PRÁCTICA: CONSTRUCCIÓN DE UN CORTAFUEGOS: LISTAS DE ACCESO. ACL´s (Access Control Lists) EN EL ROUTER.

Sesión de laboratorio

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.

   He decidido poner las listas de acceso en las interfaces de salida porque si las hubiese puesto en las entradas, tendría que haber configurado el firewall para que no descartara los paquetes de ruta que se intercambian ambos routers.

7. Escribe la configuración necesaria que has utilizado.

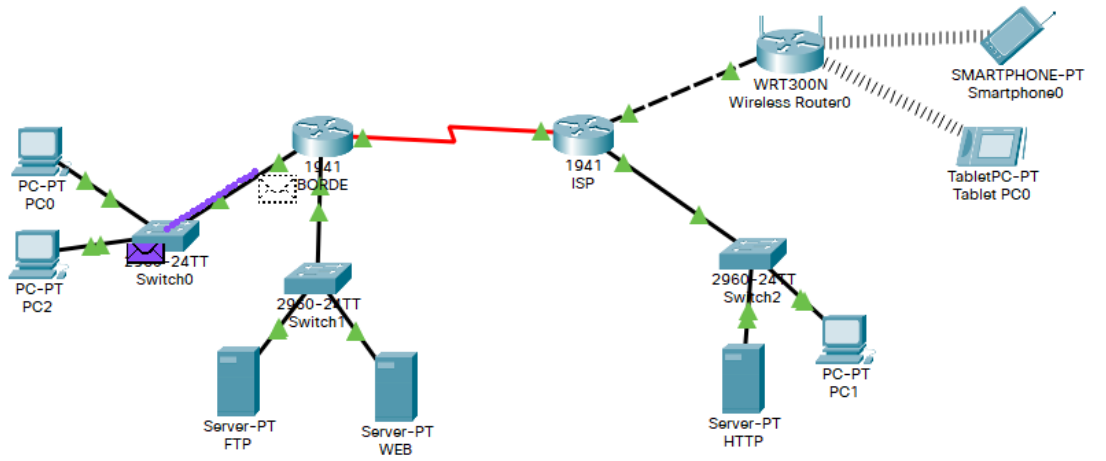
Para la interfaz gigabitEthernet 0/0 he usado la siguiente configuración:
access-list 100 permit tcp any host 150.30.0.2 eq 20
access-list 100 permit tcp any host 150.30.0.2 eq 21
access-list 100 permit tcp any host 150.30.0.3 eq 80
access-list 100 deny ip any any
int g0/1

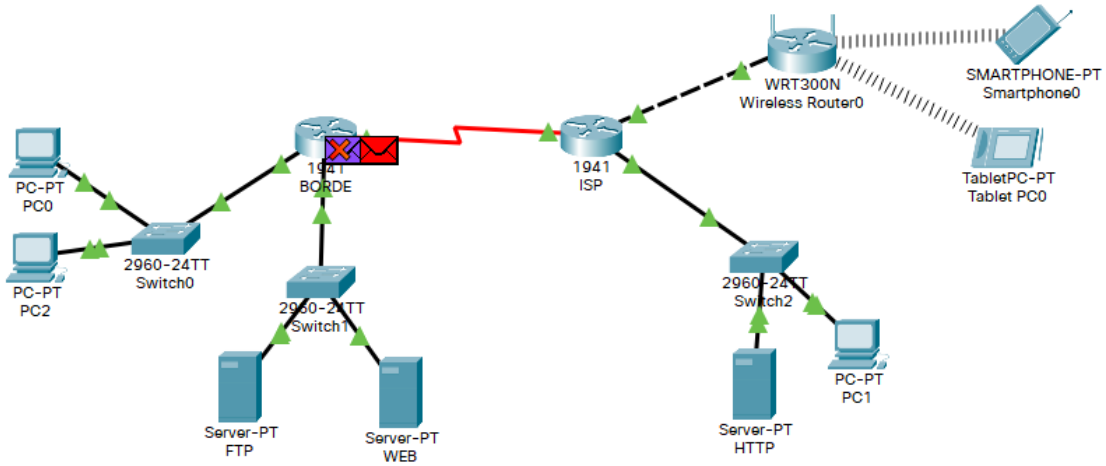
Para la interfaz gigabitEthernet 0/1 he usado la siguiente configuración:
ip access-group 100 out
access-list 101 permit tcp any 172.16.0.0 0.0.255.255
access-lits 101 deny ip any any
int g0/0
ip access-group 101 out

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

Con la herramienta de simulación podemos ver como no nos deja enviar un PING al servidor Web, mientras que sí nos permite acceder desde el navegador del equipo. Esto es porque hemos configurado en la lista de acceso que solo se pueda acceder al servidor web por el puerto 80 (HTTP) y hemos denegado todo lo demás.

Las siguientes imágenes muestran como se descarta la trama ICMP (ping).





La siguiente imagen muestra como permite acceder al servidor web: