**Mejores prácticas para el diseño de ACLs EXTENDIDA**

**1. Identificar la fuente (tráfico fuente) y el destino**

**2. Trazar el trayecto del tráfico no permitido.**

**3. Trazar el trayecto del tráfico permitido.**

**4. Identificar el router donde se instalará la lista de control de acceso.**

**5. Identificar la interfaz donde se va a asociar la lista de control de acceso.**

**6. Escribir la ACL, instalarla y probarla.**

**NOTA: Realizar pruebas de conectividad antes y después de instalar una ACL**

**REGLA:**

**1. LAS LISTAS DE ACCESO ESTÁNDAR SE DEBEN INSTALAR LO MAS CERCA DEL**

**DESTINO.**

**2. LAS LISTAS DE ACCESO EXTENDIDAS SE DEBEN INSTALAR LO MAS CERCA DEL**

**ORIGEN. PARA EVITAR QUE EL TRÁFICO LLEGUE A LUGARES DONDE NO**

**NECESITE LLEGAR.**

**------------------------------------------------------------**

**Ejercicio 1.**

**------------------------------------------------------------**

**a. Diseña una lista de control de acceso estándar para impedir**

**que las computadoras de la subred de Alumnos tengan acceso**

**a la subred de Directivos.**

**¿En qué router instalarás esta lista de control de acceso?**

**RouterA**

**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any**

**int g0/0**

**ip access-group 10 out**

**------------------------------------------------------------**

**Ejercicio 2.**

**------------------------------------------------------------**

**b. Diseña una lista de control de acceso estándar para impedir que**

**las computadoras de la subredes de Profesores y Alumnos tengan acceso**

**a la subred de Directivos.**

**RouterA**

**access-list 20 deny 132.254.89.232 0.0.0.7**

**access-list 20 deny 132.254.89.0 0.0.0.127**

**access-list 20 permit any**

**int g0/0**

**ip access-group 20 out**

**------------------------------------------------------------**

**Ejercicio 3.**

**------------------------------------------------------------**

**c. Diseña una lista de control de acceso estándar para que el**

**visitante 01 no pueda acceder a la sección de servidores**

**RouterA**

**access-list 30 deny 132.254.89.120 0.0.0.0**

**access-list 30 permit any**

**int g0/1**

**ip access-group 30 out**

**------------------------------------------------------------**

**Ejercicio 4.**

**------------------------------------------------------------**

**a. Diseña una lista de control de acceso estándar para impedir que**

**las computadoras de los Alumnos tengan acceso a la**

**subred de Directivos y a la subred de Profesores.**

**Router A y B**

**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any**

**int g0/0**

**ip access-group 10 out**

**------------------------------------------------------------**

**Ejercicio 5.**

**------------------------------------------------------------**

**b. Diseña una lista de control de acceso extendida para impedir que**

**las computadoras de los Alumnos tengan acceso a la**

**subred de Directivos y a la subred de Profesores.**

**Router B**

**access-list 110 deny ip 132.254.89.0 0.0.0.127 132.254.89.192 0.0.0.31**

**access-list 110 deny ip 132.254.89.0 0.0.0.127 132.254.89.232 0.0.0.7**

**access-list 110 permit ip any any**

**int g0/1**

**ip access-group 110 in**

**------------------------------------------------------------**

**Ejercicio 6.**

**------------------------------------------------------------**

**Diseña una lista de control de acceso extendida para impedir**

**que las computadoras de la subred de Profesores tengan acceso**

**al server de la subred de Directivos.**

**Router B**

**!access-list 120 deny ip 132.254.89.232 0.0.0.7 132.254.89.221 0.0.0.0 Equipo no cisco**

**!host lo permite CISCO**

**access-list 120 deny ip 132.254.89.232 0.0.0.7 host 132.254.89.221**

**access-list 120 permit ip any any**

**int g0/0**

**ip access-group 120 in**

**------------------------------------------------------------**

**Ejercicio 7.**

**------------------------------------------------------------**

**e.Diseña una lista de control de acceso extendida para que la sección de Alumnos no pueda**

**acceder al servidor de profesores vía el protocolo WEB ni por FTP.**

**Router B**

**access-list 140 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.238 eq 20**

**access-list 140 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.238 eq 21**

**access-list 140 deny tcp 132.254.89.0 0.0.0.127 host 132.254.89.238 eq 80**

**access-list 140 permit ip any any**

**int G0/1**

**ip access-group 140 in**

**------------------------------------------------------------**

**Ejercicio 8.**

**------------------------------------------------------------**

**g. Diseña una lista de control de acceso extendida para que ninguna**

**dirección IP interna de nuestra red pueda acceder al servidor de**

**LOL vía el protocolo WEB.**

**Router B**

**access-list 150 deny tcp any host 111.65.32.1 eq 80**

**access-list 150 permit ip any any**

**int s0/0/0**

**ip access-group 150 out**