Aaron Andal & Cristian Condolo (Iptables) (Repaso Examen)

Reglas:

INPUT:

- Todo lo que **entra** a nuestro ordenador desde **servicio externo**.
- Accede a un **servicio interno** que tenemos.

OUTPUT:

- Todo lo que **sale** de nuestro ordenador hacía un **servicio externo**.
- Accede a un **servicio externo** que hay al exterior.

FORWARD:

- El paquete pasa por nosotros pero no es para nosotros. Lo **reenviamos.**

PREROUTING:

- **Antes** de ser enrutado, se le cambia el **encabezado** y se le aplican **reglas**.

POSTROUTING:

- **Después** de ser enrutado, se le cambia el **encabezado** y se le aplican **reglas**.

PORT FORWARDING:

- **Después** de ser enrutado, se le cambia el **encabezado** y se le aplican **reglas**. Se le **reenvía** a otro **puerto**.

Cheats:

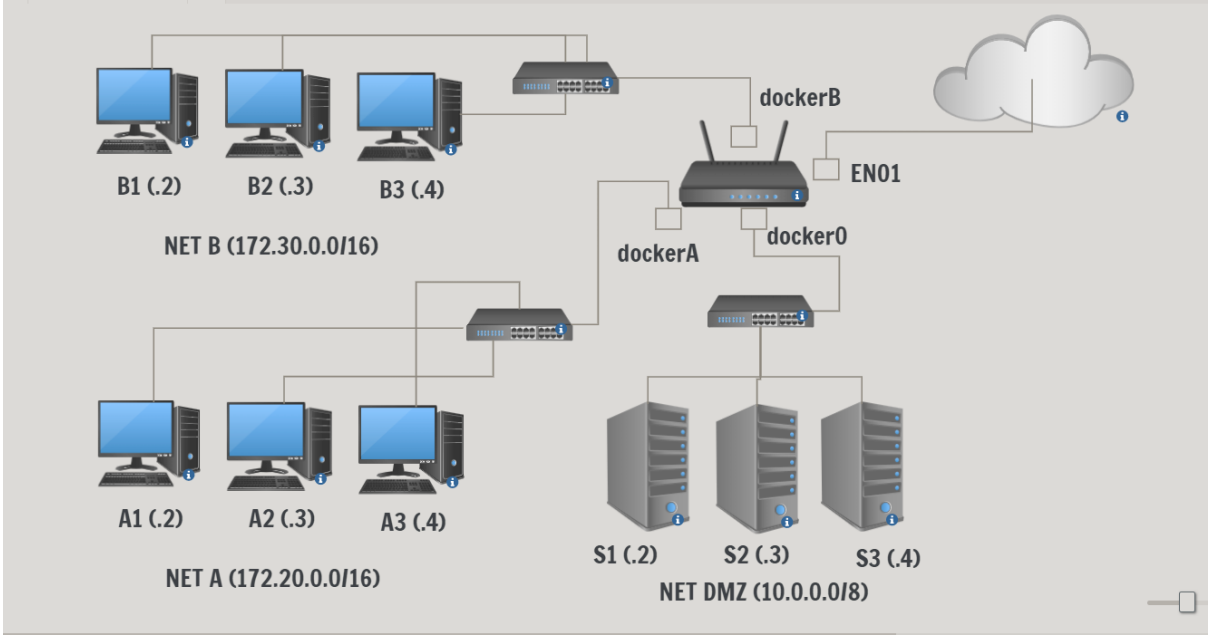
- *1. Crear esquema.*
- *2. Analizar con detalle cada punto.*

NOTA (Importante):

- *No escribir todas las reglas, sólamente las que vayamos a utilizar.*
- *Utiilizar una o más frases que hagan las reglas. Lenguaje natural sin términos informáticos.*
- *Indicar las rutas de **ida** y **vuelta. Si se trata de una respuesta indicarlo claramente.***
- ***Puertos:***
  - ***WEB: 80***
  - ***SMTP: 25***
  - ***SSH: 22***
- *Política por defecto, puede afectar a **forward.** No sabemos si está abierto o cerrado.*

- ☐ En tots els exercicis cal explicar en **una** o **més frases** que fan les regles, en una explicació en llenguatge natural, sense termes informàtics de regles.
- ☐ En tots els exercicis cal indicar **clarament** els **camins d'anada** i **tornada** i si es tracta de tràfic de **resposta indicar-ho apropiadament**.
- ☐ Considerem que per navegar per **internet/web** n'hi ha prou configuració el **port 80** (per simplificar).
- ☐ Desconeixem si la política per defecte es **drop** o **accept**. Ull! En especial això us afecta amb **forward** que no sabem si està ***obert*** o ***tancat***!
- ☐ Els exercicis son independents els uns dels altres.

MAPA



Topología:

S'ha implementat una topologia amb docker segons el model següent:

- **Neta** 172.20.0.0/16, hosts **a1(.2)**, **a2(.2)** i **a3(.3)**.
- **Netb** 172.30.0.0/16 host**s b1(.2)**, **b2(.2)** i **b3(.3)**.
- **Netdmz** 10.0.0.0/8, servers **s1(.1)**, **s2(.2)** i **s3(.3)**.

El ***router*** té les interfícies

- **docker0** per a la xarxa Netdmz
- **dockera** per a la xarxa Neta
- **dockerb** per a la xarxa Netb
- **eno1** per a la xarxa de l'aula (xarxa pública). Useu l'adreça IP del host on esteu asseguts. **lo** per el loopback.

Firewall/ Iptables

1) Escriu les ordres iptables necessàries per buidar de contingut totes les regles actuals i establir política **drop** o **accept** per defecte a les cadenes *input*, *output* i *forward* i *Nat*.

1. **Buidar regles.**

iptables -F - **Flush / Elimina política creada**

iptables -X - **Delete chain / Elimina las reglas**

iptables -Z - **Poner a 0 los contadores de bytes /**

iptables -t nat -F - **FLUSH REGLAS NAT**

2. **Establir polítiques per defecte.**

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -a nat -P PREROUTING ACCEPT

iptables -a nat -P POSTROUTING ACCEPT

2) Escriu les ordres iptables necessàries per fer **nat** de les xarxes **internes NetA** i **NetB**. Escriu una frase(s) explicant què fas.

iptables -t nat -A POSTROUTING **-s** 172.20.0.0/16 **-o** eno1 -j MASQUERADE

iptables -t nat -A POSTROUTING **-s** 172.30.0.0/16 **-o** eno1 -j MASQUERADE

NOTAS:

-t nat -A POSTROUTING = MASQUERADE siempre es POSTROUTING

-s (source) [networkOrigen/mascara]

-o (outputDev) [interficieSalida]

REGLA PARA HACER NAT AL EXTERIOR

3) Al host amfitrió (**router**) no s'hi permeten connexions **SSH** provinents de l'exterior. Excepte si provenen del host 192.168.2.1 . Recorda que no sabem si les polítiques per defecte són **drop** o **accept**. Escriu una frase(s) explicant què fas.

Análisis previo:

Al host amfitrió (**router**) no s'hi permeten connexions **SSH** provinents de l'exterior - **INPUT DROP del exterior pero aceptamos 192.168.2.1.**

Solución:

RESUMEN: *ELLOS HACEN EL SSH (SÓLO 1 MÁQUINA) Y NOSOTROS CONTESTAMOS, EL RESTO BLOQUEADO.*

Todo lo que ***entre*** *(****-A INPUT****) de la (****-s****)* ***IP 192.168.2.1****, que* ***entre*** *de la* ***interface (-i) "eno1"*** *y vaya dirigido al puerto (****--dport*** *)* ***22 SSH*** *de nuestra máquina, lo* ***ACEPTAMOS.***

iptables **-A INPUT** -s 192.168.2.1 **-p** tcp **--dport** 22 **-i** eno1 -j ACCEPT

Todo lo que ***salga*** *de nuestro ordenador (****-A OUTPUT****) a la (****-d****)* ***IP 192.168.2.1****, que* ***salga*** *de la* ***interface (-o) "eno1"*** *y sea una respuesta del (****-m state –state ESTABLISHED,RELATED****) puerto (****--sport*** *)* ***22 SSH*** *de nuestra máquina, lo* ***ACEPTAMOS.***

iptables -A OUTPUT -d 192.168.2.1 -p tcp --sport 22 -o eno1 -m state --state ESTABLISHED, RELATED -j ACCEPT

Todo lo que entre a nuestro ordenador ***dirigidos*** *al puerto* ***22*** *del* ***RESTO*** *y que entren por la interfície* ***"eno1"*** *lo* ***BLOQUEAMOS.***

iptables -A INPUT -p tcp --dport 22 -i eno1 -j DROP

4) Al host **amfitrió (router)** pot fer **connexions ssh** a **la xarxa pública** només si van destinades a la xarxa **192.168.2.0/24** . Recorda que no sabem si les polítiques per defecte són **drop** o **accept**. Escriu una frase(s) explicant què fas.

RESUMEN: *NOSOTROS HACEMOS EL SSH Y ELLOS NOS CONTESTAN (LA RED 2.0/24)*

Todo el ***SSH*** *que* ***salga*** *de nuestro ordenador (****-A OUTPUT****) a la (****-d****)* ***red 192.168.2.0/24****, que* ***salga*** *de la* ***interface (-o) "eno1"*** *y vaya dirigido al puerto (****--dport*** *)* ***22 SSH*** *de la* ***RED 192.168.2.0/24****, lo* ***ACEPTAMOS.***

Toda ***petición SSH*** *que vaya dirigida al* ***puerto 22*** *de la red* ***192.168.2.0/24*** *y que salga de la* ***interfície eno1*** *lo* ***aceptamos.***

iptables -A OUTPUT **-d** 192.168.2.0/24 -p tcp --dport 22 **-o eno1** -j ACCEPT

Todo el ***SSH*** *que* ***entre*** *a nuestro ordenador (****-A INPUT****) que* ***provenga*** *del (****--sport****)* ***PUERTO 22 de la red 192.168.2.0/24****, que* ***entre*** *de la* ***interfaz (-i) "eno1"*** *y sea una respuesta del (****-m state –state ESTABLISHED,RELATED****), lo* ***ACEPTAMOS.***

Todo lo que ***provenga*** *del* ***puerto 22*** *de la* ***red 192.168.2.0/24*** *y sea una* ***respuesta*** *a nuestra* ***petición SSH****, lo* ***aceptamos.***

iptables -A INPUT -s 192.168.2.0/24 -p tcp --sport 22 -i eno1 -m state --state ESTABLISHED, RELATED -j ACCEPT

Todo el ***SSH*** *que* ***salga*** *de nuestro ordenador al* ***RESTO*** *y que* ***salga*** *por la interfície* ***"eno1"*** *lo* ***BLOQUEAMOS.*** *Básicamente no podemos hacer SSH a otras redes pero sólamente a la 192.168.2.0/24.*

Toda ***petición SSH*** *que vaya dirigida al* ***puerto 22*** *del* ***RESTO*** *y que salga de la* ***interfície eno1*** *lo* ***denegamos.***

iptables -A OUTPUT -p tcp --dport 22 -o eno1 -j DROP

5) La **xarxa interna Neta** no pot accedir a cap host de la **xarxa Netb** excepte el **b1**. Recordeu que no sabem si les polítiques per defecte són drop o accept. Escriu una frase(s) explicant que fas.

NetA: 172.20.0.0/16

NetB: 172.30.0.0/16

B1: 172.20.0.2

RESUMEN: NetA** puede acceder **sólamente** a **b1** de la **red NetB. No puede acceder a otros ordenadores.

*Todo lo que **sea reenviado** (**-A FORWARD**) que **provenga** de la (**-s**) **red 172.20.0.0/16** y que vaya dirigido a la **IP 172.30.0.2** de la **netB,** lo **ACEPTAMOS.***

*Todo el **tráfico** que provenga de la **netA,** que pase por nuestro ordenador (**router**) y será reenviado al ordenador **b1 (172.30.0.2)** de la **netB,** será **ACEPTADO.***

iptables -A FORWARD -s 172.20.0.0/16 -d 172.30.0.2 -j ACCEPT

*Todo lo que **sea reenviado** (**-A FORWARD**) que **vaya dirigido** a la (**-d**) **red 172.20.0.0/16** , que **provenga** de la **(-s) IP 172.30.0.2** y sea una respuesta de **él (b1)** del (**-m state –state ESTABLISHED,RELATED**), lo **ACEPTAMOS.***

*Todo el **tráfico de respuesta** que provenga de **b1 (172.30.0.2)** y vaya dirigido a la red **netA,** que pase por nuestro ordenador (**router**) y será **contestado y ACEPTADO.***

iptables -A FORWARD -d 172.20.0.0/16 -s 172.30.0.2 -m state --state ESTABLISHED, RELATED -j ACCEPT

*Todo lo que **sea reenviado** (**-A FORWARD**) que **provenga** de la (**-s**) **red 172.20.0.0/16** y que vaya dirigido a **OTROS ORDENADORES** de la **netB,** lo **DENEGAMOS.***

*Todo el **tráfico** que provenga de la **netA,** que pase por nuestro ordenador (**router**) y será reenviado al **OTROS ORDENADORES** de la **netB,** será **DENEGADO. Sólamente** la **netA puede entrar a la b1,** el resto **FUERA.***

iptables -A FORWARD -s 172.20.0.0/16 -d 172.30.0.0/16 -j DROP

6) Obrir el **port 80** del host **amfitrió** a la xarxa pública perquè en realitat permet l'accés al **servei web (80)** del servidor de la **DMZ s1**. Cal assegurar-se que els **hosts exteriors** poden, doncs, accedir al servidor **web s1**. Recorda que no sabem si les polítiques per defecte són drop o accept. Escriu una frase(s) explicant què fas.

***PREROUTING:** Modifica los paquetes entrantes antes de que se tome una decisión de enrutamiento.*

*Todo el tráfico que será **modificado antes de ser enrutado** y que vaya dirigido al puerto **80 (WEB),** que **entre** por la **interfície "eno1"** se le cambiará el **DESTINO,** por el **router.** Será **reenviado** a **s1** (NetDMZ) al puerto 80 **(WEB)***

*Todo el **tráfico de fuera** que vaya dirigido al **puerto 80 de nuestro ordenador** será **reenviado** al servidor **s1** de la **DMZ (netDMZ)** a su **servidor web (80)**.*

iptables -t nat -A PREROUTING -p tcp --dport 80 -i eno1 -j DNAT --to 10.0.0.2:80

*Todo el tráfico **de afuera,** que entre por la **interfície "eno1"** y que vaya **dirigido** al servidor **web (puerto 80)** de **s1 (10.0.0.2),** serà **ACEPTADO.***

*Todo el **tráfico** que provenga de fuera**,** que pase por nuestro ordenador (**router**), será reenviado al ordenador al **puerto 80 (web)** de **s1 (172.30.0.2),** serà **ACEPTADO.***

iptables -A FORWARD -i eno1 -d 10.0.0.2 -p tcp --dport 80 -j ACCEPT

*Todo el **tráfico de respuesta** que **provenga** del **servidor web (80)** de **s1 (10.0.0.2)**, será **reenviado** (**-A FORWARD**) a la **interfície "eno1",** será **ACEPTADO y contestado.***

*Todo el **tráfico de respuesta** que **provenga del servidor web** (80) del **servidor s1**, pasará por nuestro **ordenador (-A FORWARD)** y será **reenviado** a la **interfície de salida "eno1",** será **contestado** y **aceptado**.*

iptables -A FORWARD -o eno1 -s 10.0.0.2 -p tcp --sport 80 -m state --state ESTABLISHED, RELATED -j ACCEPT

7) Tot **accés** que es **realitza** a un **servidor SMTP exterior/públic** des de la xarxa Neta ha de ser engabiat i enviar al servei **SMTP** del **host s1** de la **DMZ**.

SMTP: port 25

Exterior/públic: -o eno1

NetA: 172.20.0.0/16

*Todo el **tráfico de acceso** que será **modificado antes de ser enrutado** y que vaya dirigido al puerto **25 (SMTP),** que **salga** por la **interfície "eno1"** se le cambiará el **DESTINO,** por el **router,** será **ACEPTADO.***

*Todo el **tráfico de acceso** que vaya dirigido al **puerto 25 a un servidor externo/público** será **ACEPTADO. DNAT =***

iptables -t nat -A PREROUTING -p tcp --dport 25 -o eno1 -j DNAT

*Todo el **tráfico que entre** a la **interfície docker0,** será **reenviado** al puerto **25 (SMTP) del servidor s1 (10.0.0.2),** será **ACEPTADO.***

*Todo el **tráfico de acceso** que entre a la **docker0** irá **dirigido al puerto 25 (SMTP) del servidor s1,** será **ACEPTADO.***

iptables -A FORWARD -i docker0 -d 10.0.0.2 -p tcp --dport 25 -j ACCEPT

*Todo el **tráfico de respuesta que salga** del **puerto 25 (SMTP)** y de la **interfície docker0,** será **contestado y ACEPTADO.***

*Todo el **tráfico de respuesta** que salga de**l servidor SMTP de s1** y de la **interfície docker0,** será **contestado** y **aceptado**.*

iptables -A FORWARD -o docker0 -s 10.0.0.2 -p tcp --sport 25 --sport 25 -m state --state RELATED, ESTABLISHED -j ACCEPT

8) El host amfitrió (el router) pot fer pings pero no en **contesta**.

*8-PING(echo)-REQUEST (**HACER PING**)*

*–ICMP-TYPE **8***

*0-PING(echo)-REPLY (**CONTESTAR PING**)*

*–ICMP-TYPE **0***

Petición** de **PING OK

*Todo el **tráfico ICMP (PING REQUEST)** que **salga** de nuestro ordenador hacía **fuera** lo **aceptamos**.*

*Todo el **tráfico ICMP (PING REPLY) de fuera** que **entre** a nuestro ordenador **aceptamos**.*

Podemos hacer ping y que nos conteste de fuera.

Yo puedo hacer ping al EXTERIOR

iptables -A OUTPUT -p icmp --icmp-type 8 -j ACCEPT

Las respuestas del exterior me las aceptas, porque yo he iniciado el REQUEST DE PING

iptables -A INPUT -p icmp --icmp-type 0 -j ACCEPT

*Todo el **tráfico ICMP (PING REQUEST)** que **salga** de nuestro ordenador hacía **fuera** lo **aceptamos**.*

*Todo el **tráfico ICMP (PING REPLY) de fuera** que **entre** a nuestro ordenador **aceptamos**.*

Podemos hacer ping y que nos conteste de fuera.

No puedo contestar a los pings del EXTERIOR, que te hagan a tu máquina

iptables -A OUTPUT -p icmp --icmp-type 0 -j DROP

No me pueden hacer pings desde el EXTERIOR

iptables -A INPUT -p icmp --icmp-type 8 -j DROP

9) El **host a1** es connecta al **servei web** del host **extern 192.168.2.1**. Indica ip-origen, port-origen, ip-destí, port-destí en cada cas:

*El **destino** se **mantiene**. → **e1 = destino // EN LA IDA***

*El **origen** se **mantiene**. → **e1 = origen // EN LA VUETA***

Router = r1.

Host nuestro = a1 = NUESTRA IP.

***Host remoto = e1 =* 192.168.2.1.**

Puertos dinámicos:

d1:** Puerto dinámico de **a1

d2:** Puerto dinámico de **router r1

Camí d'anada: ip-org:port-org / ip-dest:port-dest

*En la **ida**, desde el **origen, se abre un** puerto dinámico **(d1)** del **host a1** y queremos ir al **puerto 80 (web)** del destino **e1. Se mantiene el destino.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Sortida del host a1: ***a1:d1 → e1:80***

*En la **entrada** al **router**, el **origen** sigue siendo el **mismo** que el **anterior. Se mantiene el destino.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada al Router: ***a1:d1 → e1:80***

*En la **salida** del **router**, el origen se modifica, se cambia a la IP del ROUTER **(r1)** y se cambia a un puerto dinámico del ROUTER **(d2)**. **Se mantiene destino.***

CHEAT: OrigenIP_changeToRouter-r1-Port_changeToPort-D2/ DestIP-Port_same

- Sortida del Router: ***r1:d2 → e1:80***

*En la **entrada** al **host remoto**, el origen **se mantiene** y el destino **se mantiene.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada en el host remot: ***r1:d2 → e1:80***

Camí de tornada: ip-org:port-org / ip-dest:port-dest

*En la **vuelta**, desde el **puerto web 80** del host remoto **e1, se mantiene el origen.** Le devuelve la respuesta al **router (r1)** por el **puerto dinámico** al que le **envió la petición (d2).***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Sortida del host remot: ***e1:80 → r1:d2***

*En la **entrada** al **router**, el **destino** sigue siendo el **mismo** que el **anterior.** **Se mantiene el origen.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada al router: ***e1:80 → r1:d2***

*En la **salida** del **router**, el **destino** se modifica, se cambia a la IP del **host A1(a1)** y se cambia a un **puerto dinámico** del **host A1** (**d1**).* ***Se mantiene origen.***

CHEAT: OrigenIP-Port_same / DestIP_changeTo-A1-Port_changeToPort-D1

- Sortida del Router: ***e1:80 → a1:d1***

*En la **entrada** al **a1**, el origen **se mantiene** y el **destino se mantiene. Se completa la RESPUESTA.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada al host a1: ***e1:80 → a1:d1***

10) El host **Remot 192.168.2.1 (e1)** accedeix al **port 80** del **Router (r1)** que en realitat es redirigit al **servei HTTP** del servidor **s1** de la **DMZ**

*El **destino** se **mantiene**.* → ***e1 = destino // EN LA IDA***

*El **origen** se **mantiene**.* → ***e1 = origen // EN LA VUETA***

Router = r1.

Host nuestro = a1 = NUESTRA IP.

Host remoto = e1 = **192.168.2.1.**

Host DMZ s1 = dmz

Puertos dinámicos:

d1: *Puerto dinámico de **a1***

d2: *Puerto dinámico de **router r1***

Camí d'anada: ip-org:port-org / ip-dest:port-dest

*En la **ida**, desde el **origen, se abre un** puerto dinámico (**d1**) del **host Remoto e1** y queremos ir al **puerto 80 (web)** del destino **router r1.** **Se mantiene el destino.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Sortida del host remot: **e1:d1 → r1:80**

*En la **entrada** al **router**, el **origen** sigue siendo el **mismo** que el **anterior.** **Se mantiene el destino.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada al Router: **e1:d1 → r1:80**

*En la **salida** del **router**, el **destino** se modifica, se cambia a la IP del **s1** (**dmz1**) y hace un **port-forwarding** al **puerto 80** del mismo **servidor**. **Se mantiene origen. Se mantiene puerto destino (port-forwarding)***

CHEAT: OrigenIP-Port_same / DestIP_changeToDMZ-Port_same

- Sortida del Router: **e1:d1 → dmz1:80**

*En la **entrada** del **servidor s1**, el **destino y origen** se **mantienen**.*

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada en el host s1: **e1:d1 → dmz1:80**

Camí de tornada: ip-org:port-org / ip-dest:port-dest

*En la **vuelta**, desde el **puerto web 80** del host **s1 (dmz).** Le devuelve la respuesta al **destino (e1)** por el **puerto dinámico** al que le **envió la petición (d1).***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Sortida del host s1: **dmz1:80 → e1:d1**

*En la **entrada** al **router**, el **origen** sigue siendo el **mismo** que el **anterior.** **Se mantiene el destino.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada al Router: **dmz1:80 → e1:d1**

*En la **salida** del **router**, el **origen** se modifica, se cambia a la IP de origen a la IP del **router(r1)** y el **puerto 80** del **router**. **Se mantiene el destino.***

CHEAT: OrigenIP_changeToRouter-Port_same / DestIP-Port_same

- Sortida del Router: **r1:80 → e1:d1**

*En la **entrada** del **router**, el **origen** sigue siendo el **mismo** que el **anterior**. **Se mantiene el destino.***

CHEAT: OrigenIP-Port_same / DestIP-Port_same

- Entrada al host remot: **r1:80 → e1:d1**