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.

Las listas de acceso se configuran en el Router borde, también hace de Firewall.

7. Escribe la configuración necesaria que has utilizado.

Lista de acceso 100 aplicada como regla de salida en la interfaz G0/1 de BORDE:
access-list 100 remark Allow Web y FTP
permit tcp any host 150.30.0.3 eq www
permit tcp any host 150.30.0.2 eq ftp
deny ip any any

Lista de acceso 101 aplicada como regla de salida en la interfaz G0/0 de BORDE:
access-list 101 remark Acceso intranet
permit tcp any 172.16.0.0 0.0.255.255 established
deny ip any any

Se niega todo el tráfico que entre en intranet que no sea TCP de una conexión ya establecida. De este modo intranet tiene acceso a Internet, pero ni Internet ni DMZ pueden iniciar conexiones con Intranet, solo pueden aceptarlas.

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