

**Ejercicio 11. Listas de control de acceso (ACLs)**

#### En la realización de estos ejercicios debes considerar como independiente cada una de las ACLs. Para probar las ACLs en PT se te recomienda desactivar las ACLs previas a cada inciso.

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



Este esquema tenemos varias subredes, la subred de alumnos con 128-2 direcciones disponibles.

La subred de profesores con 8-2 direcciones disponibles.

Tres servidores simulando Intenet (cnn solo ping) Facebook y LOL si se pueden acceder por TCP

**Pruebas de conectividad con servidores son exitosos. Hay conectividad desde directores hacia el Internet**

Pc (Director A) directores hacia servidor 65.0.1.10 Facebook.com (WEB)

Pc (Director A) directores hacia servidor 111.65.32.1 LOL Server (WEB)

Pc (Director A)directores hacia 65.10.56.1 CNN por ping

**Para checar tráfico de subred de Alumnos a Directores**

Tablet01 (Visitante 01) acceder a través del protocolo Web a los directivos (**Server Directivos) 132.254.89.221**.

**Para checar tráfico de Alumnos a Servidores**

Tablet01 (Visitante 01) acceder a través del protocolo Web al servidor **Murillo 132.254.89.130** y **Escolar 132.254.89.131 (Punto Azul)**

**Para checar tráfico de Alumnos a Profesores**

Tablet01 (Visitante 01)acceder a través del protocolo Web al servidor **Profesores 132.254.89.232**

La conectividad existe.

El tráfico llega al router y se analiza. **Las listas de control de acceso estándar bloquean todo el tráfico web y ping.** (capa 3 ping y capa 4 aplicaciones protocolo http)

Mejores prácticas para el diseño de ACLs

1. Identificar la fuente/origen (tráfico fuente) **SUBRED ALUMNOS**
2. Identificar el tráfico no permitido. trayecto de la fuente al destino Trazar el flujo de tráfico
3. Identificar el 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. Determinar la interface donde se va a insertar la lista de acceso. Si pongo lista de acceso en la interfaz s0/0/0 las subredes de servidores y directores no recibirán tráfico de los alumnos y eso no se pide. La interface g0/0/0 es la que hay que seleccionar ya que es la que se conecta con la subred morada.

**REGLA, LA LISTA DE ACESO ESTÁNDAR SE DEBEN INSTALAR LO MAS CERCA DEL DESTINO.**

Red de estudiantes hacia Internet, servidores,

1. 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**.

**access-list número\_lista {permit|deny} IP\_Origen wildcard**

**access-list 10 (lista entre 1 y 99 acceso estándar)**

**access-list 10 deny 132.254.89.0/25 wildcard**

255.255.255.1000 0000

**255.255.255.255**

**- 255.255.255.128**

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

**0 . 0. 0. 127**

**access-list 10 deny 132.254.89.0 0.0.0.127 (negamos el tráfico de todas la redes, por eso tenemos que permitir el tráfico de las otras redes)**

**0 . 0. 0. 127**

**¡deny any IMPLICITO (negamos el tráfico el tráfico anterior y de TODAS LAS redes a la subred de directivos, por eso tenemos que permitir el tráfico de las otras redes)**

**DISEÑO DE LA ACL**

**access-list 10 deny 132.254.89.0 0.0.0.127**

**access-list 10 permit any QUE PERMITA EL RESTO DEL TRÁFICO**



**ASOCIAR ACL A LA INTERFAZ**

**Una vez diseñada la ACL se asigna a una interfaz**

**interface int\_número**

**ip access-group número list {in | out}**

int g0/0

ip access-group 10 {in | out}



**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**

¿En qué router instalarás esta lista de control de acceso? \_\_RouterA\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_ **access-list 10 deny 132.254.89.0 0.0.0.127**

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

router(config)#\_\_\_\_ **access-list 10 permit any**

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

router(config)# interface \_g0/0\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_ **ip access-group 10 out** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Primero **pruebo el acceso de Tablet visitantes 01 a un servidor de directores** (funciona)

Después **copio y pego la configuración de la lista de acceso en el router A** en config t.

Intentar acceso de **alumnos (tablet visitantes 01)**

* Al servidor de directivos 132.254.89.221 por **web (no)**
* Al servidor de directivos 132.254.89.221 por **ping (no)**
* Al servidor Murillo (Servidores) (Murillo 132.254.89.130)
* Al servidor de profesores (Profesores) (132.254.89.238)
* Al Intenet Facebook 65.0.1.10

**El tráfico llega al router y se analiza. Las listas de control de acceso estándar bloquean todo el tráfico web y ping.**

* **Capa 3 del modelo OSI (red) donde está incluido el ping**
* **Capa 4 del modelo OSI (transporte) donde están los protocolos de transporte tcp /udp donde está incluido el protocolo http (80) con la que funciona la aplicación web**

Hay que probar lista de acceso y luego la desinstalo o la hago independiente. Desasocio la lista de control de acceso, la desactivo. No elimino la lista de acceso, solamente la desasocio o la desactivo. **Checo conectividad y checo sh run y la interface yo no tiene asociada una lista de acceso.**

**no ip acces-group 10 out**



La interface g0/0 es la que da servicio a los directores

La interface g0/1 es la que da servicio a los servidores.

En la interface g0/0 es donde vamos a instalar la lista de control de acceso.

**Hay dos direcciones de tráfico en las interfaces**, el tráfico de entrada hacia el router **(in)** y el tráfico de **salida** hacia los dispositivos. **G0/0 y dirección de salida**

1. Diseña una lista de control de acceso estándar para **impedir** que las computadoras de la subred de **Profesores** tengan acceso a la subred de **Directivos**.

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

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

access-list 20 deny 132.254.89.232/29

**access-list 20 deny 132.254.89.232 0.0.0.7**

255.255.255.11111000

255.255.255.255

255.255.255.248

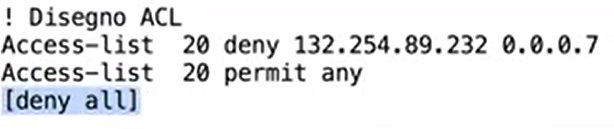
---------------------------

0.0.0.7

**¡deny any IMPLICITO POR DEFAULT**

**access-list 20 permit any (si quito este comando nadie va a poder entrar a la subred de Directivos ya que una un deny any implícito)**

**Al poner el comando permit any se elimina el deny any**



**int g0/0**

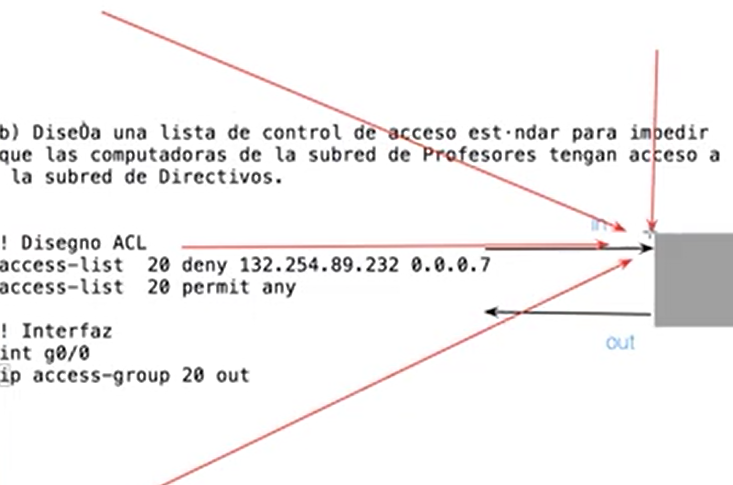
**ip access-group 20 out**

Tengo que apagar mi lista de acceso anterior, ya que solamente puedo tener una lista de acceso in y otra out.

**no ip access-group 10 out (tengo que desactivar mi lista de acceso anterior de la interface, no la quito solo la desactivo) 10 o 20 es como darle un nombre a la lista de acceso. Las interfaces ya no tendrían asociadas listas de control de acceso.**

**Si tengo dos listas de acceso in, va a tomar la última lista instalada.** Cuantas listas soporta: una interface de entrada y una lista soporta una interface de salida. **Solamente podemos tener**

**una lista de entrada y una de salida por interface. Cuantas listas puede soportar una interface: una en el canal de entrada y otra en el canal de salida.**

****



1. 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**.

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

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

access-list 20 deny 132.254.89.232/29

**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**

255.255.255.11111000

255.255.255.255

255.255.255.248

---------------------------

0.0.0.7

Pregunta si invertimos que haría

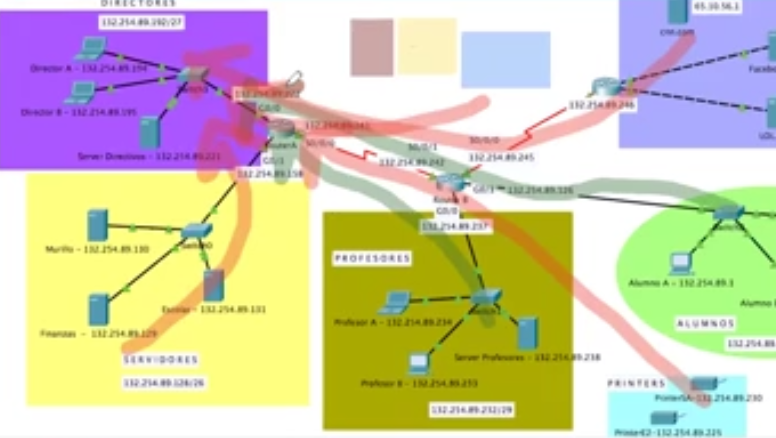
**access-list 20 permit 132.254.89.232 0.0.0.7**

**access-list 20 permit 132.254.89.0 0.0.0.127**

**access-list 20 deny any (niega el acceso a todas la demás subredes, incluyendo nuevas)**

**int g0/0**

**ip access-group 20 out**



Tengo que apagar mi lista de acceso anterior, ya que solamente puedo tener una lista de acceso in y otra out. Si tengo dos listas de acceso in, va a tomar la última lista instalada. Cuantas listas soporta una interface de entrada y una lista soporta una interface de salida. Solamente podemos tener una lista de entrada y una de salida.

**No ip access-group 20 out no quito la lista de control de acceso, solo la desactvo de la interface. Hay listas que no se están ocupando.**

1. Diseña una lista de control de acceso estándar para que el **visitante 01** no pueda acceder a la sección de **servidores**

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

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

router(config)# interface \_\_\_\_\_\_\_\_\_

router(config-if)#\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**access-list 30 deny 132.254.89.120 0.0.0.0 (match exacto con la dirección ip)**

**hAY UN DENY ANY POR DEFAULT, POR ESO TENGO QUE PONER PERMIT ANY. Y ESTO BLOQUEARÍA TODO EL TRÁFICO.**

**access-list 30 permit any**

**int g0/1**

**ip access-group 30 out**

**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 (ACCESS GROUP ES UN GRUPO DE INSTRUCCIONES)**

**access-list 30 deny host 132.254.89.120 (es lo mismo que lo anterior, niega al host el acceso y los comandos son equivalentes) SOLAMENTE EN NOMENCLATURA DE CISCO**

**access-list 30 permit any**

**int g0/1**

**ip access-group 30 out**

access-list 10 deny 132.254.89.0 0.0.0.127

access-list 10 permit any

access-list 20 deny 132.254.89.232 0.0.0.7

access-list 20 permit any

access-list 30 deny host 132.254.89.120

access-list 30 permit any

En el router hay 3 listas de acceso, la última sería la que tendría efecto alguno.

SI QUISIERAMOS BLOQUEAR TAMBIÉN EL ACCESO A DIRECTORES PUEDO APLICAR LA LISTA DE ACCESO A DIRECTORES G0/0

PROBAR DE MANERA INDEPENDIENTE CADA LISTA.

LA EJECUCIÓN DE LOS COMANDOS VA DE ARRIBA HACIA ABAJO.

CUMPLE PRIMERA REGLA, SEGUNDA REGLA Y SINO TENGO UN DENY ANY CONFIGURADO, ESTÁ IMPLÍCITO AL FINAL.

**AL FINAL HAY QUE PERMITIR TODO EL TRÁFICO O NEGAR TODO EL TRÁFICO DE FORMA EXPLICITA.**