
	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	255/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Práctica complementaria y obligatoria 6

Firewall básico

Capa 7 del Modelo OSI

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	256/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

1.- Objetivos de Aprendizaje

- El alumno analizará, investigará e implementará mecanismos adecuados de seguridad en los puertos lógicos de entrada de un servidor de red.
- El alumno aprenderá las reglas básicas para implementar las distintas opciones de entrada de paquetes a través de un Firewall de seguridad en los puertos lógicos del servidor en red.


2.- Conceptos teóricos

Un servidor de red es un ordenador que ofrece el acceso a los recursos o servicios compartidos entre las estaciones de trabajo u otros servidores conectados en una red de datos. Los recursos o servicios compartidos pueden incluir acceso a hardware, como discos duros, impresoras, software, servicios de email o acceso a internet.

Un firewall, también conocido como cortafuegos, es un elemento informático (es decir, es un dispositivo de hardware o un software) que trata de bloquear el acceso, a una red privada conectada a Internet, a usuarios no autorizados. Por tanto, el cortafuegos se centra en examinar cada uno de los mensajes que entran y salen de la red para obstruir la llegada de aquellos que no cumplen con unos criterios de seguridad, al tiempo que da vía libre a las comunicaciones que sí están reglamentadas.

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

- Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.
- Registrar todos los intentos de entrada y salida de una red. Los intentos de entrada y salida se almacenan en logs.
- Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones. Así por lo tanto con el filtro de direcciones se puede bloquear o aceptar el acceso a un equipo con cierta dirección IP a través del puerto 22. Recordar solo que el puerto 22 acostumbra a ser el puerto de un servidor SSH.
- Filtrar determinados tipos de tráfico en la red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado. Distintos tipos de protocolos que se pueden utilizar son http, https, Telnet, TCP, UDP, SSH, FTP, etcétera.
- Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.
- Controlar las aplicaciones que pueden acceder a Internet. Así por lo tanto se puede restringir el acceso a ciertas aplicaciones, como por ejemplo dropbox, a un determinado grupo de usuarios.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	257/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

3.- Equipo y material necesario

Equipo del Laboratorio:

- Software de simulación de redes Cisco Packet Tracer.

4.- Desarrollo


En esta práctica se realizarán y explicarán las reglas para restringir el acceso a la entrada de los puertos lógicos de un servidor en red. Es importante mencionar que existen distintos tipos de servidores de red con una gran variedad de sistemas operativos, pero en general las reglas de un firewall aplican a todos ellos.

Modo de trabajar

La práctica se desarrollará en parejas.

4.1 Construcción de la topología

- 4.1.1** Ejecute el software Cisco Packet Tracer e inmediatamente aparecerá la interfaz gráfica (Ver Figura No. 1)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	258/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

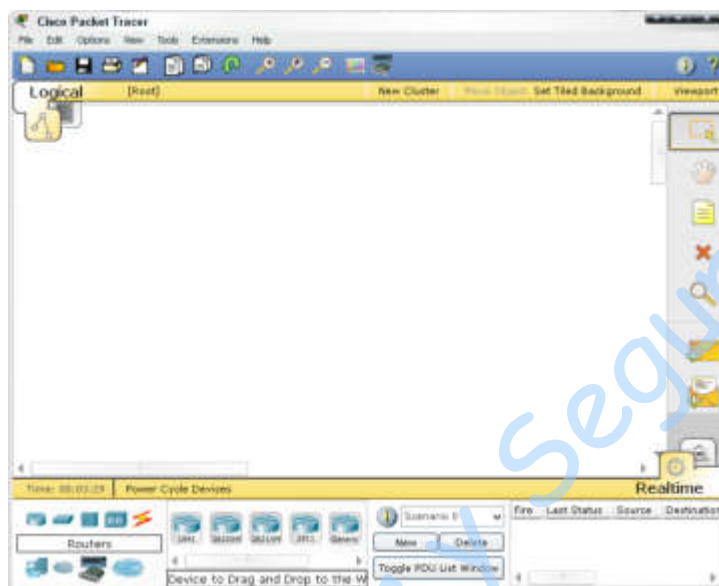



Figura No. 1. Interfaz gráfica de PT

- 4.1.2** Cuando Packet Tracer se inicia, muestra por default una vista lógica de red; el área de trabajo lógica es el espacio central en blanco donde se pueden colocar y conectar los dispositivos.
- 4.1.3** En la esquina inferior izquierda de la interfaz se encuentran las secciones para elegir y colocar dispositivos en el área lógica de trabajo (Ver figura No. 2.)



Figura No. 2. Secciones de dispositivos

- 4.1.4** La sección 1 contiene símbolos que representan Grupos de Dispositivos. Cuando se coloca el puntero del mouse sobre alguno de los símbolos, en el cuadro de texto del centro aparece el nombre de este grupo.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	259/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.1.5 La sección 2 muestra los Dispositivos Específicos al grupo seleccionado en la sección 1. Si se da clic sobre algún grupo de la sección 1, los dispositivos de la sección 2 se actualizarán.

4.1.6 Con ayuda de su profesor realice una topología básica de red agregando al área de trabajo de Packet Tracer 2 switches de 24 puertos (modelo 2950-24), 1 router genérico (router-PT), un par de servidores (server-PT) y 3 dispositivos finales (2 PC y una laptop), como se muestra en la figura No. 3.

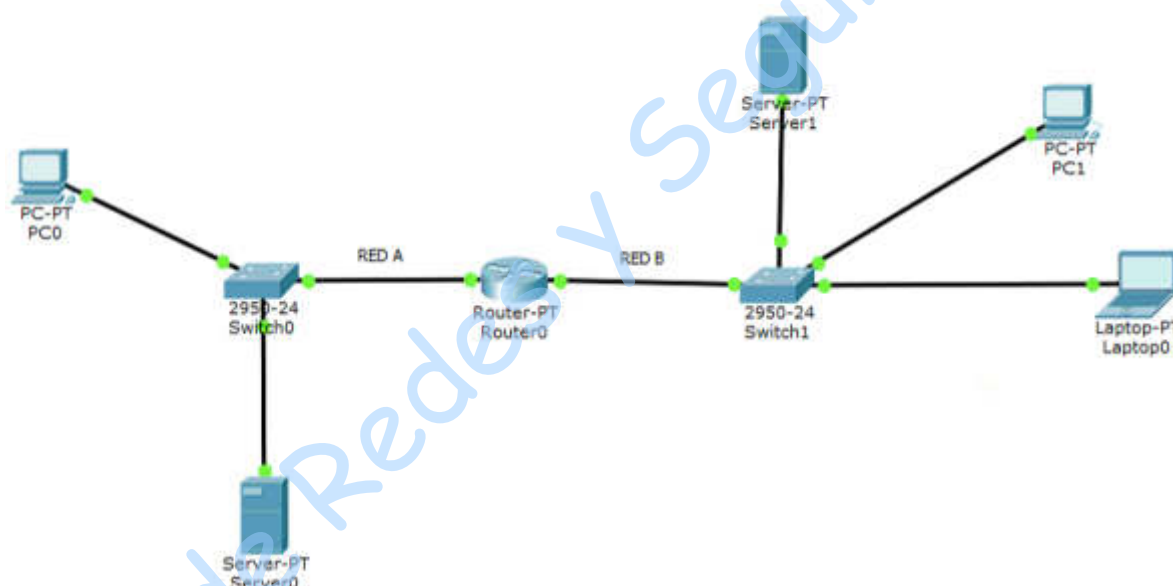



Figura No. 3. Topología básica

4.1.7 Conecte la interfaz FastEthernet 0/0 del Router0 con la interfaz FastEthernet 0/1 del Switch0 y la interfaz FastEthernet 1/0 del Router0 con la interfaz FastEthernet 0/1 del Switch1.

4.1.8 Conecte la interfaz FastEthernet 0/2 del Switch0 con la interfaz FastEthernet 0 del Server0 y la interfaz FastEthernet 0/3 del Switch0 con la interfaz FastEthernet 0 de la PC0.

4.1.9 Conecte la interfaz FastEthernet 0/2 del Switch1 con la interfaz FastEthernet 0 del Server1, la interfaz FastEthernet 0/3 del Switch1 con la interfaz FastEthernet 0 de la PC1 y la interfaz FastEthernet 0/4 del Switch1 con la interfaz FastEthernet 0 de la Laptop0.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	260/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.2 Configuración de las interfaces del router

4.2.1 Seleccione el Router0 y dé clic sobre la pestaña CLI.

4.2.2 Para configurar la interfaz FastEthernet 0/0 deben teclearse los siguientes comandos:

```
Router>enable
Router#configure t
Router(config)#int FastEthernet 0/0
Router(config-if)#ip address DIR_IP 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

NOTA: DIR_IP se sustituye por la última dirección IP utilizable de clase C para la red A


4.2.3 Para configurar la interfaz FastEthernet 1/0 deben teclearse los siguientes comandos:

```
Router>enable
Router#configure t
Router(config)#int FastEthernet 1/0
Router(config-if)#ip address DIR_IP 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

NOTA: DIR_IP se sustituye por la primera dirección IP utilizable de la clase A para la red B

4.2.4 Explique qué sucede en la ventana CLI cuando se ejecuta el comando show running-config.

Se muestran las direcciones ip asignadas a cada puerto para que haya comunicación entre los dispositivos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	261/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3 Configuración de los dispositivos

- 4.3.1** Dé clic sobre la PC conectada al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.3.2** Seleccione la pestaña **Desktop** y seleccione **IP Configuration**.
- 4.3.3** Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. Ingrese los datos que se muestran en la Tabla No.1.

Tabla No.1. Datos para la configuración de los dispositivos conectados al Switch0

IP Address	Cualquier dirección IP utilizable de la red A excepto la última Anote la dirección IP que empleó <u>192.168.1.2</u>
Subnet Mask	255.255.255.0
Default Gateway	Dirección IP asignada a la interfaz Fa0/0 del Router0

- 4.3.4** Dé clic sobre el Server0 conectado al Switch0, en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.3.5** Seleccione la pestaña Desktop y seleccione IP Configuration.
- 4.3.6** Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. utilice los datos de Subnet Mask y Default Gateway que se muestran en la Tabla No.1. y anote la dirección IP (distinta a la que utilizó en la PC0) que empleó 192.168.1.254.
- 4.3.7** Dé clic sobre la PC conectada al Switch1 en el área de trabajo, con lo que aparecerá la ventana de configuración.
- 4.3.8** Seleccione la pestaña Desktop y seleccione IP Configuration.
- 4.3.9** Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. Ingrese los datos que se muestran en la Tabla No.2.


	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	262/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

Tabla No.2. Datos para la configuración de los dispositivos conectados al Switch1

IP Address	Cualquier dirección IP utilizable de la red B excepto la primera Anote la dirección IP que empleó <u>192.168.2.2</u>
Subnet Mask	255.0.0.0
Default Gateway	Dirección IP asignada a la interfaz Fa1/0 del Router0

4.3.10 Dé clic sobre el Server1 conectado al Switch1 en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.3.11 Seleccione la pestaña Desktop y seleccione IP Configuration.


4.3.12 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. utilice los datos de Subnet Mask y Default Gateway que se muestran en la Tabla No.2. y anote la dirección IP (distinta a la que utilizó en la PC1) que empleó 192.168.2.3.

4.3.13 Dé clic sobre la Laptop0 conectado al Switch1 en el área de trabajo, con lo que aparecerá la ventana de configuración.

4.3.14 Seleccione la pestaña Desktop y seleccione IP Configuration.

4.3.15 Se abrirá una ventana solicitando la dirección IP, máscara de red y el gateway. utilice los datos de Subnet Mask y Default Gateway que se muestran en la Tabla No.2. y anote la dirección IP (distinta a la que utilizó en la PC1 y Server1) que empleó 192.168.2.4.

4.3.16 Para validar el funcionamiento de las comunicaciones entre los dispositivos de la red A y los de la red B, se debe dar clic en cualquier dispositivo de la red A (PC0 o Server0), seleccione la pestaña Desktop y posteriormente seleccione la opción de Command Prompt como se muestra en la Figura No. 4.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	263/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

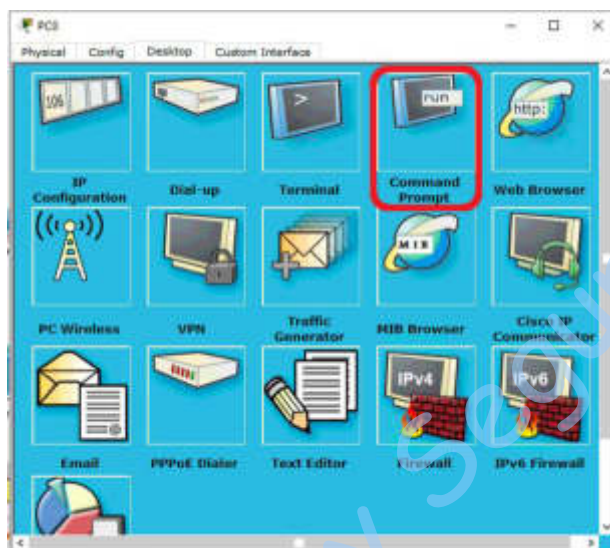


Figura No. 4. Seleccionando la Opción de Command Prompt

4.3.17 Usando el comando ping desde el dispositivo seleccionado de la red A pruebe la conexión con algún dispositivo de la red B. Anote los resultados obtenidos.

Se pudo realizar un ping de PC0 a PC1

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.2.2


Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=0ms TTL=127
Reply from 192.168.2.2: bytes=32 time=2ms TTL=127
Reply from 192.168.2.2: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>
PC>
PC>
PC>

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	264/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3.18 ¿Se logró establecer la comunicación? Explique

Efectivamente se pudo establecer una conexión con los dispositivos de la otra, gracias al router que nos permite comunicar 2 redes distintas. Aunque en mi command prompt salió la pérdida de un paquete y tardo un tiempo en hacer la conexión.

4.3.19 Seleccione nuevamente la pestaña Desktop y posteriormente seleccione la opción de Web Browser como se muestra en la Figura No. 5.

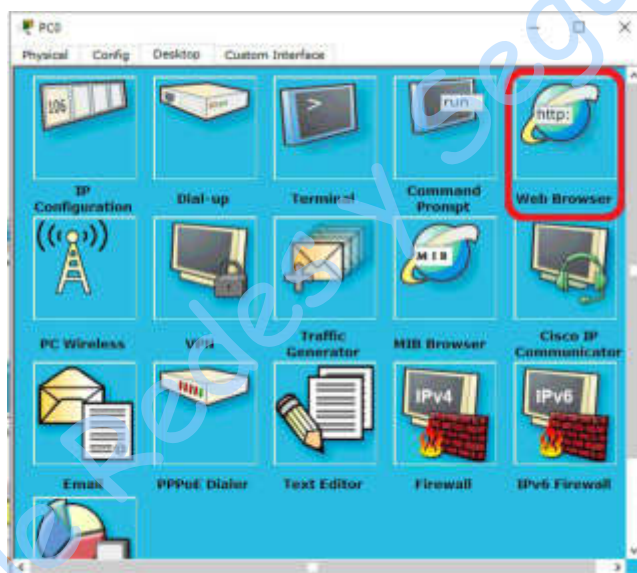



Figura No. 5. Seleccionando la Opción de Web Browser

4.3.20 Coloque en el URL del Web Browser del dispositivo seleccionado de la red A, la dirección IP del Server1 de la red B y pruebe la conexión. Anote los resultados obtenidos.

Nos aparece un mensaje de bienvenida o el index predeterminado del servidor con el que nos estamos conectando.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	265/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.3.21 ¿Se logró establecer la comunicación? Explique

Se logró igualmente hacer una conexión con el servidor como en otro tipo de servidores ya que la comunicación esta correctamente configurada nos manda a su página principal o su index predeterminado que en este caso es una bienvenida de Cisco Paquet Tracer

4.3.22 También puede probar la conectividad en el sentido inverso desde la red B hacia la red A. Indique el resultado obtenido.


De las misma manera la comunicación se logra establecer gracias al router que nos permite conectar la red A con la red B ya estando configurados los puertos y direcciones, también nos muestra el mismo mensaje de bienvenida al conectar con la PC1 de la red B con el servidor de la red A.

4.4 Configuración del Firewall a través del Router

4.4.1 Seleccione el Router0 y dé clic sobre la pestaña CLI y teclee lo siguiente:

```
Router>enable
Router#configure t
Router(config)# access-list 101 deny icmp any any host-unreachable
Router(config)# access-list 101 permit tcp any any eq www
Router(config)# interface FastEthernet1/0
Router(config-if)# ip access-group 101 in
```

4.4.2 Para validar el funcionamiento de las comunicaciones entre los dispositivos de la red A y los de la red B, se debe dar clic en cualquier dispositivo de la red B (PC1 o Laptop1) seleccione la pestaña Desktop y posteriormente seleccione la opción de Command Prompt como se muestra en la Figura No. 6.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	266/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

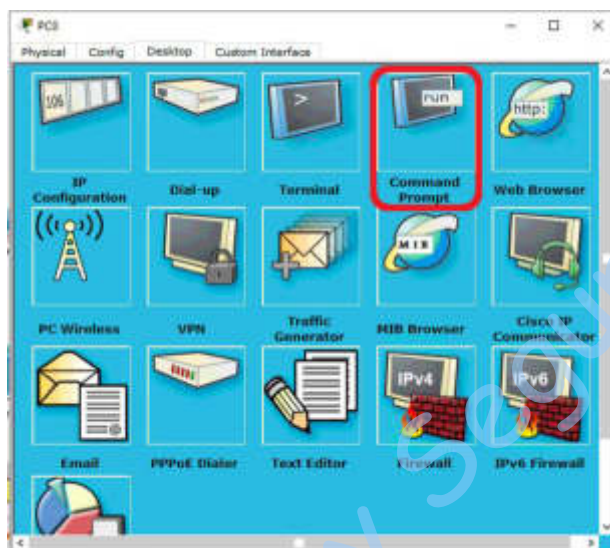


Figura No. 6. Seleccionando la Opción de Command Prompt

- 4.4.3** Usando el comando ping desde el dispositivo seleccionado de la red B pruebe la conexión con el Server0 de la red A. Anote los resultados obtenidos.

El host de destino es inalcanzable

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2


Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>

```

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	267/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4.4 De acuerdo con las reglas de entrada puestas en el Router0 ¿Se logró el bloqueo de los paquetes de entrada en la interfaz Ethernet 1/0 del router? Explique

Nos manda un mensaje de destino inalcanzable que es resultado del bloqueo que se hizo en la interfaz Ethernet 1/0 para el tráfico de entrada.

4.4.5 Seleccione nuevamente la pestaña Desktop y posteriormente seleccione la opción de Web Browser como se muestra en la Figura No. 7.

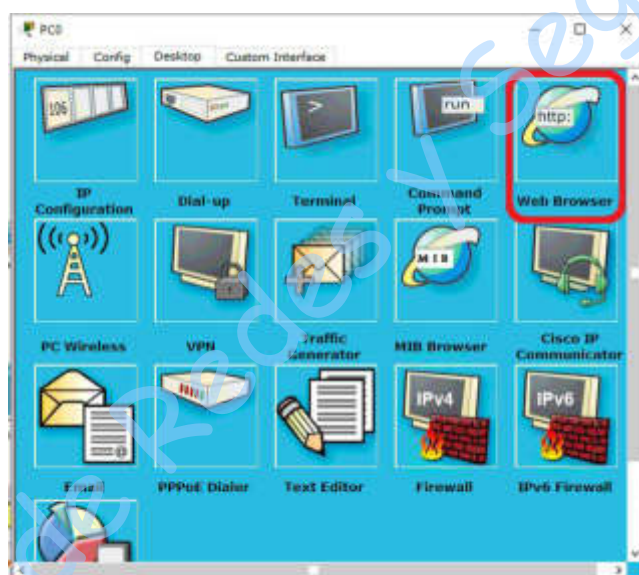


Figura No. 7. Seleccionando la Opción de Web Browser


4.4.6 Coloque en el URL del Web Browser del dispositivo seleccionado de la red B la dirección IP del Server0 de la red A y pruebe la conexión. Anote los resultados obtenidos.

Nos muestra la pantalla de bienvenida o index del servidor A

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
[A small page](#)
[Copyrights](#)
[Image page](#)
[Image](#)

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	268/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

- 4.4.7** De acuerdo con las reglas de entrada puestas en el Router0 verificar si se permite la entrada de los paquetes http en la interfaz Ethernet 1/0 del router. Anote los resultados obtenidos.

En la primera línea denegamos los servicios con un protocolo icmp y con la segunda línea activamos el tráfico disponible para el protocolo http de esa lista desde cualquier red.


- 4.4.8** También es importante probar la conectividad en el sentido inverso desde la red A hacia la red B. Tomando un dispositivo de la red A y repitiendo los pasos desde el 4.4.2 hasta el 4.4.7. Ya que la respuesta que se obtiene no es host-unreachable, indique los resultados obtenidos haciendo uso del comando ping.

Se obtiene request time out

```
Pinging 192.168.2.4 with 32 bytes of data:

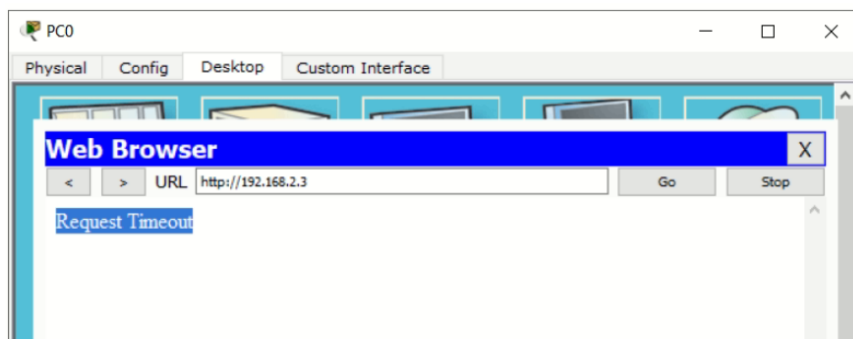
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```


	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	269/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

4.4.9 Indique los resultados obtenidos haciendo uso del Web browser.

igualmente nos manda un mensaje de time out request




EJERCICIO OPCIONAL

4.5 Implementar políticas de acceso al puerto de entrada del Router en la Interfaz Fast Ethernet 0/0 para permitir el acceso al Ping

Las instrucciones para implementar las reglas del firewall que permitan la entrada de los paquetes Ping dentro de la red B, las puede deducir del apartado **Configuración del Firewall a través del Router**.

4.5.1 Proceda a realizar el escenario para definir las reglas de configuración del firewall y así usted podrá definir cuáles servicios se pueden acceder desde una red externa e incluso de alguna que pertenezca a Internet y que sea capaz de acceder a su red local.

4.5.2 Indique los comandos tecleados.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	270/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

```
enable
config t
access list 102 permit icmp any any
interface FastEthernet 0/0
ip access-group 102 in
```

```
enable
config t
access list 101 permit icmp any any
interface FastEthernet 1/0
ip access-group 101 in
```


- 4.5.3** Valide el funcionamiento de las comunicaciones entre los dispositivos de la red A y los de la red B, tomando un dispositivo de la red A y repitiendo los pasos del 4.4.2 al 4.4.7. Indique los resultados obtenidos.

Ya hay funcionamiento dado que activamos en el puerto 0/0 y en el 0/1 el uso de ping

```
Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=0ms TTL=127
Reply from 192.168.2.4: bytes=32 time=3ms TTL=127
Reply from 192.168.2.4: bytes=32 time=0ms TTL=127
Reply from 192.168.2.4: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```


	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	271/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

5.- Conclusiones

Anote sus conclusiones revisando los objetivos planteados al inicio de la práctica.

Martínez Rojas José Eduardo

En resumidas cuentas se logró entender el funcionamiento de un firewall y aplicarlo en la herramienta de cisco packet tracer para limitar el tráfico de alguna red como entrada o salida. También se pudo aprender un poco más sobre los protocolos utilizados y los ACL en este caso los ACL extendidos.

	Manual de prácticas del Laboratorio de Redes de Datos Seguras	Código:	MADO-31
		Versión:	04
		Página	272/297
		Sección ISO	8.3
		Fecha de emisión	17 de agosto de 2021
Facultad de Ingeniería		Área/Departamento: Laboratorio de Redes y Seguridad	
La impresión de este documento es una copia no controlada			

PRÁCTICA COMPLEMENTARIA Y OBLIGATORIA 6

Firewall básico

Cuestionario Previo

1. Mencione la definición de red local y red externa.
2. ¿Qué es un Firewall?
3. Mencione las características de un Firewall con reglas de entrada.
4. ¿Qué es un servidor de red?
5. ¿Para qué sirve el servicio ICMP?
6. ¿Para qué sirve el comando access-list 101 deny icmp any any host-unreachable?
7. ¿Para qué sirve el comando access-list 101 permit tcp any any eq www?
8. ¿Para qué sirve el comando ip access-group 101 in?
9. ¿Cuál es la diferencia entre un Firewall perimetral y uno local?