

PRÁCTICA 8 (almellonesfernandez-practica8)

U.D.3. COMUNICACIÓN DE DISPOSITIVOS Y SISTEMAS INFORMÁTICOS (I). PROXY INVERSO.

Evidenciar toda esta práctica, mediante dos videos, ejercicio número 2 y 3 (videoXXxx-1-2) y ejercicio número 4 (videoXXxx-3), no superior a 3 minutos cada uno (si es posible). Se debe evidenciar cada una de las opciones que aparecen abajo. Si algún apartado/ejercicio no se ha realizado debe ponerse en este enunciado que no se ha realizado.

1. (1 punto) Modificaciones en el firewall perimetral para que lo que llegue por wan en el puerto 8080 (haproxy) y 8404 (estadística de haproxy), sea reenviado al servidor DMZ (10.0.?.2). Servidor donde convivirán tanto el servicio apache (puerto 80) como el servicio haproxy (8080). Es obligatorio mostrar movimiento en contadores.

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v --line-number
Chain PREROUTING (policy ACCEPT 5 packets, 253 bytes)
num  pkts bytes target    prot opt in     out     source               destination           tcp dpt:80 redir por
1    ts 3128 0      0 REDIRECT 6     --  lan2   *       172.16.102.0/24      0.0.0.0/0             tcp dpt:80 redir por
2    ts 3129 0      0 REDIRECT 6     --  wlan2  *       192.168.102.0/24     0.0.0.0/0             tcp dpt:80 redir por
3    0      0 DNAT     6     --  wan2   *       0.0.0.0/0            0.0.0.0/0             tcp dpt:80 to:10.0.1
4    0      0 DNAT     6     --  wan2   *       0.0.0.0/0            0.0.0.0/0             tcp dpt:443 to:10.0.
5    0      0 DNAT     6     --  wan2   *       0.0.0.0/0            0.0.0.0/0             tcp dpt:8080 to:10.0
6    0      0 DNAT     6     --  wan2   *       0.0.0.0/0            0.0.0.0/0             tcp dpt:8404 to:10.0
7    0      0 DNAT     6     --  wan2   *       0.0.0.0/0            0.0.0.0/0             tcp dpt:2222 /* Ej N
ATP */ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination           /* Enmascar de DMZ
1    0      0 MASQUERADE 0     --  *       wan2    10.0.102.0/24      0.0.0.0/0
a WAN */
2    0      0 MASQUERADE 0     --  *       wan2    172.16.102.0/24    0.0.0.0/0             /* Enmascar de LAN
a WAN */
3    0      0 MASQUERADE 0     --  *       wan2    192.168.102.0/24   0.0.0.0/0             /* Enmascar de WLAN
a WAN */
```


Álvaro Almellones Fernández

17	0	0	ACCEPT	17	--	lan2	wan2	172.16.102.3	0.0.0.0/0	udp dpt:53
18	0	0	ACCEPT	1	--	lan2	wan2	172.16.102.3	0.0.0.0/0	
19	0	0	ACCEPT	17	--	lan2	wan2	172.16.102.3	0.0.0.0/0	udp dpt:123
20	0	0	DROP	6	--	lan2	wan2	172.16.102.4	0.0.0.0/0	tcp dpt:80
21	0	0	ACCEPT	6	--	lan2	wan2	172.16.102.4	0.0.0.0/0	tcp dpt:443
22	0	0	ACCEPT	17	--	lan2	wan2	172.16.102.4	0.0.0.0/0	udp dpt:53
23	0	0	ACCEPT	1	--	lan2	wan2	172.16.102.4	0.0.0.0/0	
24	0	0	ACCEPT	17	--	lan2	wan2	172.16.102.4	0.0.0.0/0	udp dpt:123
25	0	0	ACCEPT	0	--	wan2	lan2	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABL
ISHED /* Respuesta WAN a LAN */										
26	0	0	DROP	6	--	wlan2	wan2	192.168.102.2	0.0.0.0/0	tcp dpt:80
27	0	0	ACCEPT	6	--	wlan2	wan2	192.168.102.2	0.0.0.0/0	tcp dpt:443
28	0	0	ACCEPT	17	--	wlan2	wan2	192.168.102.2	0.0.0.0/0	udp dpt:53
29	0	0	ACCEPT	1	--	wlan2	wan2	192.168.102.2	0.0.0.0/0	
30	0	0	ACCEPT	17	--	wlan2	wan2	192.168.102.2	0.0.0.0/0	udp dpt:123
31	0	0	ACCEPT	0	--	wan2	wlan2	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABL
ISHED /* Respuesta WAN a WLAN */										
32	0	0	ACCEPT	6	--	wan2	dmz2	0.0.0.0/0	10.0.102.2	tcp dpt:80
33	0	0	ACCEPT	6	--	wan2	dmz2	0.0.0.0/0	10.0.102.2	tcp dpt:443
34	0	0	ACCEPT	6	--	wan2	dmz2	0.0.0.0/0	10.0.102.2	tcp dpt:8080
35	0	0	ACCEPT	6	--	wan2	dmz2	0.0.0.0/0	10.0.102.2	tcp dpt:8404
36	0	0	ACCEPT	6	--	wan2	dmz2	0.0.0.0/0	10.0.102.2	tcp dpt:22
37	0	0	ACCEPT	0	--	dmz2	wan2	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABL
ISHED										
38	0	0	LOG	0	--	lan2	wlan2	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 4
prefix "LAN to DMZ DENIED AlmellonesF"										
39	0	0	DROP	0	--	lan2	wlan2	0.0.0.0/0	0.0.0.0/0	
40	0	0	LOG	0	--	lan2	dmz2	0.0.0.0/0	0.0.0.0/0	LOG flags 0 level 4
prefix "LAN to DMZ DENIED AlmellonesF"										
41	0	0	DROP	0	--	lan2	dmz2	0.0.0.0/0	0.0.0.0/0	

Chain OUTPUT (policy DROP 0 packets, 0 bytes)

Activar Windows
Ve a Configuración para activar Windows.

192.168.1.111:8080



No se puede acceder a este sitio web

La página 192.168.1.111 ha rechazado la conexión.

Prueba a:

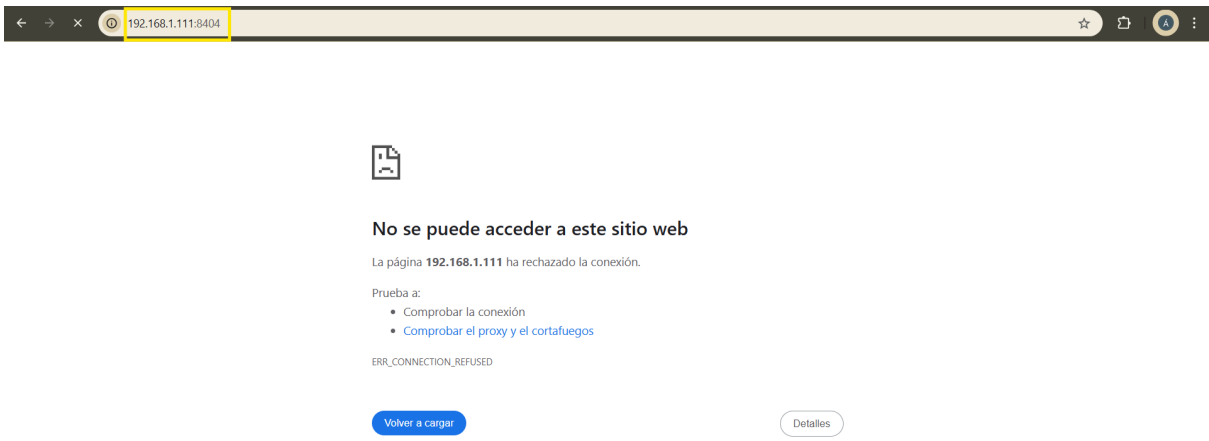
- Comprobar la conexión
- Comprobar el proxy y el cortafuegos

ERR_CONNECTION_REFUSED

Volver a cargar

Detalles

Activar Windows
Ve a Configuración para activar Windows.



Ahora mismo no aparece ninguna página porque no hemos configurado el haproxy, solo lo hemos instalado en el servidor

```
root@almellonesfernandez-firewall:~/scripts# iptables -t nat -L -n -v --line-number
Chain PREROUTING (policy ACCEPT 82 packets, 4207 bytes)
num  pkts bytes target    prot opt in     out     source            destination
1      0      0 REDIRECT  6    --  lan2   *       172.16.102.0/24   0.0.0.0/0          tcp dpt:80 redir por
ts 3128
2      0      0 REDIRECT  6    --  wlan2  *       192.168.102.0/24  0.0.0.0/0          tcp dpt:80 redir por
ts 3129
3      0      0 DNAT      6    --  wan2   *       0.0.0.0/0         0.0.0.0/0          tcp dpt:80 to:10.0.1
02.2:80
4      0      0 DNAT      6    --  wan2   *       0.0.0.0/0         0.0.0.0/0          tcp dpt:443 to:10.0.
102.2:443
5      45    2340 DNAT      6    --  wan2   *       0.0.0.0/0         0.0.0.0/0          tcp dpt:8080 to:10.0
.102.2:8080
6      45    2340 DNAT      6    --  wan2   *       0.0.0.0/0         0.0.0.0/0          tcp dpt:8404 to:10.0
.102.2:8404
7      0      0 DNAT      6    --  wan2   *       0.0.0.0/0         0.0.0.0/0          tcp dpt:2222 /* Ej N
ATP */ to:10.0.102.2:22

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source            destination

Chain POSTROUTING (policy ACCEPT 90 packets, 4680 bytes)
num  pkts bytes target    prot opt in     out     source            destination
1      0      0 MASQUERADE 0    --  *       wan2    10.0.102.0/24     0.0.0.0/0          /* Enmascar de DMZ
```

Álvaro Almellones Fernández

```
15      0      0 DROP      6      -- lan2 wan2 172.16.102.3 0.0.0.0/0 tcp dpt:80
16      0      0 ACCEPT    6      -- lan2 wan2 172.16.102.3 0.0.0.0/0 tcp dpt:443
17      0      0 ACCEPT    17     -- lan2 wan2 172.16.102.3 0.0.0.0/0 udp dpt:53
18      0      0 ACCEPT    1      -- lan2 wan2 172.16.102.3 0.0.0.0/0
19      0      0 ACCEPT    17     -- lan2 wan2 172.16.102.3 0.0.0.0/0 udp dpt:123
20      0      0 DROP      6      -- lan2 wan2 172.16.102.4 0.0.0.0/0 tcp dpt:80
21      0      0 ACCEPT    6      -- lan2 wan2 172.16.102.4 0.0.0.0/0 tcp dpt:443
22      0      0 ACCEPT    17     -- lan2 wan2 172.16.102.4 0.0.0.0/0 udp dpt:53
23      0      0 ACCEPT    1      -- lan2 wan2 172.16.102.4 0.0.0.0/0
24      0      0 ACCEPT    17     -- lan2 wan2 172.16.102.4 0.0.0.0/0 udp dpt:123
25      0      0 ACCEPT    0      -- wan2 lan2 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
ISHD /* Respuesta WAN a LAN */
26      0      0 DROP      6      -- wlan2 wan2 192.168.102.2 0.0.0.0/0 tcp dpt:80
27      0      0 ACCEPT    6      -- wlan2 wan2 192.168.102.2 0.0.0.0/0 tcp dpt:443
28      0      0 ACCEPT    17     -- wlan2 wan2 192.168.102.2 0.0.0.0/0 udp dpt:53
29      0      0 ACCEPT    1      -- wlan2 wan2 192.168.102.2 0.0.0.0/0
30      0      0 ACCEPT    17     -- wlan2 wan2 192.168.102.2 0.0.0.0/0 udp dpt:123
31      0      0 ACCEPT    0      -- wan2 wlan2 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
ISHD /* Respuesta WAN a WLAN */
32      0      0 ACCEPT    6      -- wan2 dmz2 0.0.0.0/0 10.0.102.2 tcp dpt:80
33      0      0 ACCEPT    6      -- wan2 dmz2 0.0.0.0/0 10.0.102.2 tcp dpt:443
34      45 2340 ACCEPT    6      -- wan2 dmz2 0.0.0.0/0 10.0.102.2 tcp dpt:8080
35      45 2340 ACCEPT    6      -- wan2 dmz2 0.0.0.0/0 10.0.102.2 tcp dpt:8404
36      0      0 ACCEPT    6      -- wan2 dmz2 0.0.0.0/0 10.0.102.2 tcp dpt:22
37      90 3600 ACCEPT    0      -- dmz2 wan2 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
ISHD
38      0      0 LOG      0      -- lan2 wlan2 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 4
prefix "LAN to DMZ DENIED AlmellonesF"
39      0      0 DROP      0      -- lan2 wlan2 0.0.0.0/0 0.0.0.0/0
40      0      0 LOG      0      -- lan2 dmz2 0.0.0.0/0 0.0.0.0/0 LOG flags 0 level 4
prefix "LAN to DMZ DENIED AlmellonesF"
41      0      0 DROP      0      -- lan2 dmz2 0.0.0.0/0 0.0.0.0/0
```

Activar Windows
Ve a Configuración para activar Windows.

2. (6 puntos) Shell script lo más personalizado posible (./XXxx-arranque.sh) para arrancar 5 microservicios de una misma imagen (ubuntu+php+apache2) usando para ello un bucle, y del arranque de servicio haproxy (sin dockerizar) configurado para los 5 nodos de forma equitativa. Se valorará de la siguiente forma:

a) (1,5 puntos) Hay evidencias en la misma ejecución del script de que se ha producido el arranque de los 5 microservicios dockerizados y del servicio haproxy, tanto de escuchas como evidencias de establecimiento de la conexión. Enviar mensajes de que se ha producido correctamente el arranque del script.

b) (1,5 puntos) Script lo más personalizado (XXxx, variables) posible con XXxx todo lo que pueda del script (nombre de contenedores, hash de los contenedores, nombre del alumno, nombre de nodos de haproxy, variables, comentarios). Se valorará la claridad, explicación y funcionalidad del script.

c) (1,5 puntos) Hacer una web con php/node lo más personalizable posible donde aparezca la IP que solicitó la petición de la página, día y hora de la conexión, microservicio que ha proporcionado el servicio (nombre del nodo (contenedor) con su IP y puerto) y todo lo que se te ocurra para personalizar y hacer más profesional el ejercicio.

d) (1,5 puntos) En relación a la web de estadística de haproxy (IP/haproxy?stats):

- Fichero de configuración de haproxy personalizado.
- Evidencia donde se comprueba que se ejecuta correctamente en el puerto adecuado y que existen conexiones establecidas tanto desde el cliente como desde el lado del servidor.
- Evidencia de que funciona correctamente el balanceo de carga con todos los nodos/contenedores (se aconseja el uso de un bucle para probar el funcionamiento).
- Evidencia de que si se para **uno** o **varios** contenedores, sigue funcionando el balanceador de carga haproxy sin problemas.
- Evidencia de que sí se para **todos** los contenedores, no se puede descargar la web solicitada, ya que no existen microservicios arrancados.
- Evidenciar que el nodo número 1, responde más veces que el resto de los otros nodos (opción weight).

3. (1 punto) Shell script para la parada y borrado (**./XXxx-paradaborrado.sh**) de los 5 microservicios y parada del servicio haproxy y evidencias en el mismo script de que se ha parado los contenedores y el servicio haproxy. Se deja al alumno que muestre las capturas que se necesite para evidenciar dicho apartado.

4. (2 puntos) Modificación de los dos scripts anteriormente creados (./XXxx-arranque.sh número) (./XXxx-parada.sh número) para que se le pase como opción el número de nodos a arrancar/parar. El número representa el número de contenedores y de nodos del servicio haproxy. Antes de arrancar haproxy habrá que construir previamente el fichero haproxy.cfg con el número de nodos indicado como parámetro (pero no manualmente).

Por ejemplo, se puede probar que se crean 20 contenedores y se adapta el fichero de configuración haproxy.cfg para dichos microservicios. Se deja al alumno que muestre las capturas que necesite para evidenciar que los scripts funcionan correctamente (web de la estadística, ps, netstat, fichero de configuración, conexión desde cliente, etc.). Debe aparecer en la comprobación, que se arranca 20, que posteriormente se borran esos 20, y que después se arranca 15 y se vuelven a parar. Todo ello sin **interrupción** y lanzado mediante los scripts que se han preparado.

NORMAS PARA TODA LA PRÁCTICA.

- **No** se puede usar docker-compose en la práctica.
- Se deja a elección del alumno el número de los puertos para arrancar los diferentes contenedores.
- Uso de volúmenes **obligatoriamente** para la web de los contadores.
- Los **nombres (--name)** de los contenedores tienen que tener **obligatoriamente** de la siguiente forma (XXxx-web1).
- En cada apartado no pueden faltar capturas sobre systemctl, tcpdump, netstat, iptraf-ng y por supuesto de todos los comandos/opciones (docker container ...).
- Personalización lo máximo posible de los diferentes scripts, como son uso de variables, comentarios, comandos para mostrar evidencias en el mismo script (&&, ficheros de configuración, etc). Personalizar lo máximo posible de la web (nombre alumno, contenedor que responde, desde donde se conecta el cliente, etc.).

CRITERIOS DE EVALUACIÓN	
5.a	Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.
5.b	Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.
5.c	Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.
5.e	Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.