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 Pertenecen el PC0 y PC2
   - Red de servidores públicos: 150.30.0.0/16 Son los servidores FTP y WEB
   - Red WAN: (Enlace entre routers) 10.0.0.0/30 El router ISP y BORDE
   - Zona DMZ: 198.3.2.0/24 Son el PC1 y el servidor HTTP

4. Prueba la conectividad y el acceso web al servidor desde el Desktop de los PCs que están en la Intranet y en Internet.
   Al tratar de conectarse desde un PC de Intranet a Internet, el ping nunca llega debido al que el destino es inaccesible por la NAT.

   Pero al contrario, de Internet a Intranet si que llega el ping.

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.

   La lista del Router BORDE será:

```
enable
conf t
access-list 100 permit tcp 172.16.0.1 0.0.255.255 host 150.30.0.2 eq ftp
access-list 100 permit tcp 172.16.0.1 0.0.255.255 host 150.30.0.3 eq 80
access-list 100 permit tcp 198.3.2.1 0.0.0.255 host 150.30.0.2 eq ftp
access-list 100 permit tcp 198.3.2.1 0.0.0.255 host 150.30.0.2 eq 80
int s0/1/0
ip access-group 100 out
end
```

b. Los terminales externos (INTERNET) y los servidores de la DMZ no puedan realizar ninguna conexión a la zona privada (INTRANET)

La lista del Router BORDE será:

```
enable
conf t
access-list 101 deny tcp 198.3.2.1 0.0.0.255 198.3.2.1 0.0.0.255
access-list 101 deny tcp any 175.16.0.0 0.0.255.255
int g0/0
ip access-group 101 out
exit
int s0/1/0
ip access-group 101 in
exit
int g0/1
ip access-group 101 in
end
```

c. Los equipos conectados a la red local privada (INTRANET) tengan pleno acceso a Internet.

La lista del Router ISP será:

```
enable
conf t
access-list 102 permit tcp any 172.16.0.0 0.0.255.255
int s0/1/0
ip acces-group 102 in
end
```

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.
Creo las listas de acceso 100, 101 y 102. Las dos primeras irán en el router BORDE, y la última va en el router ISP.

7. Escribe la configuración necesaria que has utilizado.
Mirar el punto 5

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