

**Nombre de la Materia:** Interconexión de redes**Nombre:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Nombre del Profesor:** Lizethe Pérez Fuertes **Matrícula:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Reto 4. “Listas de control de acceso”**

*“Apegándome al Código de Ética de los Estudiantes del Tecnológico de Monterrey, me comprometo a que mi actuación en este examen esté regida por la honestidad académica”*

**Evidencias:**

1. El archivo de **Packet Tracer** con la solución implementada.
2. El documento con la información solicitada.
3. Las impresiones de pantalla de cada prueba de conectividad realizada.

En la realización de este reto, puedes utilizar la configuración del archivo **Reto4.pkt** para instalar las ACLs y comprobar su funcionamiento correcto.

En la realización de esta actividad debes considerar como independiente cada una de las ACLs. Para probar con éxito las ACLs en Packet Tracer se te recomienda desactivar las ACLs previas en cada inciso.

Utiliza la información de la siguiente gráfica y diseña cada una de las listas de control de acceso solicitadas.

Diagrama

Descripción generada automáticamente

1. Diseña una lista de control de **acceso estándar** 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)#

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Tablet Visitante01** | **Finanzas** | **132.254.89.129** | Fail | Fail |
| **Tablet Visitante01** | **Server Directivos** | **132.254.89.221** | Success | Success |
| **Tablet Visitante01** | **Server Profesores** | **132.254.89.238** | Success | Success |
| **Tablet Visitante01** | **Facebook.com** | **65.0.1.10** | Success | Success |

1. Diseña una lista de control de **acceso estándar** 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)#

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

1. Diseña una lista de control de **acceso extendida** 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(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Alumno A** | **LOL.com** | **111.65.32.1** | Fail | Success |
| **Server Profesores** | **LOL.com** | **111.65.32.1** | Fail | Success |
| **Escolar** | **LOL.com** | **111.65.32.1** | Fail | Success |
| **Server Directivos** | **LOL.com** | **111.65.32.1** | Success | Success |

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) |
| **Alumno A** | **Facebook.com** | **65.0.1.10** | Success |
| **Server Profesores** | **Facebook.com** | **65.0.1.10** | Success |
| **Escolar** | **Facebook.com** | **65.0.1.10** | Success |
| **Server Directivos** | **Facebook.com** | **65.0.1.10** | Success |

1. 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(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Alumno B** | **Escolar** | **132.254.89.131** | Success | Success |
| **Server Directivos** | **Escolar** | **132.254.89.131** | Success | Success |
| **Server Profesores** | **Escolar** | **132.254.89.131** | Fail | Fail |
| **Facebook.com** | **Escolar** | **132.254.89.131** | Fail | Fail |

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Web Browser**  (Fail / Success) |
| **Alumno B** | **Finanzas** | **132.254.89.129** | Success |
| **Server Directivos** | **Finanzas** | **132.254.89.129** | Success |
| **Server Profesores** | **Murillo** | **132.254.89.130** | Success |
| **Facebook.com** | **Murillo** | **132.254.89.130** | Success |

1. Diseña una lista de control de acceso extendida 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.).

**NOTAS:**

* El username y el password del servidor de Finanzas para acceso por ftp es **cisco**
* Para salir de ftp hay que usar el comando **quit**.

router(config)#

router(config)#

router(config)#

router(config)#

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

router(config)# interface

router(config-if)#

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **FTP**  (Fail / Success) | **Web Browser**  (Fail / Success) | **Ping**  (Fail / Success) |
| **Alumno A** | **Finanzas** | **132.254.89.129** | Fail | Success | Success |
| **Server Directivos** | **Finanzas** | **132.254.89.129** | Success | Success | Success |
| **Server Profesores** | **Finanzas** | **132.254.89.129** | Success | Success | Success |
| **Facebook.com** | **Finanzas** | **132.254.89.129** | Fail | Success | Success |