



Tecnológico de Monterrey

Unidad de formación:
Análisis de criptografía y seguridad

Actividad 3.2. Configuración de Firewalls usando Políticas Basadas en Zonas

Profesores

Oscar Labrada

Alberto Martínez

Integrantes del equipo:

Luis Fernando Navarro Saucedo	A00833148
María Fernanda Lee Ponce	A00830974
Axel Quiroga Caldera	A00832676
Avril Michelle Ruiz	A00833018
Juan Ángel Lucio Rojas	A00833112

Miércoles 07 de junio de 2023

Monterrey, N.L.

Actividad 3.2. Configuración de Firewalls usando Políticas Basadas en Zonas

En este reporte se presenta la siguiente práctica proporcionada por Cisco, para elaborar el programa de la misma empresa global, Cisco Packet Tracer. A continuación, se realizará la configuración de firewalls, que por definición exhibe el tráfico de red de alguna manera, bloqueando el tráfico que se cree pueda ser inapropiado, peligroso o ambos (Freed, N., 2000).

Topología:

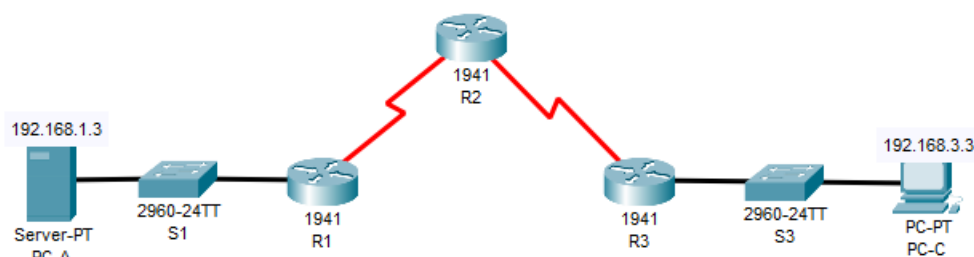


Fig. 1: Topología, Fuente: Cisco

Direcciones:

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	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	N/A	N/A
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	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

Tabla 1: “Direcciones de los dispositivos listados”, Fuente: Cisco

Objetivos:

- Verificar la conectividad de los dispositivos antes de la configuración del firewall.
- Configurar una política basada en zona en R3.
- Verificar Políticas Basadas en Zonas usando ping, SSH y un navegador web.

Escenario:

ZPFs (Firewalls usando Políticas Basadas en Zonas) son el último desarrollo en la evolución de las tecnologías de firewall de Cisco. En esta actividad, se configurará un ZPF básico en un router R3 que permita a los hosts internos acceder a recursos externos y bloquee el acceso de los hosts externos a los recursos internos. Luego, se verificará la funcionalidad del firewall desde los hosts internos y externos.

Los routers han sido pre-configurados de la siguiente manera:

- o Contraseña de la consola: ciscoconpa55
- o Contraseña para las líneas vty: ciscovtypa55
- o Habilitar contraseña: ciscoenpa55
- o Nombre de hosts y direcciones IP
- o Nombre del usuario local y contraseña: Admin / Adminpa55
- o Enrutamiento estático

1. Verificación de la Conectividad de una Red Básica.

En esta parte se verificará la conectividad antes de la configuración ZBP.

- Paso 1: Del comando prompt de PC-A hacer ping de PC-C a 192.168.3.3

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

➤ Paso 2: Accesar a R2 usando SSH

- a. Accesar desde el command prompt con el usuario Admin y la contraseña Adminpa55 para entrar a SSH a la interfaz S0/0/1 en R2 con la ip 10.2.2.2

```
C:\>ssh -l Admin 10.2.2.2

Password:

R2#
```

- b. Salir de SSH

```
R2#exit

[Connection to 10.2.2.2 closed by foreign host]
```

2. Crear Firewalls en R3

➤ Paso 1: Habilitar el paquete Security Technology

- a. En R3, usar comando de ver versión para ver la información del paquete Security Technology y sobre la licencia.

```
R3#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 37 minutes, 15 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
--More--
```

- b. Si no está habilitado el paquete, utiliza el siguiente comando para habilitarlo.

```
R3#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#license boot module cl900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.
```

Use of this product feature requires an additional license from Cisco, together with an additional payment. You may use this product feature on an evaluation basis, without payment to Cisco, for 60 days. Your use of the product, including during the 60 day evaluation period, is subject to the Cisco end user license agreement

http://www.cisco.com/en/US/docs/general/warranty/English/EULKEN_.html

If you use the product feature beyond the 60 day evaluation period, you must submit the appropriate payment to Cisco for the license. After the 60 day evaluation period, your use of the product feature will be governed solely by the Cisco end user license agreement (link above), together with any supplements relating to such product feature. The above applies even if the evaluation license is not automatically terminated and you do not receive any notice of the expiration of the evaluation period. It is your responsibility to determine when the evaluation period is complete and you are required to make payment to Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one product shall be deemed your acceptance with respect to all such software on all Cisco products you purchase which includes the same software. (The foregoing notwithstanding, you must purchase a license for each software feature you use past the 60 days evaluation period, so that if you enable a software feature on 1000 devices, you must purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of your acceptance of this agreement.

- c. Aceptar los términos y condiciones de la licencia.

```
ACCEPT? [yes/no]: yes
```

```
% use 'write' command to make license boot config take effect on next boot
```

- d. Guardar la configuración y reiniciar el router para habilitar la licencia.

IOS Image Load Test

```
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##### [OK]
Smart Init is enabled
smart init is sizing iomem

      TYPE      MEMORY_REQ
      HWIC Slot 0      0x00200000
      HWIC Slot 1      0x00200000      Onboard devices &
      buffer pools      0x01E8F000
-----
TOTAL:      0x02E8F000
Rounded IOMEM up to: 48Mb.
Using 6 percent iomem. [48Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

      cisco Systems, Inc.
      170 West Tasman Drive
      San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040
```

- e. Verificar que el paquete de seguridad ha sido habilitado con el comando de mostrar versión.

License UDI:

```
-----
Device#   PID                      SN
-----
*0        CISCO1941/K9                FTX152446W3
```

Technology Package License Information for Module:'c1900'

```
-----
Technology      Technology-package      Technology-package
Current          Type                    Next reboot
-----
ipbase          ipbasek9                Permanent      ipbasek9
security        disable                 None           securityk9
data            disable                 None           None
```

Configuration register is 0x2102

- Paso 2: Crear una zona de seguridad interna, una IN-ZONE.

```
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
```

- Paso 3: Crear una zona de seguridad externa, una OUT-ZONE.

```
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
```

3. Identificar el tráfico usando Class-Map

- Paso 1: Crear una ACL que define el tráfico interno.

Con el comando de access-list, crear una access list extendida 101 para permitir todas las IPs 192.168.3.0/24 a cualquier destino.

```
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#
```

- Paso 2: Crear una class map referenciando al tráfico interno ACL.

Usa el comando class-map type inspect con la opción match-all para crear un mapa de clase llamado IN-NET-CLASS-MAP, posteriormente usar el comando access-group para encontrar la ACL 101.

```
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
R3(config)#
```

4. Definir las reglas del Firewall

- Paso 1: Crear un policy map para determinar que hacer con el tráfico que hizo match.

Usar el comando de inspección policy-map type y crear un policy map llamado IN-2-OUT-PMAP.

```
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#
```

- Paso 2: Especifique un tipo de clase de inspección y referencia el mapa de clases IN-NET-CLASS-MAP.


```
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#
```

- Paso 3: Especifica la acción de inspeccionar para este policy map.

El uso del comando inspect invoca el control de acceso basado en el contexto (otras opciones incluyen pass y drop).

```
R3(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols
will be inspected
R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#
```

5. Aplicar las políticas del Firewall

- Paso 1: Crea un par de zonas: Utilizando el comando zone-pair security, crea un par de zonas llamado IN-2-OUT-ZPAIR. Especifica las zonas de origen y destino que fueron creadas en la Tarea 1.

```
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#
```

- Paso 2: Especifica el policy map para manejar el tráfico entre las dos zonas. Adjunta un policy map y sus acciones asociadas al par de zonas utilizando el comando service-policy type inspect y haz referencia al policy map creado previamente, IN-2-OUT-PMAP.

```
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#
```

- Paso 3: Asigna las interfaces a las zonas de seguridad correspondientes.: Utiliza el comando `zone-member security` en el modo de configuración de interfaz para asignar G0/1 a IN-ZONE y S0/0/1 a OUT-ZONE.

```
R3(config)#interface g0/1
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#interface s0/0/1
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#
```

- Paso 4: Copia la configuración en ejecución a la configuración de inicio.

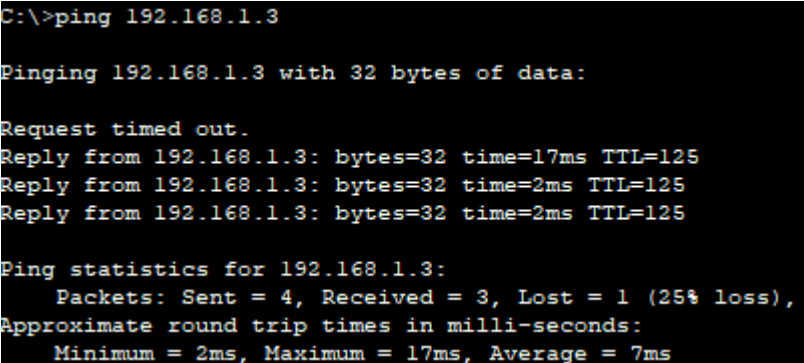
```
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

6. Prueba la funcionalidad del Firewall desde IN-ZONE a OUT-ZONE

Verifica que los hosts internos aún puedan acceder a recursos externos después de configurar el ZPF.

- Paso 1: Desde la PC interna PC-C, realiza un ping al servidor externo PC-A.

Desde la línea de comandos de PC-C, ejecuta el comando `ping` hacia PC-A en la dirección IP 192.168.1.3. El ping debería tener éxito.



```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=17ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 17ms, Average = 7ms
```

- Paso 2: Desde la PC interna PC-C, realiza una conexión SSH a la interfaz S0/0/1 del router R2.

a. Desde la línea de comandos de PC-C, realiza una conexión SSH a R2 en la dirección IP 10.2.2.2. Utiliza el nombre de usuario Admin y la contraseña Adminpa55 para acceder a R2. La sesión SSH debería tener éxito.

```
[Connection to 10.2.2.2 closed by foreign host]
C:\>ssh -l Admin 10.2.2.2

Password:

R2#
```

b. Mientras la sesión SSH esté activa, ejecuta el comando show policy-map type inspect zone-pair sessions en R3 para ver las sesiones establecidas.

```
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR

Service-policy inspect : IN-2-OUT-PMAP

Class-map: IN-NET-CLASS-MAP (match-all)
  Match: access-group 101
  Inspect

    Number of Established Sessions = 1
    Established Sessions
      Session 4026600864 (192.168.3.3:1028)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
        Created 00:02:48, Last heard 00:00:58
        Bytes sent (initiator:responder) [2119:3478]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes

R3#
```

¿Cuál es la dirección IP de origen y el número de puerto?

IP de origen: 192.168.3.3, Puerto de origen: 1028

¿Cuál es la dirección IP de destino y el número de puerto?

IP de origen: 10.2.2.2, Puerto de destino: 22

➤ Paso 3: Desde PC-C, cierra la sesión SSH en R2 y cierra la ventana de la línea de comandos.

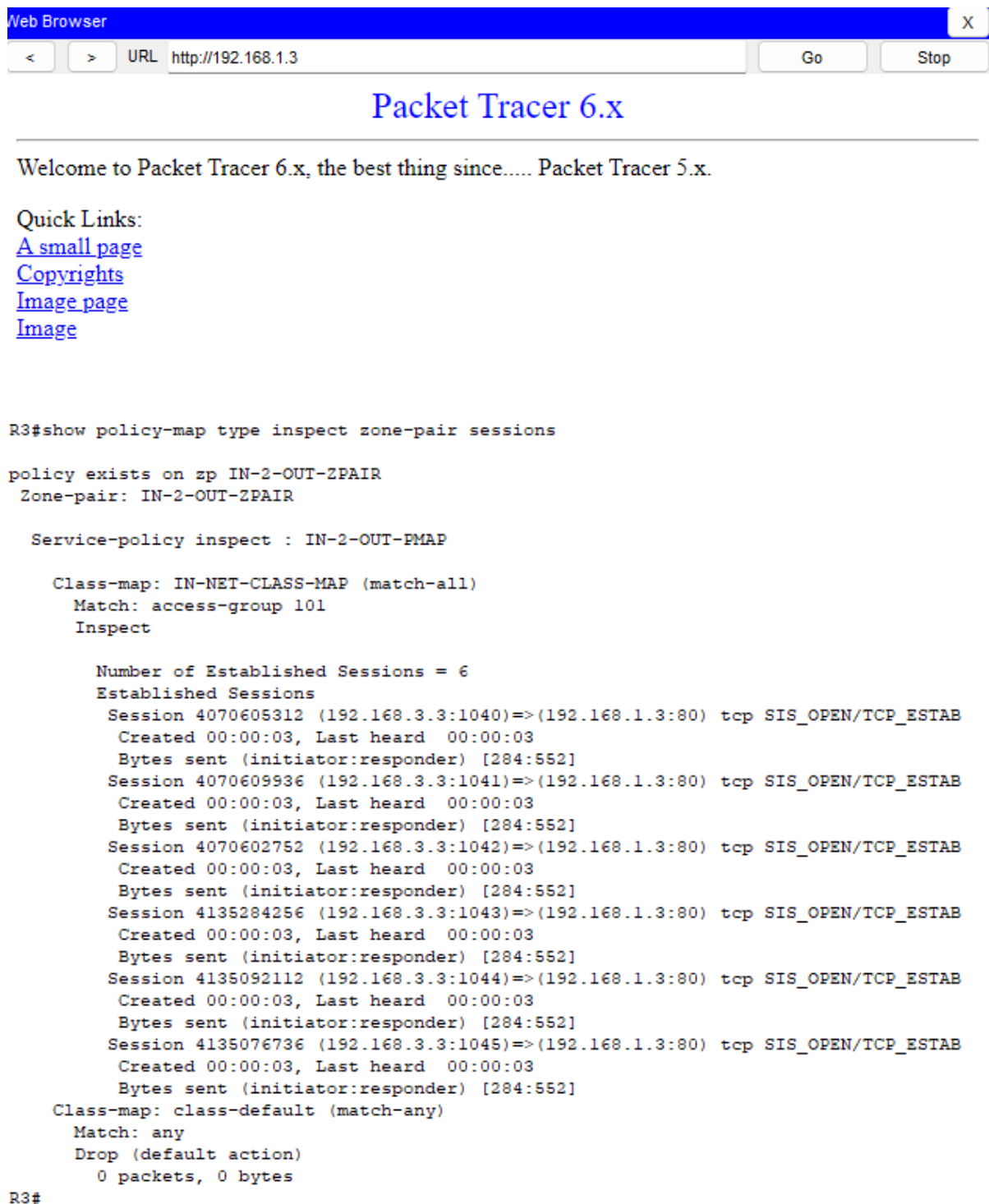
```
R2#exit

[Connection to 10.2.2.2 closed by foreign host]
C:\>
```

- Paso 4: Desde la PC interna PC-C, abre un navegador web hacia la página web del servidor PC-A.

Ingresa la dirección IP del servidor 192.168.1.3 en el campo de URL del navegador y haz clic en Ir (o Enter). La sesión HTTP debería tener éxito.

Mientras la sesión HTTP esté activa, ejecuta el comando show policy-map type inspect zone-pair sessions en R3 para ver las sesiones establecidas.



The screenshot shows a web browser window titled "Web Browser" with a single tab. The address bar contains "http://192.168.1.3" and buttons for "<", ">", "Go", and "Stop". The main content area displays the "Packet Tracer 6.x" logo and a welcome message. Below this, there are "Quick Links" for "A small page", "Copyrights", "Image page", and "Image". The bottom section of the browser displays the output of the command "R3#show policy-map type inspect zone-pair sessions".

```
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR

Service-policy inspect : IN-2-OUT-PMAP

Class-map: IN-NET-CLASS-MAP (match-all)
  Match: access-group 101
  Inspect

    Number of Established Sessions = 6
    Established Sessions
      Session 4070605312 (192.168.3.3:1040)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:03, Last heard 00:00:03
        Bytes sent (initiator:responder) [284:552]
      Session 4070609936 (192.168.3.3:1041)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:03, Last heard 00:00:03
        Bytes sent (initiator:responder) [284:552]
      Session 4070602752 (192.168.3.3:1042)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:03, Last heard 00:00:03
        Bytes sent (initiator:responder) [284:552]
      Session 4135284256 (192.168.3.3:1043)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:03, Last heard 00:00:03
        Bytes sent (initiator:responder) [284:552]
      Session 4135092112 (192.168.3.3:1044)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:03, Last heard 00:00:03
        Bytes sent (initiator:responder) [284:552]
      Session 4135076736 (192.168.3.3:1045)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:03, Last heard 00:00:03
        Bytes sent (initiator:responder) [284:552]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes

R3#
```

¿Cuál es la dirección IP de origen y el número de puerto?

IP de origen: 192.168.3.3, Puerto de origen: 1040

¿Cuál es la dirección IP de destino y el número de puerto?

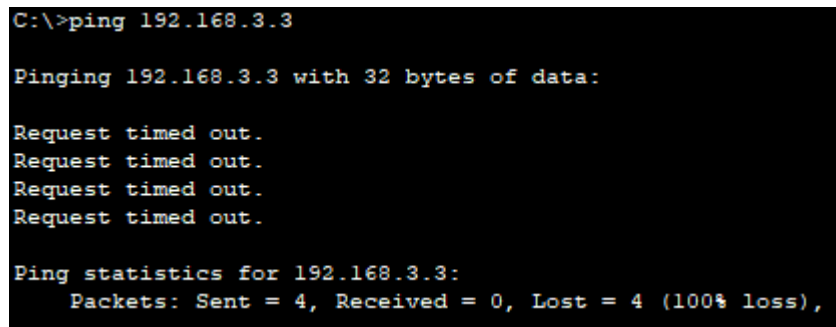
IP de destino: 192.168.1.3, Puerto de destino: 80

7. Prueba la funcionalidad del Firewall desde OUT-ZONE hacia IN-ZONE

Verifica que los hosts externos NO PUEDAN acceder a los recursos internos después de configurar el ZPF.

- Paso 1: Desde el command prompt del servidor de PC-A, realiza un ping a PC-C.

Desde el command prompt del servidora de PC-A, realiza un ping a PC-C en la dirección IP 192.168.3.3. El ping debería fallar.



```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

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

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Paso 2: Desde R2, realiza un ping a PC-C.

Desde R2, realiza un ping a PC-C en la dirección IP 192.168.3.3. El ping debería fallar.

```
R2#ping 192.168.3.3
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)
```

```
R2#
```

➤ Paso 3: Revisa los resultados.

Tu porcentaje de finalización debería ser del 100%. Haz clic en Check results para ver comentarios y verificación de qué componentes requeridos se han completado.

Activity Results Time Elapsed: 04:28:08

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R3				
ACL				
✓ 101	Correct	0	ACL	
Class Maps				
Class Map List				
IN-NET-CLASS-MAP				
Map Type	Correct	1	Other	
Statements	Correct	0	Other	
access-group 101	Correct	1	Other	
Policy Maps				
Policy Map List				
Policy Map N-2-OUT-PMAP				
Inspect Class IN-NET-CLASS-MAP	Correct	1	Other	
Action	Correct	1	Other	
Class Map	Correct	1	Other	
Policy Map Name	Correct	1	Other	
Policy Map Type	Correct	1	Other	
Ports				
GigabitEthernet0/1				
Zone Member	Correct	0	Other	
Serial0/0/1				
Zone Member	Correct	0	Other	
Zone Based Firewall				
Zone Names				
IN-ZONE	Correct	1	Other	
OUT-ZONE	Correct	1	Other	
Zone Pairs				
Zone Pair N-2-OUT-ZPAIR				
Destination Zone	Correct	1	Other	
Name	Correct	1	Other	
Service Policy	Correct	1	Other	
Source Zone	Correct	1	Other	

Score : 15/15

Item Count : 15/15

Component	Items/Total	Score
ACL	1/1	1/1
Other	14/14	14/14

Conclusión:

La práctica anterior se trató de la configuración de firewalls, mediante políticas basadas en zonas. Primeramente se comprobó que hubiera una conexión de ambos dispositivos con la red, y al ser ese el caso, fue notable que era necesario implementar los firewalls.

La creación de Firewalls no puede lograrse sin habilitarse el paquete de Security Technology, el cual tiene los protocolos y procesos necesarios para que se creen las zonas de seguridad tanto interna como externa (inclusive se demostró a modo de prueba y error).

Para verificar que la configuración de firewalls fue exitosa, se usó tanto el método de ping, el protocolo SSH y un navegador web. Con el ping se comprueba una conectividad, y lo

que queremos es que no se establezca. En el caso del protocolo SSH, ya que como este establece conexiones seguras, queríamos que si se establecieran las conexiones y afortunadamente se logró para los routers 2 y 3. Y el navegador web nos permitió observar la conexión entre la PC-C con el servidor PC-A.

Esta actividad fue de mucha utilidad para comprender más el programa de Cisco Packet Tracer, así como para construir firewalls que nos permita proteger el sistema de ciberseguridad para empresas, instituciones y hogares. No es un proceso difícil y en definitiva sería de alta ayuda.

Bibliografia:

Freed, N. (2000). *Behavior of and Requirements for Internet Firewalls*. Network Working Group. <https://www.ietf.org/rfc/rfc2979.txt>