PRÁCTICA 6

Firewall ACL

Carlos Cano Espinosa

ÍNDICE

Enunciado

1. En esta sesión de laboratorio vamos a utilizar un router configurado mediante ACLs para construir un firewall (cortafuegos) que permita proteger nuestra red interna del exterior (Internet).

2. Se crearán tres zonas:
    a. Intranet
    b. Zona desmilitarizada (DMZ) donde estarán los servidores a los que se podrá acceder desde el exterior
    c. Internet

3. Comprueba la configuración de los equipos con las siguientes direcciones IP y el routing:

    - Red local privada: 172.16.0.0/16
    - Red de servidores públicos: 150.30.0.0/16
    - Red WAN: (Enlace entre routers) 10.0.0.0/30
    - INTERNET: 198.3.2.0/24

4. Prueba la conectividad y el acceso web al servidor desde el Desktop de los PCs que están en la Intranet y en Internet.

5. Queremos proteger la red interna de intrusos. Diseña las listas de acceso necesarias para que:

    a. Los terminales externos (INTERNET) e internos (INTRANET) sólo puedan acceder a los servicios Web y FTP de la red de servidores.
    b. Los terminales externos (INTERNET) y los servidores de la DMZ no puedan realizar ninguna conexión a la zona privada (INTRANET)
    c. Los equipos conectados a la red local privada (INTRANET) tengan pleno acceso a Internet.

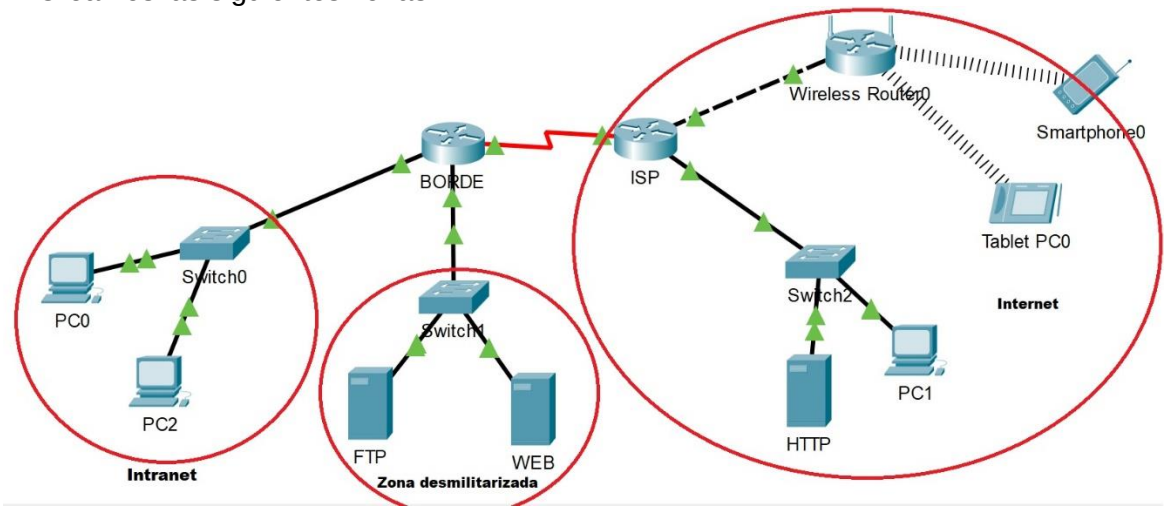
6. Decide donde has de poner las listas de acceso y configura el firewall. Puedes poner tantas listas de acceso como creas necesario, pero has de limitarlas al mínimo posible.

7. Escribe la configuración necesaria que has utilizado.

8. Prueba el funcionamiento de las ACLs ayudándote de la herramienta de simulación.

Solución

2. Creamos las siguientes zonas:



4. Realizamos un ping desde el PC0 al PC1 y podemos comprobar que no hay ningún problema de conectividad

6.Para que los servidores estén protegidos debemos poner la lista de acceso justo en la interfaz en la que están conectados los servidores.
Para que la intranet este protegida debemos poner la lista de acceso justo en la interfaz en la que están conectados los equipos.
Para que la intranet tenga plena acceso a internet no hay que poner ninguna lista.
7.

```
en
conf t
access-list 100 permit tcp any host 150.30.0.3 eq 80
access-list 100 permit tcp any host 150.30.0.3 eq 443
access-list 100 permit tcp any host 150.30.0.3 eq 53
access-list 100 permit udp any host 150.30.0.3 eq 53
access-list 100 permit tcp any host 150.30.0.2 eq 21
access-list 100 permit tcp any host 150.30.0.2 eq 20
access-list 100 deny ip any any

access-list 101 permit tcp any 172.16.0.0 0.0.255.255 established
access-list 101 permit udp host 150.30.0.100 eq 53 172.16.0.0 0.0.255.255
access-list 101 deny ip any any

int g0/0
ip access-group 101 out
```

```
exit

int g0/1
ip access-group 100 out
exit
```