1. Diseña una lista de control de **acceso estándar** (5) que **impida** que las computadoras de la subred de **Alumnos** tengan acceso a la subred de **Servidores**

router(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

**Router A**

**access-list 5 deny 132.254.89.0 0.0.0.127**

**access-list 5 permit any**

**int g0/1**

**ip access-group 5 out**

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping**  (Fail / Success) |
| **Alumno A** | **Murillo** | **132.254.89.130** | Fail |
| **Alumno A** | **Server Directivos** | **132.254.89.221** | Success |
| **Alumno A** | **Server Profesores** | **132.254.89.238** | Success |
| **Alumno A** | **Facebook.com** | **65.0.1.10** | Success |

1. Diseña una lista de control de **acceso estándar** (10) que **impida** que las computadoras de la subred de **Alumnos** tengan acceso a la subred de **Profesores**

router(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

**Router 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**

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping**  (Fail / Success) |
| **Alumno B** | **Escolar** | **132.254.89.131** | Success |
| **Alumno A** | **Server Directivos** | **132.254.89.221** | Success |
| **Alumno A** | **Server Profesores** | **132.254.89.238** | Fail |
| **Alumno A** | **LOL.com** | **111.65.32.1** | Success |

1. Diseña una lista de control de **acceso extendida** (100) que **impida** que las computadoras de la subred de **Alumnos y Profesores** tengan acceso externo a los servicios de **WEB** del servidor **LOL.com**. El resto de las direcciones IP pueden acceder sin restricción a todos los servicios de Internet incluyendo todo el tráfico que no sea **WEB** y se dirija al servidor de **LOL.com**

router(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

**Router B**

**access-list 100 deny tcp 132.254.89.0 0.0.0.127 host 111.65.32.1 eq 80**

**access-list 100 deny tcp 132.254.89.232 0.0.0.7 host 111.65.32.1 eq 80**

**access-list 100 permit ip any any**

**int s0/0/0**

**ip access-group 100 out**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Alumno B** | **LOL.com** | **111.65.32.1** | Fail | Success |
| **Profesor A** | **LOL.com** | **111.65.32.1** | Fail | Success |
| **Escolar** | **LOL.com** | **111.65.32.1** | Success | Success |
| **Director B** | **LOL.com** | **111.65.32.1** | Success | Success |

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) |
| **Alumno B** | **Facebook.com** | **65.0.1.10** | Success |
| **Profesor A** | **Facebook.com** | **65.0.1.10** | Success |
| **Escolar** | **Facebook.com** | **65.0.1.10** | Success |
| **Director B** | **Facebook.com** | **65.0.1.10** | Success |

1. Diseña una lista de control de **acceso extendida** (115) que **impida** que las computadoras de la subred de **Directores y Servidores** tengan acceso externo a los servicios de **WEB** del servidor **Facebook.com**. El resto de las direcciones IP pueden acceder sin restricción a todos los servicios de Internet incluyendo todo el tráfico que no sea **WEB** y se dirija al servidor de **Facebook.com**

router(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

**Router B**

**access-list 115 deny tcp 132.254.89.192 0.0.0.31 host 65.0.1.10 eq 80**

**access-list 115 deny tcp 132.254.89.128 0.0.0.63 host 65.0.1.10 eq 80**

**access-list 115 permit ip any any**

**int s0/0/0**

**ip access-group 115 out**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Visitante01** | **Facebook.com** | **65.0.1.10** | Success | Success |
| **Profesor B** | **Facebook.com** | **65.0.1.10** | Success | Success |
| **Finanzas** | **Facebook.com** | **65.0.1.10** | Fail | Success |
| **Director A** | **Facebook.com** | **65.0.1.10** | Fail | Success |

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) |
| **Visitante01** | **LOL.com** | **111.65.32.1** | Success |
| **Profesor B** | **LOL.com** | **111.65.32.1** | Success |
| **Finanzas** | **LOL.com** | **111.65.32.1** | Success |
| **Director A** | **LOL.com** | **111.65.32.1** | Success |

1. Diseña una lista de control de **acceso extendida** (120) que únicamente **permita el acceso** al servidor de **Finanzas** desde cualquier IP asociada con la subred de los **Directores** pero que **impida el acceso** a este servidor desde otras direcciones IP. En esta ocasión el servidor de **Finanzas** al no permitir ningún tipo de tráfico desde direcciones diferentes de **Directores** dará la impresión de que no existe.

router(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

**Router A**

**access-list 120 permit ip 132.254.89.192 0.0.0.31 host 132.254.89.129**

**access-list 120 deny ip any host 132.254.89.129**

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

**int g0/1**

**ip access-group 120 out**

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping**  (Fail / Success) |
| **Alumno A** | **Finanzas** | **132.254.89.129** | Fail |
| **Director A** | **Finanzas** | **132.254.89.129** | Success |
| **Profesor A** | **Finanzas** | **132.254.89.129** | Fail |
| **LOL.com** | **Finanzas** | **132.254.89.129** | Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping**  (Fail / Success) |
| **Alumno A** | **Escolar** | **132.254.89.131** | Success |
| **Director A** | **Escolar** | **132.254.89.131** | Success |
| **Profesor A** | **Murillo** | **132.254.89.130** | Success |
| **LOL.com** | **Murillo** | **132.254.89.130** | Success |

3. Diseña una lista de control de acceso extendida (115) que impida que las

computadoras de la subred de Alumnos, Profesores y Servidores tengan acceso

externo a los servicios de WEB del servidor LOL.com.

El resto de las direcciones IP pueden acceder sin restricción a todos

los servicios de Internet incluyendo todo el tráfico que no sea WEB y

se dirija al servidor de LOL.com

**Router B**

**access-list 115 deny tcp 132.254.89.0 0.0.0.127 host 111.65.32.1 eq 80**

**access-list 115 deny tcp 132.254.89.232 0.0.0.7 host 111.65.32.1 eq 80**

**access-list 115 deny tcp 132.254.89.128 0.0.0.63 host 111.65.32.1 eq 80**

**access-list 115 permit ip any any**

**int s0/0/0**

**ip access-group 115 out**

4. Diseña una lista de control de acceso extendida que únicamente permita el

acceso al servidor Escolar desde cualquier IP asociada con la subred de los

Alumnos y de los Directores pero que impida el acceso a este servidor desde

otras direcciones IP. En está ocasión el servidor de Escolar al no permitir

ningún tipo de tráfico desde direcciones diferentes de Alumnos y Directivos

dará la impresión de que no existe.

**Router A**

**access-list 120 permit ip 132.254.89.0 0.0.0.127 host 132.254.89.131**

**access-list 120 permit ip 132.254.89.192 0.0.0.31 host 132.254.89.131**

**access-list 120 deny ip any host 132.254.89.131**

**access-list 120 permit ip any any // access-list 120 permit ip any 132.254.89.128 0.0.0.63**

**int g0/1**

**ip access-group 120 out**

5. Diseña una lista de control de acceso extendida (120) que únicamente permita el

acceso vía FTP al servidor de Finanzas desde cualquier IP asociada con la subred

de los profesores y de los Directores. El resto del tráfico pasa libremente (WEB, SMTP, icmp, etc.).

**access-list 130 permit tcp 132.254.89.232 0.0.0.7 host 132.254.89.129 eq 20**

**access-list 130 permit tcp 132.254.89.232 0.0.0.7 host 132.254.89.129 eq 21**

**access-list 130 permit tcp 132.254.89.192 0.0.0.31 host 132.254.89.129 eq 20**

**access-list 130 permit tcp 132.254.89.192 0.0.0.31 host 132.254.89.129 eq 21**

**access-list 130 deny tcp any host 132.254.89.129 eq 20**

**access-list 130 deny tcp any host 132.254.89.129 eq 21**

**access-list 130 permit ip any any**

**Router A**

**int g0/1**

**ip access-group 130 out**