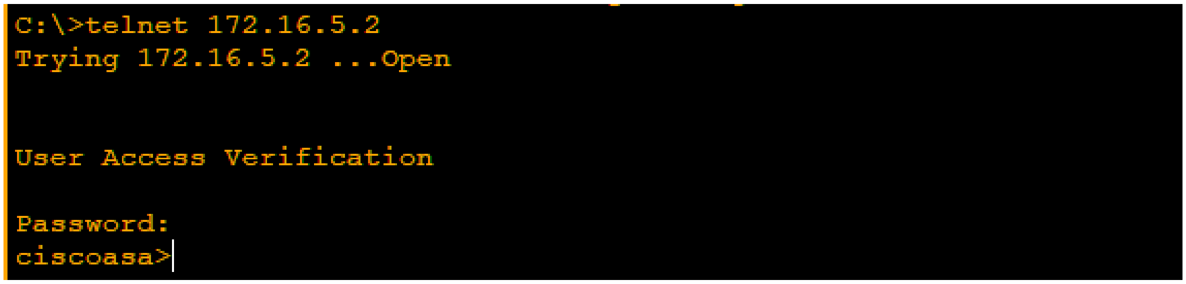


```
C:\>ping 172.16.5.1

Pinging 172.16.5.1 with 32 bytes of data:

Reply from 172.16.5.1: bytes=32 time<1ms TTL=254
Reply from 172.16.5.1: bytes=32 time=8ms TTL=254
Reply from 172.16.5.1: bytes=32 time<1ms TTL=254
Reply from 172.16.5.1: bytes=32 time<1ms TTL=254

Ping statistics for 172.16.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

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



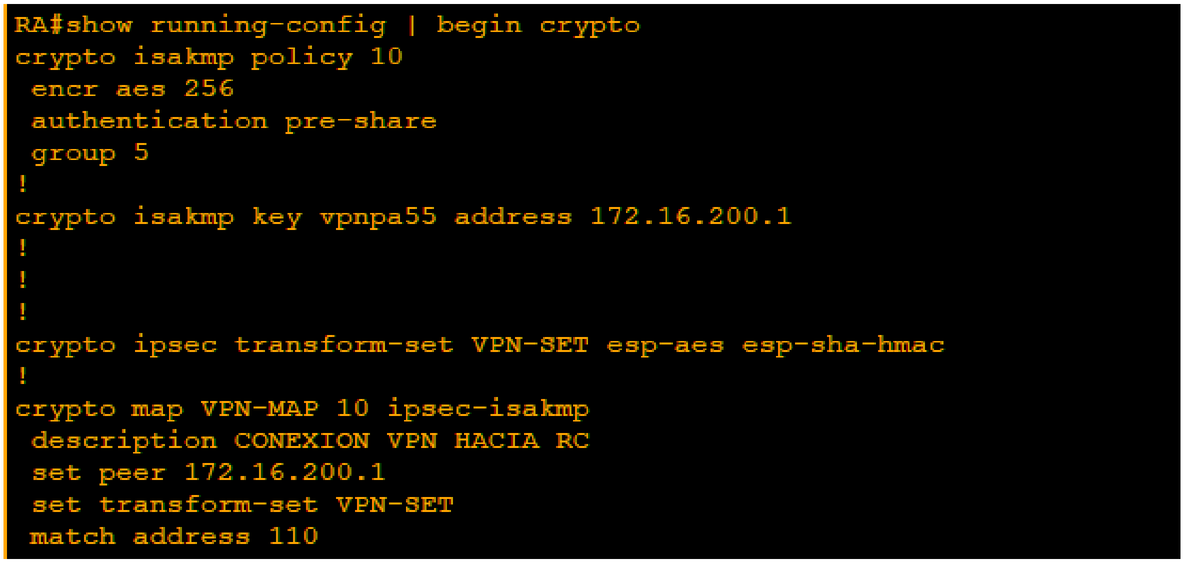
```
ciscoasa#show run | include passwd
passwd XK9CbN4MkQEI0jdt encrypted
ciscoasa#show run | include telnet
telnet 172.16.250.3 255.255.255.255 OUTSIDE
telnet timeout 5
ciscoasa#
```



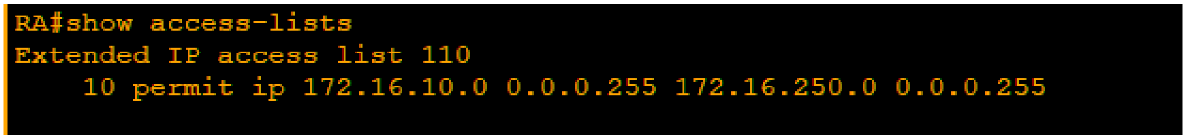
```
C:\>telnet 172.16.5.2
Trying 172.16.5.2 ...Open


User Access Verification

Password:
ciscoasa>
```

Implementar VPN Site to Site entre RA y RC (Realizar pruebas que validen su funcionamiento)

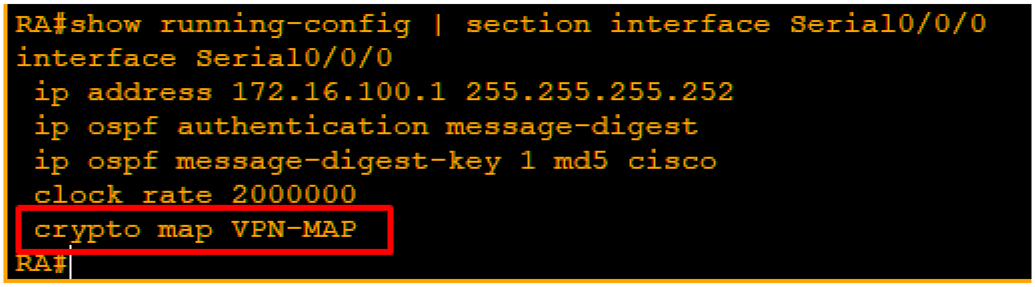
RA



```
RA#show running-config | begin crypto
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 172.16.200.1
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description CONEXION VPN HACIA RC
 set peer 172.16.200.1
 set transform-set VPN-SET
 match address 110
```

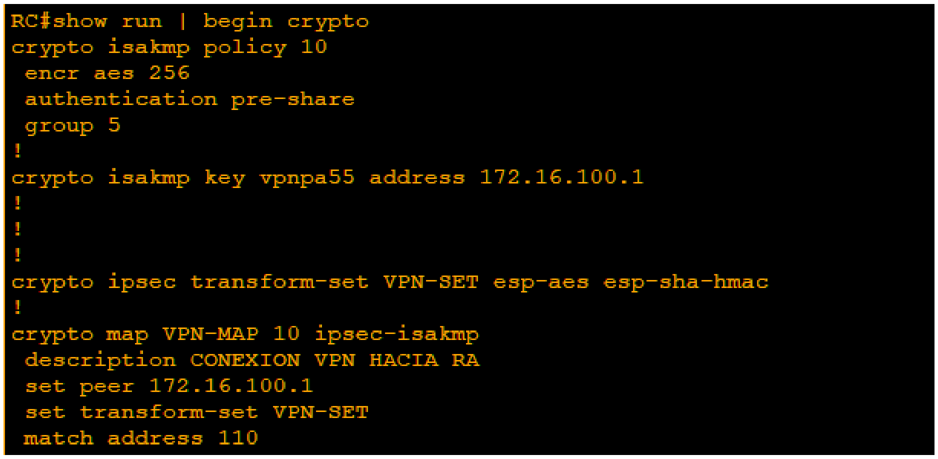


```
RA#show access-lists
Extended IP access list 110
    10 permit ip 172.16.10.0 0.0.0.255 172.16.250.0 0.0.0.255
```

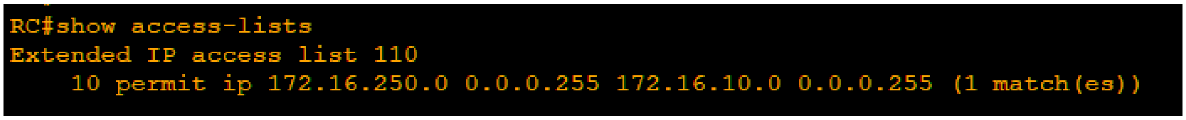


```
RA#show running-config | section interface Serial0/0/0
interface Serial0/0/0
 ip address 172.16.100.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 clock rate 2000000
 crypto map VPN-MAP
RA#
```

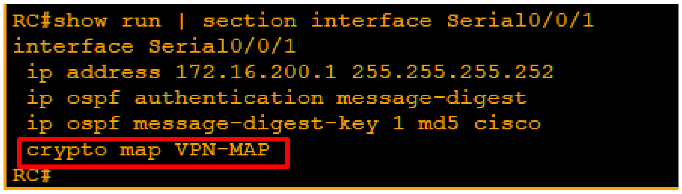
RC



```
RC#show run | begin crypto
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpa55 address 172.16.100.1
!
!
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description CONEXION VPN HACIA RA
 set peer 172.16.100.1
 set transform-set VPN-SET
 match address 110
```

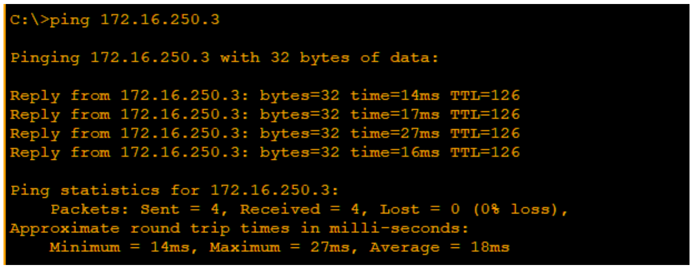


```
RC#show access-lists
Extended IP access list 110
    10 permit ip 172.16.250.0 0.0.0.255 172.16.10.0 0.0.0.255 (1 match(es))
```

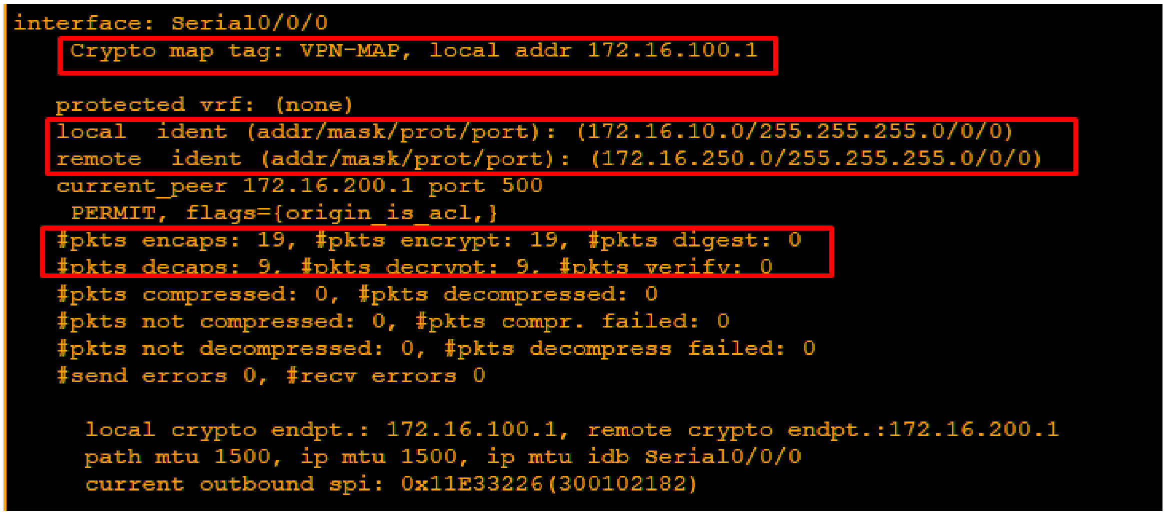


```
RC#show run | section interface Serial0/0/1
interface Serial0/0/1
 ip address 172.16.200.1 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 crypto map VPN-MAP
RC#
```

VALIDACIÓN VPN



```
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=14ms TTL=126
Reply from 172.16.250.3: bytes=32 time=17ms TTL=126
Reply from 172.16.250.3: bytes=32 time=27ms TTL=126
Reply from 172.16.250.3: bytes=32 time=16ms TTL=126

Ping statistics for 172.16.250.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 27ms, Average = 18ms
```



```
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: 19, #pkts encrypt: 19, #pkts digest: 0
   #pkts decaps: 9, #pkts decrypt: 9, #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 0, #recv errors 0

     local crypto endpt.: 172.16.100.1, remote crypto endpt.:172.16.200.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x11E33226(300102182)
```

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

Política de Control de Acceso: Uso de VPN Site-to-Site entre Routers RA y RC

Objetivo

El objetivo de esta política es garantizar la seguridad y eficiencia del túnel VPN site-to-site entre los routers RA y RC, protegiendo los datos, asegurando la continuidad del negocio y optimizando el rendimiento y uso eficiente de la red.

Alcance

Esta política se aplica a todo el tráfico de red que transita por la VPN, así como a todos los dispositivos y usuarios que accedan a recursos de las redes conectadas a través de los routers RA y RC.

Lineamientos Generales

Tráfico Permitido: Se permitirá únicamente el tráfico necesario para las operaciones de negocio. El tráfico no esencial será bloqueado o se le dará baja prioridad.

Autenticación y Cifrado: La conexión VPN debe usar cifrado robusto (p. ej., AES-256) y autenticación fuerte. Las claves de autenticación deben rotarse cada 90 días.

Priorización de Tráfico (QoS): Se priorizará el tráfico crítico (como VoIP y videoconferencias) para asegurar un rendimiento óptimo. El tráfico de menor importancia tendrá una prioridad más baja.

Uso de Ancho de Banda: Se monitoreará el uso del ancho de banda de la VPN para prevenir cuellos de botella y asegurar un dimensionamiento adecuado.

Seguridad y Monitoreo: Se implementarán firewalls y se mantendrán registros de actividad (logs) que serán auditados para detectar anomalías. Se utilizarán sistemas de detección de intrusiones (IDS/IPS).

Sanciones por Incumplimiento

El incumplimiento de esta política se considera una falta grave y estará sujeto a las siguientes sanciones:

Advertencia formal: Se emitirá una advertencia por escrito y se podrá restringir temporalmente el acceso a servicios no críticos.

Suspensión de acceso: En caso de reincidencia, se suspenderá temporalmente el acceso a la red y a la VPN. Se requerirá una capacitación obligatoria en seguridad.

Terminación de acceso: Las faltas graves o el incumplimiento reiterado pueden resultar en la revocación permanente del acceso a la red, y se podrán iniciar acciones disciplinarias o legales según corresponda.