DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.5**	**Práctica 3**	Configurar IP ACL para mitigar ataques				
Unidad:	2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	23/04/2021
Compet. Genéricas		4.1, 4.5, 5.2, 5.5		Compet.		CP1-1	

1. Objetivo(s) de la actividad

- Aplicar los tipos de listas de control de acceso.

2. Introducción

Los controles de acceso son soluciones de hardware y software que se utilizan para administrar el acceso a recursos y a los sistemas, las listas de control de acceso (ACL) definen el tipo de tráfico permitido en una red informática.

3. Objetivos

- Verificar la conectividad entre los dispositivos antes de la configuración del firewall.
- Utilizar las ACL para garantizar que el acceso remoto al router está disponible sólo desde la estación de administración de PC-C.
- Configurar ACL en Router 1 y Router 3 para mitigar los ataques.
- Verificar las funciones ACL en esta página.

4. Instrucciones (Descripción) de la actividad

1. Usar el archivo de ejemplo de prácticas para realizar el reporte esta actividad.
2. Tomar impresiones de pantalla completa de la actividad, (recuerda ir haciendo las impresiones conforme vas realizando la práctica en el simulador) , con tu nombre en la impresión.
3. Subir el reporte terminado de WORD y el archivo de PACKET TRACERT, dar clic para marcar como entregada la actividad.

4. Resumen

Listas de acceso estándar
Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

Listas de acceso extendidas
Las listas de acceso extendidas controlan el tráfico por la comparación de las direcciones de origen y de destino de los paquetes IP a las direcciones configuradas en la ACL.

Listas de acceso reflexivas
Permiten que se filtren los paquetes IP según la información de sesión de capa superior. Generalmente, se utilizan para permitir el tráfico saliente y para limitar el tráfico entrante en respuesta a las sesiones que se originan dentro del router. Solo se pueden definir con ACL con nombre IP extendidas.

Listas de acceso dinámicas
La configuración de cerradura y llave comienza con la aplicación de una ACL extendida para bloquear el tráfico a través del router. Los usuarios que desean atravesar el router son bloqueados por la ACL extendida hasta que realicen una conexión Telnet al router y sean autenticados. Luego, la conexión Telnet se pierde y se agrega una ACL dinámica de una única entrada a la ACL extendida existente. Esto permite el tráfico por un período de tiempo determinado; son posibles los tiempos de espera inactivo y absoluto

Listas de acceso basadas en tiempo
Se crea un intervalo de tiempo que define las horas específicas del día y de la semana para implementar las ACL basadas en El intervalo de tiempo se identifica con un nombre y luego se remite a él a través de una función. Por lo tanto, las restricciones de tiempo se imponen en la misma función. El intervalo de tiempo depende del reloj del sistema del router. Se puede utilizar el reloj del router, pero la función funciona mejor con la sincronización de Network TimeProtocol (NTP).

Referencias
Configuración de Listas de Acceso IP. Recuperado el 22/04/2021 de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf

5. Material y Equipo

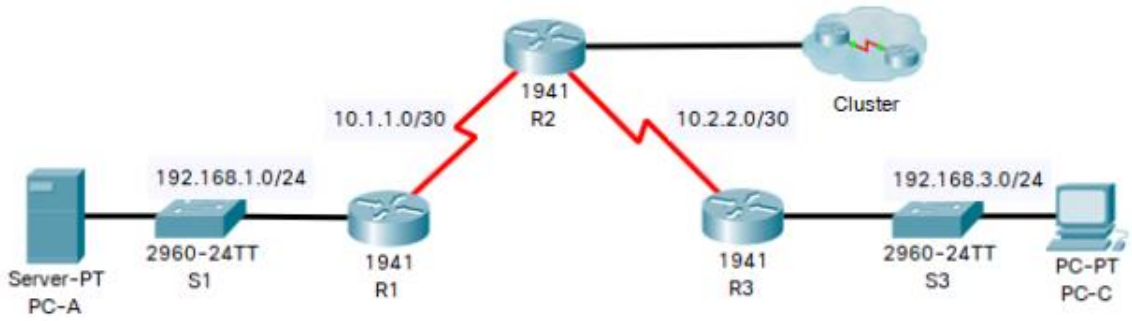
- Computadora
- Acceso a Packet Tracer

6. Desarrollo

• Tabla de Comandos

Tabla de Comandos
access-list access-list-number {permit|deny} {host|source source-wildcard|any}
ip access-group nº in|out
access-list nº permit|deny origen [wild-mask]
access-list nº permit|deny protocolo origen [wild-mask][operación] [puerto origen] destino [wild-mask][operación] [puerto destino][established]
ip access-group nº in|out
ip access-list[standard|extended][nombre]
[permit|deny][condiciones de prueba]
no[permit|deny][condiciones de prueba]
Interfaz asociación de la ACL
ip access-group[nombre][in|out]
ip access-list extended name permit protocol any any reflect name [timeoutseconds]
ip access-group {number|name} {in|out
ip access-list extended name evaluate name
username user-name password password interface <interface> ip access-group {number|name}{in|out}
access-list access-list-number dynamic name {permit|deny} [protocol] {source source-wildcard|any} {destination destination-wildcard|any} [precedence precedence][tostos][established] [log|log-input] [operator destination-port|destination port]
"Rango de tiempo": time-range time-range-name "Tiempo periódico": periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm "Tiempo absoluto": absolute [start time date] [end time date] "Usado en la ACL": ip access-list name|number <extended_definition>time-rangename_of_time-range
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} protocolsource source-wildcard destination destination-wildcard [precedence precedence] [tos tos][log|log-input] [time-range time-range-name]
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} udp sourcesource-wildcard [operator [port]] destination destination-wildcard [operator [port]] [precedenceprecedence] [tos tos] [log|log-input] [time-range time-range-name]
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} tcp sourcesource-wildcard [operator [port]] destination destination-wildcard [operator [port]][established] [precedence precedence] [tos tos] [log|log-input] [time-range time-range-name]
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny|permit} protocolsource source-wildcard destination destination-wildcard [precedence precedence] [tos tos][log|log-input] [time-range time-range-name]

• Topología



• Tabla de configuración básicas

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252		N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252		
	G0/0	209.165.200.225	255.255.255.224		
	Lo0	192.168.2.1	255.255.255.0		
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252		N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

• Procedimiento

Part 1: Verify Basic Network Connectivity

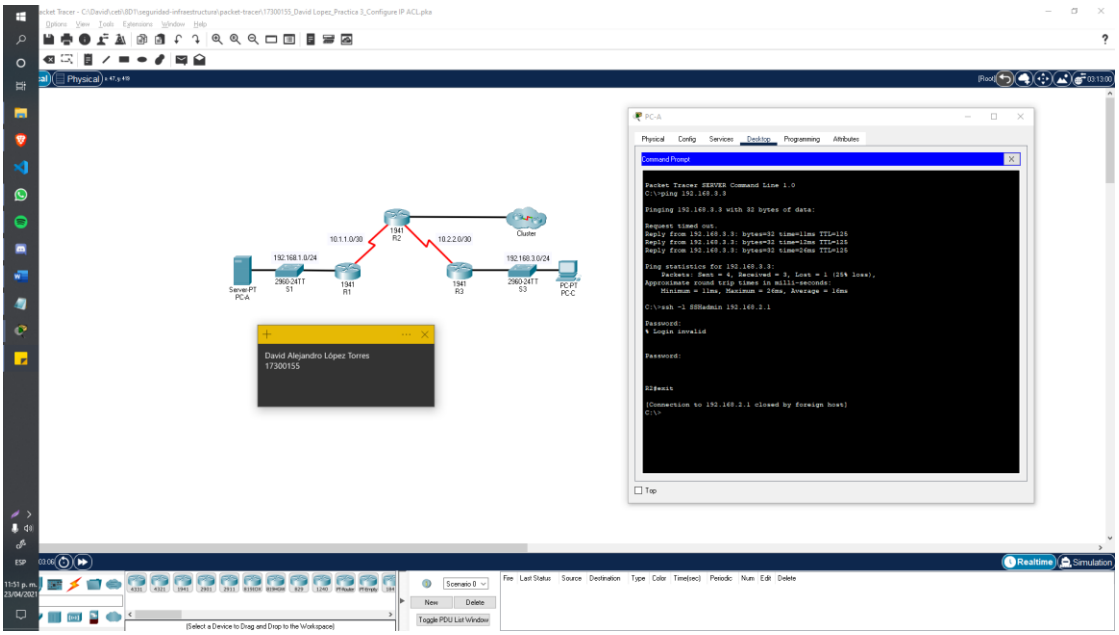
Verify network connectivity prior to configuring the IP ACLs.

Step 1: From PC-A, verify connectivity to PC-C and R2.

a. From the command prompt, ping **PC-C** (192.168.3.3).

b. From the command prompt, establish an SSH session to **R2** Lo0 interface (192.168.2.1) using username
SSHadmin and password **ciscosshpa55**. When finished, exit the SSH session.

SERVER> **ssh -l SSHadmin 192.168.2.1**



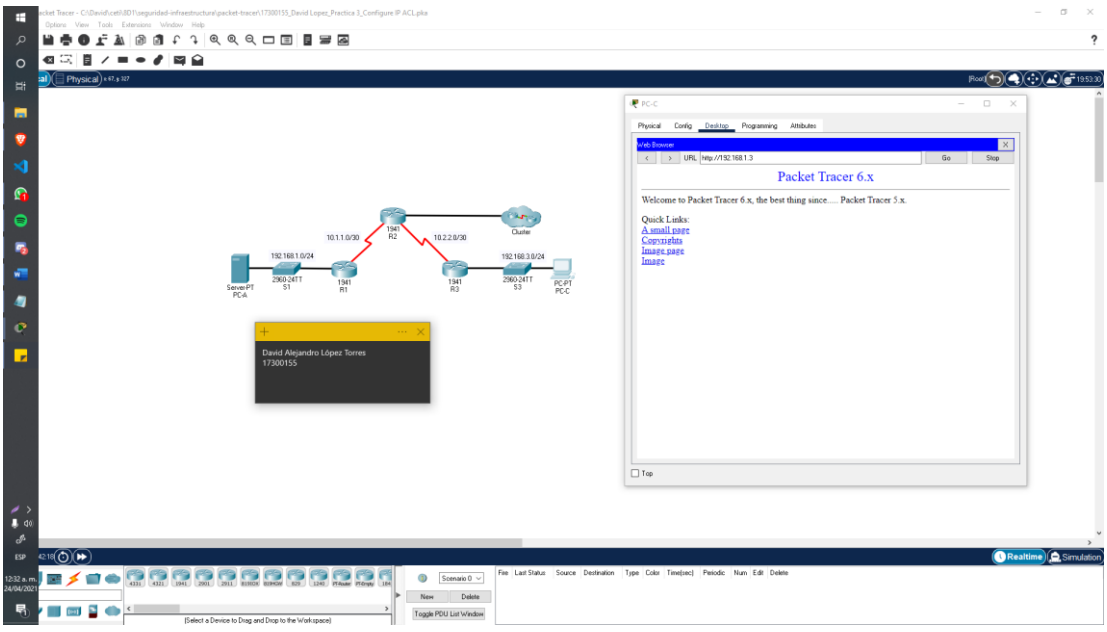
Step 2: From PC-C, verify connectivity to PC-A and R2.

a. From the command prompt, ping **PC-A** (192.168.1.3).

b. From the command prompt, establish an SSH session to **R2** Lo0 interface (192.168.2.1) using username
SSHadmin and password **ciscosshpa55**. Close the SSH session when finished.

c. Establish another SSH session to R2 G0/0 interface (209.165.200.225) using username **SSHadmin** andpassword **ciscosshpa55**. When finished, exit the SSH session.

d. Open a web browser to the **PC-A** server (192.168.1.3) to display the web page. Close the browser whendone.



Part 2: Secure Access to Routers

Step 1: Configure ACL 10 to block all remote access to the routers except from PC-C.

a. Use the **access-list** command to create a numbered IP ACL on **R1**, **R2**, and **R3**.

Step 2: Apply ACL 10 to ingress traffic on the VTY lines.

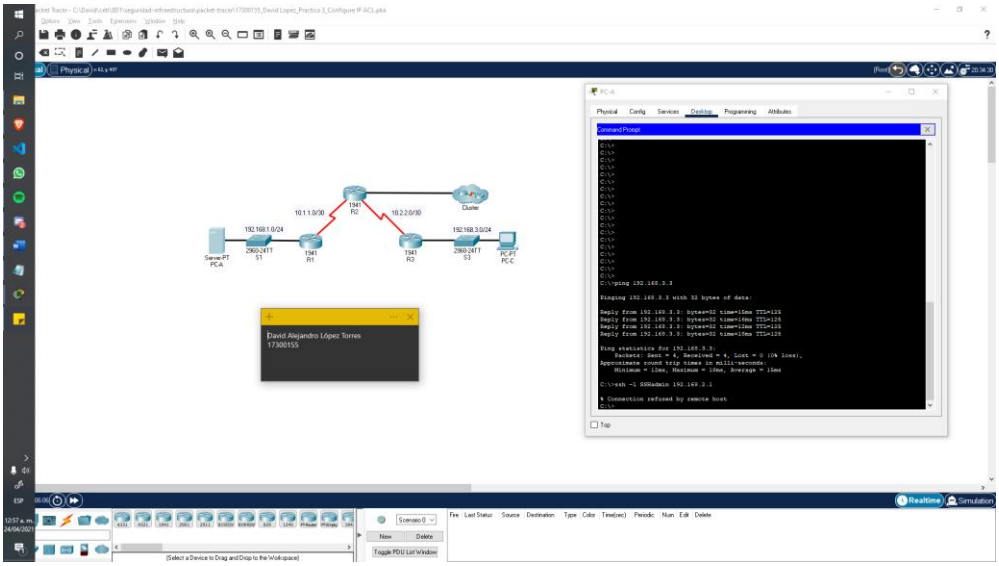
Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

Step 3: Verify exclusive access from management station PC-C.

a. Establish an SSH session to 192.168.2.1 from **PC-C** (should be successful).

b. Establish an SSH session to 209.165.200.225 from **PC-C** (should be successful).

c. Establish an SSH session to 192.168.2.1 from **PC-A** (should fail).



Part 3: Create a Numbered IP ACL 120 on R1

Create an IP ACL numbered 120 with the following rules:

- Permit any outside host to access DNS, SMTP, and FTP services on server **PC-A.**
- Deny any outside host access to HTTPS services on **PC-A.**
- Permit **PC-C** to access **R1** via SSH.

Note: Check Results will not show a correct configuration for ACL 120 until you modify it in Part 4.

Step 1: Verify that PC-C can access the PC-A via HTTPS using the web browser.

Be sure to disable HTTP and enable HTTPS on server **PC-A**.

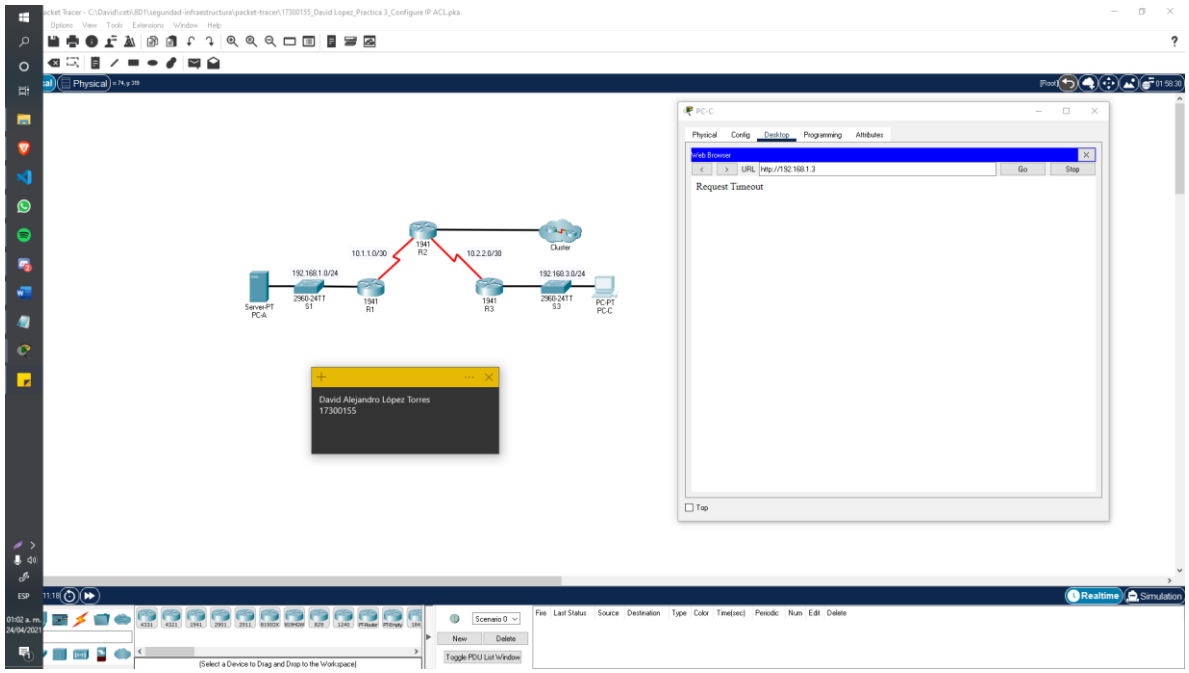
Step 2: Configure ACL 120 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

Step 3: Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

Step 4: Verify that PC-C cannot access PC-A via HTTPS using the web browser.



Part 4: Modify an Existing ACL on R1

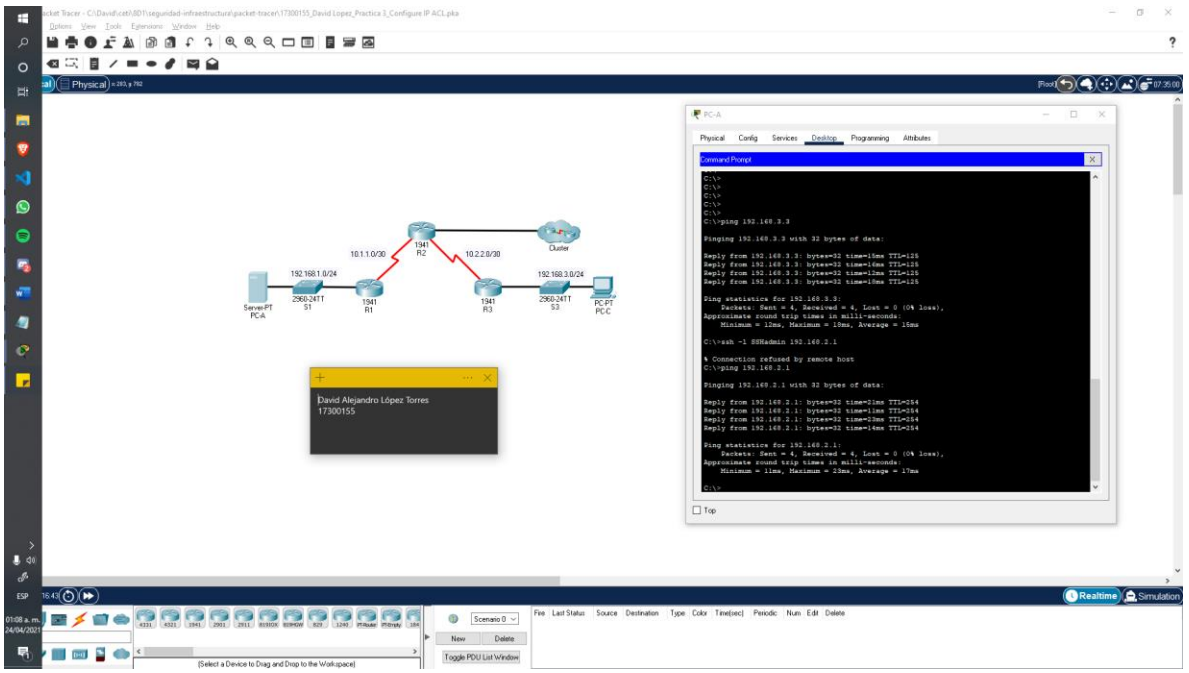
Permit ICMP echo replies and destination unreachable messages from the outside network (relative to **R1**).Deny all other incoming ICMP packets.

Step 1: Verify that PC-A cannot successfully ping the loopback interface on R2.

Step 2: Make any necessary changes to ACL 120 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

Step 3: Verify that PC-A can successfully ping the loopback interface on R2.



Part 5: Create a Numbered IP ACL 110 on R3

Deny all outbound packets with source address outside the range of internal IP addresses on **R3**.

Step 1: Configure ACL 110 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

Step 2: Apply the ACL to interface G0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface G0/1.

Part 6: Create a Numbered IP ACL 100 on R3

On **R3**, block all packets containing the source IP address from the following pool of addresses: any RFC1918 private addresses, 127.0.0.0/8, and any IP multicast address. Since **PC-C** is being used for remote administration, permit SSH traffic from the 10.0.0.0/8 network to return to the host **PC-C**.

Step 1: Configure ACL 100 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address. In this activity, your internal address space is part of the private address space specified in RFC 1918.

Use the **access-list** command to create a numbered IP ACL.

Step 2: Apply the ACL to interface Serial 0/0/1.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/1.

Step 3: Confirm that the specified traffic entering interface Serial 0/0/1 is handled correctly.

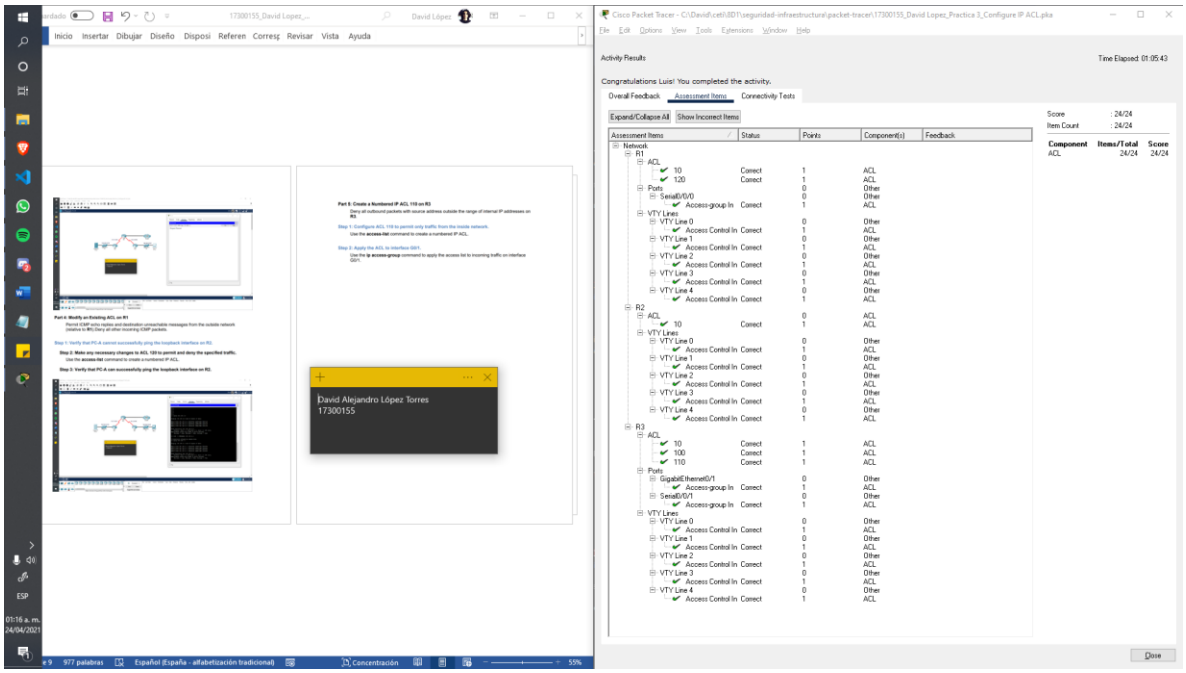
a. From the PC-C command prompt, ping the PC-A server. The ICMP echo replies are blocked by the ACL because they are sourced from the 192.168.0.0/16 address space.

b. Establish an SSH session to 192.168.2.1 from **PC-C**. (should fail)

c. Establish an SSH session to 209.165.200.225. (should be successful).

Step 4: Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.



7. Observaciones

Es recomendable contar con un directorio de puertos conectados y su relación con los dispositivos finales, de maneta que la administración por listas de control sea más intuitiva, dinámica y más eficiente; en particular, cuando se tiene una gran cantidad de dispositivos involucrados en la lista de acceso.

8. Conclusiones

La implementación de listas de accesos requiere de una particular atención en los pequeños detalles, pues un pequeño error de gestión puede representar un gran obstáculo para el desarrollo de las actividades propias de la empresa donde se implementa. Además, tener un orden estricto en la designación de permisos facilita la gestión y mantenimiento de la red y en particular del apartado correspondiente a las listas de acceso. A pesar de estar consideraciones, las ACLs constituyen en gran medida una herramienta base para garantizar la eficiencia de la red y el control del tráfico de la red. Pudimos ver como la implementación es realmente simple si se siguen los consejos que se nos han dado acerca de la gestión de las listas de accesos.

9. Referencias

Configuración de Listas de Acceso IP. Recuperado el 22/04/2021 de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf