Facultad: Ingeniería
Escuela: Electrónica
Asignatura: Interconexión de Redes de Datos

Tema: ACLs Parte II

Contenidos

- Configuración básica
- Creación y aplicación de ACLs extendidas

Objetivos Específicos

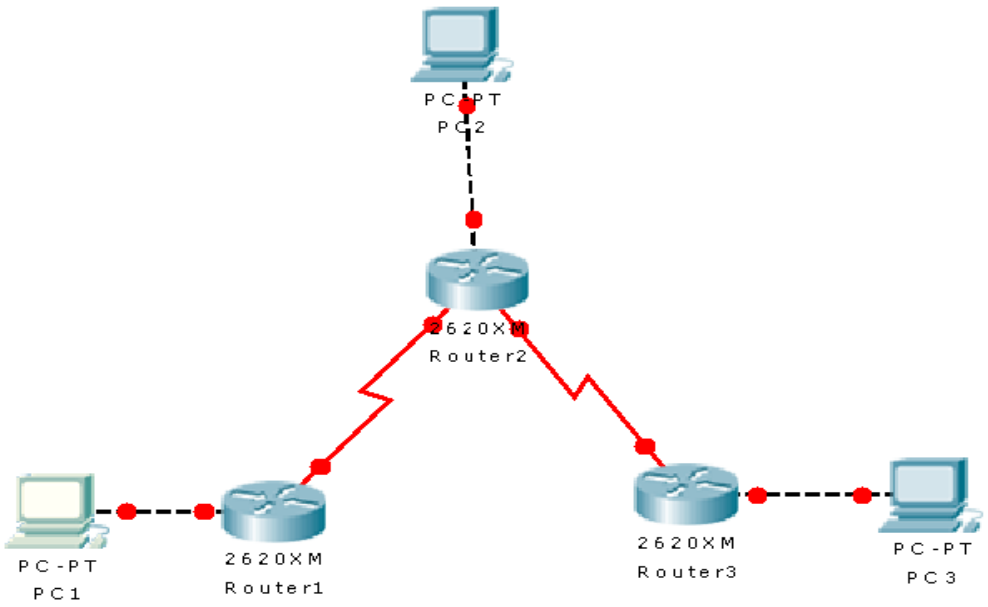
- Crear listas de control de acceso extendidas
- Poder ubicar las listas de control de acceso en el router

Materiales y Equipo

- Computadora con simulador Packet Tracer
- 3 router
- 3 Computadoras
- 3 Cables seriales
- 3 Cables de consola
- 3 Convertidores serial a USB

Procedimiento

1. Armar la siguiente topología en el simulador.



NOTA: En esta configuración las dos interfaces del Router2 usan cables DCE

2. Borre las configuraciones de los router.

   Router#erase startup-config
   Router#reload

Configuración básica.

3. Configuración de los routers

a) Router1
- Nombre de host: BORDE
- Contraseña de privilegiado encriptada: class
- Contraseña de terminales virtuales (vty): ciscotel
- Dirección y máscara de Eth0: 200.100.50.1 /24
- Dirección y máscara de S0: 204.204.7.1/30

b) Router2
- Nombre de host: CENTRO
- Contraseña de privilegiado encriptada: class
- Contraseña de terminales virtuales (vty): ciscotel
- Dirección y máscara de Eth0: 206.93.105.1 /24
- Dirección y máscara de S0: 204.204.7.2/30
- Dirección y máscara de S1: 201.100.11.1/30

c) Router3
- Nombre de host: EXTREMO
- Contraseña de privilegiado encriptada: cisco
- Contraseña de terminales virtuales (vty): ciscotel
- Dirección y máscara de Eth0: 199.6.13.1 /24
- Dirección y máscara de S0: 201.100.11.2/30

4. Configuración de las estaciones de trabajo

PC-1: Dirección ip: 200.100.50.2, máscara de subred: 255.255.255.0, gateway: 200.100.50.1
PC-2: Dirección ip: 206.93.105.2, máscara de subred: 255.255.255.0, gateway: 206.93.105.1
PC-3: Dirección ip: 199.6.13.2, máscara de subred: 255.255.255.0, gateway: 199.6.13.1

5. Configure RIPv2 en los tres enrutadores

6. Use el comando *show ip route* para verificar que en cada router aparezcan las rutas.

7. Realizar pruebas de conectividad entre computadoras con los comandos ping y traceroute

8. Almacenar los cambios hechos en la configuración en la NVRAM

9. En cualquier momento que quiera verificar el funcionamiento de una línea en específico de una ACL, utilice el comando *show access-lists*, el cual muestra las listas de control de acceso y las coincidencias (matches) en cada línea.

10. Desde las PCs verifique el acceso por telnet a todos los router.

telnet 204.204.7.1
telnet 201.100.11.1
telnet 201.100.11.2

Creación y aplicación de ACLs extendidas.

Ejemplo I

1. Configurar ACL's extendidas que denieguen las sesiones telnet desde cualquiera de las estaciones de trabajo (excepto de la PC-1) hacia BORDE. Cualquier otro tipo de tráfico será permitido.

Opción 1: Una sola ACL ubicada en BORDE (el tráfico atravesará toda la red y será detenido en la interfaz serial 0 de BORDE).

2. Configuración y ubicación de la ACL

BORDE#configure terminal
BORDE(config)#access-list 101 deny tcp any host 204.204.7.1 eq 23
BORDE(config)#access-list 101 deny tcp any host 200.100.50.1 eq 23
BORDE(config)#access-list 101 permit ip any any
BORDE(config)#interface serial 0
BORDE(config-if)#ip access-group 101 in
BORDE(config-if)#CTRL+Z

3. Intentar establecer sesiones telnet desde las estaciones PC-2 y PC-3. Los intentos deben fallar. Solamente desde PC-1 podrá establecer una conexión vía telnet exitosamente.

4. Desactivar la ACL de la interfaz serial 0 de BORDE y comprobar que se pueden establecer sesiones telnet desde PC-2 y PC-3.

Opción 2: ACL's independientes en CENTRO y EXTREMO (el tráfico será detenido lo más cerca posible del origen para no tener utilización innecesaria del ancho de banda en conexiones que serán denegadas).

5. Configuración y ubicación de ACL en CENTRO

CENTRO#configure terminal
CENTRO(config)#access-list 102 deny tcp any host 204.204.7.1 eq 23
CENTRO(config)#access-list 102 deny tcp any host 200.100.50.1 eq 23
CENTRO(config)#access-list 102 permit ip any any
CENTRO(config)#interface Ethernet 0
CENTRO(config-if)#ip access-group 102 in
CENTRO(config-if)#CTRL+Z

6. Configuración y ubicación de ACL en EXTREMO

EXTREMO#configure terminal
EXTREMO(config)#access-list 103 deny tcp any host 204.204.7.1 eq 23
EXTREMO(config)#access-list 103 deny tcp any host 200.100.50.1 eq 23
EXTREMO(config)#access-list 103 permit ip any any
EXTREMO(config)#interface Ethernet 0
EXTREMO(config-if)#ip access-group 103 in
EXTREMO(config-if)#CTRL+Z

7. Nuevamente realizar pruebas intentando conectarse vía telnet con BORDE. Las conexiones desde PC-2 y PC-3 deben fallar.

8. Desactivar las ACL's de las interfaces ethernet en los router CENTRO y EXTREMO

Configurar ACL's extendidas que permitan filtrar tráfico por tipo de servicios y por dirección de origen y destino.

Ejemplo II

9. Restringir el ping a los host con IPs pares dentro de la red LAN de EXTREMO

EXTREMO#configure terminal
EXTREMO(config)#access-list 104 permit icmp any 199.13.6.0 0.0.0.254
EXTREMO(config)#access-list 104 permit ip any any
EXTREMO(config)#interface Ethernet 0
EXTREMO(config-if)#ip access-group 104 out
EXTREMO(config-if)#CTRL+Z

10. Realizar pruebas de ping con diferentes IP dentro de la red LAN de EXTREMO, las pruebas deberán ser exitosas si el ping es dirigido a una ip par, para esto cambie la IP de PC3 con direcciones pares e impares y realizar pruebas desde las PC1 y PC2 hacia PC3

11. Desactivar la ACL.

Ejemplo III

12. Ejemplo de control de las líneas vty de CENTRO en una forma tradicional. Solo se permitirán las sesiones telnet iniciadas en la red correspondiente a la PC-2. Las redes a las que pertenecen las estaciones PC-1 y PC-3 serán denegadas. Todo el demás tráfico (que no sea telnet) será permitido.

a) Configuración de la ACL en CENTRO

CENTRO#configure terminal
CENTRO(config)#access-list 105 deny tcp 200.100.50.0 0.0.0.255 host 204.204.7.2 eq 23
CENTRO(config)#access-list 105 deny tcp 200.100.50.0 0.0.0.255 host 201.100.11.1 eq 23
CENTRO(config)#access-list 105 deny tcp 200.100.50.0 0.0.0.255 host 206.93.105.1 eq 23
CENTRO(config)#access-list 105 deny tcp 199.13.6.0 0.0.0.255 host 204.204.7.2 eq 23

CENTRO(config)#access-list 105 deny tcp 199.13.6.0 0.0.0.255 host 201.100.11.1 eq 23
CENTRO(config)#access-list 105 deny tcp 199.13.6.0 0.0.0.255 host 206.93.105.1 eq 23
CENTRO(config)#access-list 105 permit ip any any

b) Ubicación de la ACL
CENTRO(config)#interface serial 0
CENTRO(config-if)#ip access-group 105 in
CENTRO(config-if)#exit
CENTRO(config)#interface serial 1
CENTRO(config-if)#ip access-group 105 in
CENTRO(config-if)#CTRL+Z

13. Realizar las pruebas necesarias para verificar el funcionamiento deseado de la ACL. Solo la PC-2 podrá exitosamente administrar CENTRO vía telnet.

14. Desactivar las ACL's

Alternativa usando control de las VTY's
Ejemplo IV

Configuración de la ACL (siempre en CENTRO)

CENTRO#configure terminal
CENTRO(config)#access-list 1 permit 206.93.105.0 0.0.0.255
CENTRO(config)#access-list 1 deny any
CENTRO(config)#line vty 0 4
CENTRO(config-line)#access-class 1 in
CENTRO(config-line)#CTRL+Z

15. Verificar nuevamente el funcionamiento de la ACL y comprobar que solamente PC-2 puede administrar CENTRO vía telnet.

16. Desactivar las ACL's

Ejercicio I

17. Sustituya PC-2 por un servidor con ip 206.93.105.240 /24. Configure listas de acceso para los siguientes requerimientos:

    a) No se permitirá hacer ping al servidor desde las redes EXTREMO Y BORDE.
    b) Se permitirá servicio WEB (puerto 80) a las primeras 15 IP's de la red EXTREMO y a las ultimas 15 IP's de la red BORDE.
    c) Se permitirá servicio FTP (puerto 21) solamente de la red EXTREMO cuyas IP's sean pares.
    d) Entre las redes EXTREMO y BORDE, se permitirá hacer ping entre las ultimas 15 IP's (EXTREMO) con las primeras 15 IP's (BORDE).

Bibliografía

- Network+ 2005 In Depth, Tamara Dean; Course Technology PTR; 1 edition (March 15, 2005)
- Local Area Networks (McGraw-Hill Forouzan Networking Series), Forouzan McGraw-Hill Education - Europe (February 1, 2002)
- CCNA Study Guide Fourth Edition, Sybex
- Guias Practicas de la FET, REDES WAN

Hoja de cotejo: 1

Guía 9: ACLs Parte II

Alumno: Máquina No:

Docente: GL: Fecha:

EVALUACION					
	%	**1-4**	**5-7**	**8-10**	**Nota**
CONOCIMIENTO	Del 20 al 30%	Conocimiento deficiente de los fundamentos teóricos	Conocimiento y explicación incompleta de los fundamentos teóricos	Conocimiento completo y explicación clara de los fundamentos teóricos	
APLICACIÓN DEL CONOCIMIENTO	Del 40% al 60%				
ACTITUD	Del 5% al 10%	No tiene actitud proactiva.	Actitud propositiva y con propuestas no aplicables al contenido de la guía.	Tiene actitud proactiva y sus propuestas son concretas.	
TOTAL	100%				