



Instituto Tecnológico y de Estudios Superiores de
Monterrey

**Actividad 3.2. Configuración de Firewalls usando Políticas Basadas
en Zonas**

Nombre	Matrícula
Julio Avelino Amador Fernández	A01276513
Juan Pablo Echeagaray González	A00830646
Verónica Victoria García De la Fuente	A00830383
Erika Martínez Meneses	A01028621
Emily Rebeca Méndez Cruz	A00830768
Ana Paula Ruiz Alvaro	A01367467

Análisis de Criptografía y Seguridad

MA2002B.300

Dr. Alberto Francisco Martínez Herrera

5 de junio de 2022

1. Procedimiento

Los ZPF son lo último en la evolución de las tecnologías de firewalls desarrolladas por Cisco. El objetivo de esta actividad es configurar un firewall basado en políticas de zona (ZPF), esto se hace usando la tabla de direccionamiento que se proporcionó, así como el archivo de Packet Tracer diseñado por *Cisco Networking Academy* [Security, 2018].

Para comenzar a realizar el trabajo se descargó el archivo que se encuentra en la plataforma Canvas, en este se dan los datos de pre-configuración de los sistemas en la red, los cuales son los siguientes:

- Contraseña de la consola: `ciscoconpa55`
- Contraseña para líneas vty: `ciscovtypa55`
- Enable password: `ciscoenpa55`
- Nombres de anfitriones y direcciones IP
- Nombre de usuario y contraseña local: `Admin / Adminpa55`
- Enrutamiento estatico

1.1. Verificación de conectividad

Antes de implementar el firewall, se verifica el estado de la conexión en la red. Primero se realizó un ping desde la **PC-A** hacia la **PC-C** con el IP asociado `192.168.3.3`. El resultado fue exitoso como se puede ver en la figura 1.

Después se usa Secure Shell para acceder al **Router 2** desde **PC-C**. Se conectó a la interfaz `s0/0/1` con el IP `10.2.2.2`; cuando se realiza este proceso es necesario proporcionar la contraseña de administrador dada en la documentación de la tarea. La conexión fue exitosa como se puede ver en la figura 2.

Finalmente, se prueba la conexión entre la **PC-C** y el servidor **PC-A** por medio del buscador de la computadora. Dentro del navegador se captura el IP asociado al servidor `192.168.1.3`, se espera que se despliegue una imagen como la que presentamos en la figura 3.

1.2. Creación de las zonas del Firewall

Se inicia el proceso de creación del firewall verificando que el paquete **Security Technology** esté habilitado. Usando el comando `show version` dentro del **Router 3** en su modo de configuración se despliega un resumen del estado del router; al final se presenta un tabulado como en la figura 4, nótese que en la fila con la celda `security` no hay ningún paquete habilitado.

Para habilitarlo se debe de correr el comando `license boot module c1900 technology-package securityk9` dentro del mismo router en su modo de configuración. Se acepta el acuerdo de usuario, se guardan las modificaciones y se reinicia el router. Para verificar que los cambios realizados han tomado efecto, se usa de nuevo el comando `show version`, ahora este producirá un resultado como el presentado en la figura 5.

Ahora que se tiene habilitado el paquete de seguridad, se crean las zonas `IN-ZONE` y `OUT-ZONE`. Esto se realiza con el comando `zone security ZONE-NAME` en el router en su modo de configuración, al usuario se le pedirán las credenciales pertinentes. Al finalizar este proceso la consola produce un resultado como el de la figura 6.

1.3. Identificación de tráfico usando Class-Maps

Se comienza el proceso de identificado de tráfico con la creación de un `access list` extendido. Desde el router 3 (en modo configuración) diseñamos un permiso para que cualquier IP proveniente de `192.168.3.0` pueda pasar a cualquier destino por medio del comando `access-list 101 permit ip 192.168.3.0 0.0.0.255 any`.

Después se crea un `class map` que haga referencia a todo el tráfico interno del `access list` creado anteriormente, a este mapa se le da el nombre `IN-NET-CLASS-MAP`, esto se logra con la secuencia de comandos `class-map type inspect match-all IN-NET-CLASS-MAP, match access-group 101, exit`.

Los comandos que se corren en esta sección no producen una salida en la consola a menos que haya ocurrido un error, para nuestro caso esto no ha sucedido como se puede ver en la figura 7.

1.4. Especificación de políticas del Firewall

Ya que se tienen el mapa de clases se crea un mapa de políticas para determinar qué sucede con el tráfico que fluye dentro de la red. Dentro del Router 3 en su modo de configuración se corre el comando `policy-map type inspect IN-2-OUT-PMAP`, a esta política después le decimos que tipo de tráfico investigar, le daremos el que se definió en la sección anterior con el comando `class type inspect IN-NET-CLASS-MAP`. Finalizamos por decirle que queremos que investigue este tráfico con el comando `inspect`; se guardan estos cambios al correr 2 veces la ejecutiva `exit`.

Estos comandos producirán una salida similar a la de la figura 8.

1.5. Aplicación de políticas del Firewall

Una vez que se han especificado las políticas del firewall, debemos de configurar su aplicación. Esto comienza al crear un par de zonas que llamaremos `IN-2-OUT-ZPAIR`, se configura con el comando `zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE`.

Le especificamos que use la política definida en el paso anterior con el comando `service-policy type inspect IN-2-OUT-PMAP` y se guarda este proceso con el comando `exit`. Los comandos resultarán en una salida como la presentada en la figura 9.

1.6. Prueba del funcionamiento del Firewall

Para esta etapa el firewall ya ha sido configurado, lo único que resta es comprobar su buen funcionamiento. Verificaremos qué resulta de intentar conectarse del interior del firewall al exterior, y después verificaremos que el tráfico del exterior al interior del firewall es bloqueado.

1.6.1. IN-ZONE a OUT-ZONE

Hacemos una prueba de conexión entre el equipo **PC-C** hacia el servidor externo **PC-A** que tiene el IP asociado `192.168.1.3`. El resultado del `ping` se presenta en la imagen 10.

Después desde **PC-C** se utiliza Secure Shell para conectarse al **Router 2**; mientras que la conexión esté activa se checa el tráfico que viaja por el **Router 3** con el comando `show policy-map type inspect zone-pair`, producirá el resultado que se ve en la figura 11.

Vemos que el IP fuente de la sesión es `192.168.3.3` y que el de destino es `10.2.2.2`. Después terminamos la sesión SSH.

Ahora se realiza la misma prueba del navegador hecha con anterioridad, desde **PC-C** creamos una conexión desde el navegador hacia **PC-A**. Se repite el mismo proceso del paso anterior para identificar el tráfico. Como se puede ver en la figura 12.

En este caso vemos que el IP fuente es `192.168.3.3` y el de destino es `192.168.1.3`.

1.6.2. OUT-ZONE a IN-ZONE

Se realiza una prueba de conexión desde **PC-A** hacia **PC-C**, esta prueba fallará como se demuestra en la figura 13.

Ahora se prueba la conexión desde el **Router 2** hacia **PC-C**, esta prueba también regresará una evidencia de conexión fallida como en la figura 14.

Una vez que se ha realizado todo este proceso y se checan los resultados, el programa arrojará una imagen similar a la de la figura 15.

2. Conclusiones

Esta actividad fue de bastante utilidad para poder entender mejor el funcionamiento de un firewall ZBP. Con la ayuda del software Packet Tracer, pudimos ver la

simulación y el funcionamiento en el mismo y conforme se iba siguiendo el tutorial se fue entendiendo cada comando usado.

Referencias

[Security, 2018] Security, C. (2018). 4.4.1.2 Lab - Configuring Zone-Based Policy Firewalls (Instructor Version).

A. Capturas de pantalla

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

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
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Figura 1: Prueba de conectividad entre PC-A y PC-C

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Admin 10.2.2.2

Password:

R2#exit

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

Figura 2: Prueba de SSH en router 2 desde PC-C



Figura 3: Prueba del navegador entre PC-C y PC-A

```

License Info:
License UDI:
-----
Device#   PID                SN
-----
*0        CISCO1941/K9        FTX152446W3

Technology Package License Information for Module:'cl900'
-----
Technology   Technology-package   Technology-package
              Current    Type                  Next reboot
-----
ipbase       ipbasek9             Permanent            ipbasek9
security     disable              None                  None
data         disable              None                  None

Configuration register is 0x2102

```

Figura 4: Verificación de activación de paquete de seguridad en R3

```

Technology Package License Information for Module:'c1900'
-----
Technology      Technology-package      Technology-package
                  Current          Type          Next reboot
-----
ipbase          ipbasek9          Permanent    ipbasek9
security        securityk9        Evaluation   securityk9
data            disable           None         None

Configuration register is 0x2102

R3#

```

Figura 5: Paquete de seguridad habilitado en R3

```

R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#

```

Figura 6: Creación de zona interna y externa

```

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

```

Figura 7: Creación del class-map para el firewall


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

Figura 8: Especificación de las políticas del firewall

```
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)#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)#
R3(config)#
```

Figura 9: Aplicación de las políticas del firewall

```

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms 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
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

```

Figura 10: Prueba de conexión entre PC-C y PC-A

```

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 2095830576 (192.168.3.3:1027)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
        Created 00:01:23, Last heard 00:01:18
        Bytes sent (initiator:responder) [1064:895]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
R3#

```

Figura 11: Chequeo 1 de sesiones activas a través de R3

```

    0 packets, 0 bytes
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 14557024 (192.168.3.3:1038)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
        Created 00:00:02, Last heard 00:00:02
        Bytes sent (initiator:responder) [284:552]
Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    0 packets, 0 bytes
R3#

```

Figura 12: Chequeo 2 de sesiones activas a través de R3

```

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),

C:\>

```

Figura 13: Prueba de conexión desde PC-A hacia PC-C

```

User Access Verification

Password:

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)

```

Figura 14: Prueba de conexión desde R2 hacia PC-C

Cisco Packet Tracer - C:\Users\pablo\Downloads\4.4.1.1 Packet Tracer - Configuring a Zone-Based Policy Firewall (ZPF).pkt

File Edit Options View Tools Extensions Window Help

Activity Results Time Elapsed: 00:30:34

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	1	ACL	
Class Maps				
Class Map List				
IN-NET-CLASS-MAP				
Map Type	Correct	1	Other	
Statements				
access-group 101	Correct	1	Other	
Policy Maps				
Policy Map List				
Policy Map IN-2-OUT-PMAP				
Inspect Class IN-NET-CLASS-MAP				
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	1	Other	
Serial0/0/1				
Zone Member	Correct	1	Other	
Zone Based Firewall				
Zone Names				
IN-ZONE	Correct	1	Other	
OUT-ZONE	Correct	1	Other	
Zone Pairs				
Zone Pair IN-2-OUT-ZPAIR				
Destination Zone	Correct	1	Other	
Name	Correct	1	Other	

Score : 15/15

Item Count : 15/15

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

Close

Figura 15: Evidencia de finalización de actividad