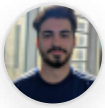

CarlosGarSil98
www.wuolah.com/student/CarlosGarSil98

Practica-6.pdf

Práctica 6

3° Interconexión de Redes de Computadores

Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería
Universidad de Huelva

Práctica 6: Construcción de cortafuegos. ACL

Topología

Objetivos

Parte 1: Verificación de requisitos y configuración

Parte 2: Construcción del cortafuegos

Parte 3: Prueba de la correcta configuración

Parte 1: Verificación de requisitos y configuración

Paso 1: Localizar las diferentes zonas

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). Se crearan tres zonas:

- Intranet.
- Zona desmilitariazada (DMZ) donde estarán los servidores a los que se podrá acceder desde el exterior.
- Internet.

Paso 2: Comprobar conexiones y direcciones IP

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

Paso 3: Probar conectividad desde los PCs al servidor

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

PC0----------

C:\>ping 150.30.0.3

Pinging 150.30.0.3 with 32 bytes of data:

Request timed out.
Reply from 150.30.0.3: bytes=32 time=1ms TTL=127
Reply from 150.30.0.3: bytes=32 time=17ms TTL=127
Reply from 150.30.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 150.30.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 17ms, Average = 6ms

PC1----------

C:\>ping 150.30.0.3

Pinging 150.30.0.3 with 32 bytes of data:

Reply from 150.30.0.3: bytes=32 time=2ms TTL=126
Reply from 150.30.0.3: bytes=32 time=12ms TTL=126
Reply from 150.30.0.3: bytes=32 time=1ms TTL=126
Reply from 150.30.0.3: bytes=32 time=11ms TTL=126

Ping statistics for 150.30.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 6ms

PC2----------

C:\>ping 150.30.0.3

Pinging 150.30.0.3 with 32 bytes of data:

Reply from 150.30.0.3: bytes=32 time<1ms TTL=127
Reply from 150.30.0.3: bytes=32 time=1ms TTL=127
Reply from 150.30.0.3: bytes=32 time<1ms TTL=127
Reply from 150.30.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 150.30.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

Parte 2: Construcción de cortafuegos

Paso 1: Diseño de lista de acceso

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

a. Los terminales externos (INTERNET) e internos (INTRANET) solo puedan acceder alos servicios Web y FTP de la red de servidores.
b. Los terminales externos (INTERNET) y los servidores 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.

Paso 2: Toma de decisiones

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. Escribe la configuración que has utilizado.

Pondremos las listas en el router BORDE, ya que por él pasan todas las posibles conexiones entre las diferentes redes.

```
BORDE> ena
BORDE# config terminal
(* Copiar y pegar en el programa *)

access-list 100 remark Permitir Acceso Servidores
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 permit tcp any host 150.30.0.3 eq 80
Access-list 100 deny ip any any

access-list 101 remark Acceso Intranet
access-list 101 deny tcp any 172.16.0.0 0.0.255.255 established
Access-list 101 deny ip any any

int g0/1
ip access-group 100 out

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