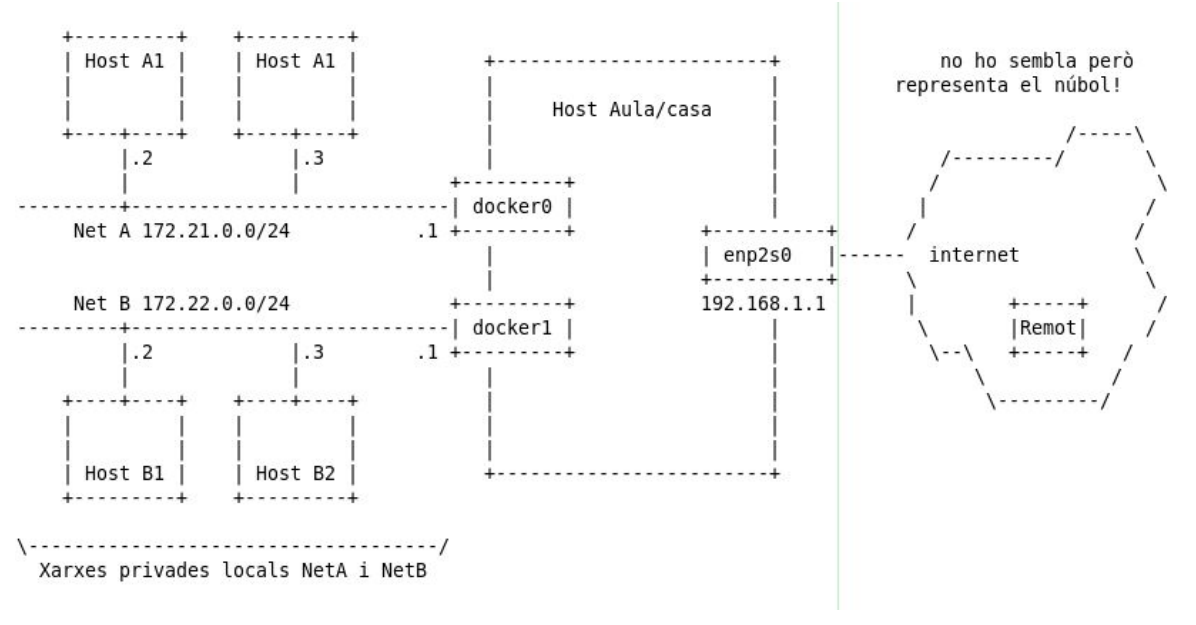
Repàs Firewalls: iptables (3)

Curs 2019 - 2020

Aquest és un repàs dels conceptes de iptables que han de quedar clars i que per l'experiència de classe normalment tot i treballar amb iptables l'alumne barreja una mica. Els concptes que ppreten aclarir són:

- ❏ Input
- ❏ Output
- ❏ Established
- ❏ NAT
- ❏ Forwarding
- ❏ Port forwarding
- ❏ DMZ
- ❏ Drop

Topologia 1: un host normal amb dues xarxes docker internes i connexió a internet



Totes les regles de iptables s'apliquen al host-aula. És on estem practicant definint diferents configuracions de firewalls.

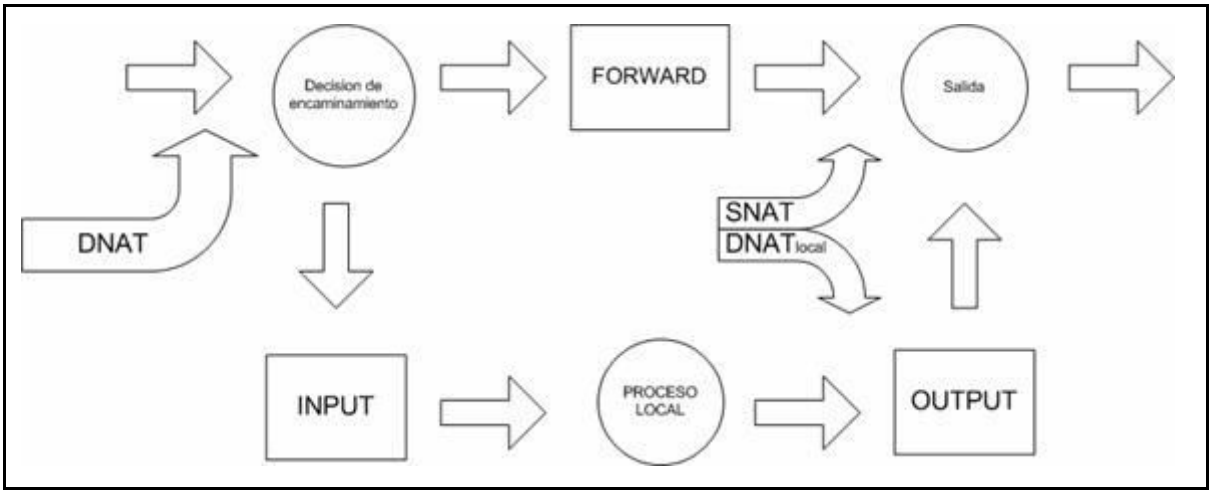
Conceptes

Socket: IP Origen + Port Origen + IP destí + Part Destí.
Connexió: Un socket descriu de manera única una connexió.
Comunicació: (no confondre en connexió) Per establir una comunicació sempre hi ha dos camins (dues connexions) una d'anada i una de tornada. L del origen al destí i la resposta del destí al origen.

Punt de vista: agafem com a punt de vista el host/router en el que estem escrivint les regles de firewall. Així doncs, des del punt de vista d'aquest host tenim (a nivell bàsic):

- ❏ **Input**: el tràfic destinat a quest host.
- ❏ **Output**: el tràfic que s'origina en aquest host.
- ❏ **Forward**: (quan el host és un router) el tràfic que creua el host.

Mapa de cadenes (bàsiques, la cosa es pot complicar moooolt més!) de iptables



Mobelm bé el cap!:

- Si host-aula **conté un servidor web** els clients que s'hi conecten utilitzen un port origen **dinàmic**. Sentit < - - - de la comunicació. El port destí al que es connecten és el port 80 de host-aula, un port **well-known**. Quan el servidor web de host-aula respón el host-aula utilitza de origen el port **well-known** 80 i destina la connexió al port **dinàmic** del client. Sentit - - - - > de la comunicació.
- Si host-aula és un client que vol comunicar amb un servidor web, genera un tràfic de sortida **output** d'un port **dinàmic** seu destinat al port 80 well-known del servidor web. Sentit - - - - > de la comunicació. Quan el servidor web respon la seva resposta prové del seu port origen **well-known** 80 i es destina al host-aula al seu port **dinàmic**. Sentiti < - - - - **input** de la comunicació.
- **Repunyeta!** En tot moment heu de mirar (us recomano dibuixar) cada paquet en quin sentit va, de on a on. Allò que és el origen i el destí en un sentit en la resposta és al revés!.

- **Més repunyeta!** És totalment diferent dir que host-aula **vol accedir** a un servidor web que dir que host aula **és un** servidor web.

Input

És tràfic input tot el tràfic destinat al host-aula. NO que passi pel host aula sinó destinat al host-aula. Qualsevol host que contacti com a destí al **host-aula** quan el tràfic arriba al host-aula aquest és tràfic que entra, **input**. Per tant se li apliquen les regles de input.

Poden ser connexions que provenen de la xarxa externa internet, de les xarxes privades internes NetA i NetB i fins i tot pot ser una propia connexió local de host-aula a host-aula.

Són típics exemples de filtrar input:

- Permetre o denegar el tràfic segons al servei (port) del host aula al que intenta accedir la connexió entrant.
- Permetre o denegar el tràfic segons l'adreça IP del host origen.
- Permetre o denegar el tràfic segons l'adreça IP de la xarxa origen.
- Combinacions de les regles anteriors tipus tots poden, però els d'aquesta xarxa no, però aquest/s concret (de la xarxa negada) si. O a l'inrevés: tots negat, però aquesta xarxa si, però a aquests/s concret (de la xarxa permesa) no.

Un exemple de tràfic és que en el host-aula hi ha obert el port 22 i s'hi connecta algú.

Output

És tràfic output tot el tràfic generat en el **host-aula**, tot el tràfic que es **genera** des del host i que '**surt**'. Tant es pot destinar a internet, com a les xarxes privades locals com al propi host-aula. Aquest tràfic és tràfic **output**.

El destí pot ser qualsevol host, inclòs ell mateix.

Són típics exemples de filtrar input:

- Permetre o denegar el tràfic segons al servei (port) del host aula al que intenta accedir la connexió entrant.
- Permetre o denegar el tràfic segons l'adreça IP del host origen.
- Permetre o denegar el tràfic segons l'adreça IP de la xarxa origen.
- Combinacions de les regles anteriors tipus tots poden, però els d'aquesta xarxa no, però aquest/s concret (de la xarxa negada) si. O a l'inrevés: tots negat, però aquesta xarxa si, però a aquests/s concret (de la xarxa permesa) no.

Un exemple és des del host aula connectar-nos a un servei (web, ssh, etc) d'un altre host o d'ell mateix.

Fixem-nos en el cas de que des del host-aula fem un ssh al mateix host-aula. La part de la connexió sortint és tràfic output i se li aplicarien les regles de output. La part del tràfic

entrant és input i se li aplicarien les regles input. Això usualment NO és així perquè en iptables normalment es configuren les interfícies locals per permetre tot el tràfic local entre elles (tot permès de host-aula a host-aula per qualsevol de les seves interfícies).

Established

Quan estem parlant de TCP sabem que hi ha una connexió inicial de tres vies i que hi ha un establiment de connexió. El client truca a la porta del servidor, negocien i s'estableix una connexió/comunicació. No té sentit en el cas de UDP que no estableix connexió

En el cas de tcp es poden establir regles verificant que el tràfic sigui **established** i **related**. El tràfic en un sentit és el que estableix la connexió i s'exigeix que el tràfic en el sentit contrari sigui només tràfic de resposta.

Per exemple no es permet tràfic **input** del protocol http al host-aula però sí navegar per internet. Això significa que es permet tràfic de sortida **output** cap a servidors de internet però només es permet tràfic d'entrada **input** de tipus http si són respostes al tràfic ja generat, **established / related**. NO si són peticions de tràfic nou entrant.

També és un exemple vàlid el contrari. No es permet al host-aula fer connexions ssh a l'exterior, **output**. Però el host-aula té engegat un servidor ssh i per tant cal permetre les peticions ssh d'entrada **input**. Els clients es connecten al servei ssh (tràfic d'entrada) però el host-aula ha de poder respondre aquestes connexions amb el tràfic de resposta, **established/related**. El que no es permet és iniciar noves sessions ssh des del host-aula a l'exterior.

NAT

Podem transformar un host en un router simplement posant a 1 el bit del kernel de forwarding. Per poder practicar NAT hem de tenir un router. Quan usem docker per defecte ja fa NAT i sualment també ho fan les configuracions de Virtualbox amb màquines virtuals.

Mirant la topologia volem que les xarxes NetA i NetB puguin sortir cap a internet, però no tenen adreces públiques de internet. La solució és que el host-aula faci NAT. Un altre exemple és el router de casa vostra, dins de casa teniu tans hosts i xarxes com volgueu, però des del punt de vista d'internet a casa vostra hi ha un sol host, el router, que és el que té l'adreça IP pública.
NAT Network Address Translation el que fa és enmascarar les adreces IP privades de les xarxes locals (del interior) per sortir a l'exterior usant l'adreça pública del router (el host-aula).

Imaginem un profe 'amb mala llet' que no permet que el alumnes de l'aula facin preguntes, només li permet al delegat de classe. Els alumnes s'organitzen de manera que cada un

d'ells la pregunta que vol fer li diu al delegat. El delegat envia un email al profe i quan aquest li contesta al delegat el delegat reenvia el email a l'alumne que originalment havia fet la pregunta.

Per poder implementar això cal una taula de traslacions (NAT). El delegat ha d'apuntar-se qui li ha fet cada pregunta i quan rep la resposta del profe consulta la taula per saber a qui li ha de reenviar la resposta del profe.

Imaginem que el host A1 té dies connexions a google. Imaginem que el host A2 té una connexió a google. Fixeu-vos que un dels 4 elements (ip origen + port origen + ip destí + port destí és almenys sempre diferent per identificar de manera única una connexió en tot l'univers i part de l'estranger!). Els clients usen ports dinàmics.

Ip:port origen ---- > ip:port destí // Aplicant NAT //	ip:port origen ---- > ip:port destí
A1:dinàmic7 ---- > google:80	host-aula:dinàmic1 ---- > google:80
A1:dinàmic9 ---- > google:80	host-aula:dinàmic2 ---- > google:80
A2:dinàmic3 ---- > google:80	host-aula:dinàmic3 ---- > google:80

Quan el servidor google respon ho fa a host-aula, per ell és amb qui s'està comunicant i no només desconeix sinó que li és impossible poder accedir als hosts de dins de la xarxa privada.

Ip:port origen ---- > ip:port destí // Aplicant NAT //	ip:port origen ---- > ip:port destí
google:80 ---- > host-aula:dinàmic1	google:80 ---- > A1:dinàmic7
google:80 ---- > host-aula:dinàmic2	google:80 ---- > A1:dinàmic9
google:80 ---- > host-aula:dinàmic3	google:80 ---- > A2:dinàmic3

Observeu que el que fa NAT és el que faria el delegat de classe, quan rep de google una comunicació al port dinàmic2 sap que en realitat és una comunicació que ha de destinar al host A1:dinamic 9.

Si mireu la taula de chains que hi ha veureu que quan es fa NAT per enmascarar xarxes privades locals MASCARADE s'aplica SNAT en la sortida del tràfic. SNAT significa que en el paquet de sortida es modifica (s'enganya que és el que significa en anglès mascarade, farsa) l'adreça ip:port origen.

Per tant, seguint l'exemple hi ha un primer salt de A1 a host-aula que és el seu router. Host aula detecta que el destí no és ell sinó google i li aplica el **POSTROUTING SNAT** modificant l'adreça:port origen posant-hi el seu i anotant-ho a la taula NAT.

Quan retorna la resposta de google la resposta va destinada al host-aula, però abans d'aplicar-se les regles input s'aplica el **PREROUTING de DNAT** (ho fa ell automàticament) i 'desembolica' el canvi que havia fet de sortida. El router host-aula detecta que és la resposta de google a la petició que ha fet en nom de A1 i modifica el paquet canviant l'adreca ip:port de destí per la de A1. Ara sí que un cop fet el canvi, com que el paquet creua el router (va de google a A1) s'apliquen les regles de **FORWARD**.

Atenció: un error freqüent dels alumnes, i que està mooolt malament (com el barça!) és creure que es produeixen dos salts, de A1 al router (on s'apliquen regles input) i després un altre salt de host-alumne/NAT a google (on s'apliquen regles output). NO ni parlar--ne.
Tampoc en la resposta tampoc hi ha dos salts de google a host-aula/NAT (on aplicar regles input) i de host-aula/NAT a google (on aplicar regles output). No, no i no!.

Així si que està bé: el tràfic de A1:dinàmic7 va destinat a google:80 i per tant se li aplica el chain FORWARD. En sortir s'aplica POSTROUTING SNAT i es modifica l'adreça ip:port orrigen de manera que realment surt una connexió de host-aula:dinàmic1 ---- > google:80.
Això també: En la resposta la connexió és de google:80 ---- > host-aula:dinàmic7, però ABANS d'aplicar-se qualsevol de les regles input/ output / forward el router detecta que es tracta d'un NAT i li aplica el PREROUTING DNAT modificant l'adreça ip:port destí.De manera que la connexió queda google:80 ---- > A1:dinàmic7.
Finalment: cal tenir en compte que un cop aplicat NAT en la resposta de tornada el paquet 'creua' el router prové de fora (google) i va a la xarxa privada (A1) de manera que se li aplica FORWARD.

Forwarding

És forwarding tot el tràfic que crea el router, que no va destinat ni s'origina en ell. El tràfic que rep però que no va destinat a ell i que ha de retransmetre FORWARD a un altre destí.

Exemple de tràfic forward és el tràfic que generen per exemple els hosts de dins d'una xarxa privada destinat a internet i les respostes que rep de internet. Un altre exemple és el tràfic entre les xarxes NetA i NetB que passa pel router.

Observeu que en una xarxa privada local amb un router fent NAT no hi pot haver tràfic provinent de la xarxa externa destinat als hosts de la xarxa local, perquè no són visibles des de l'exterior (no tenen ip pública). Només podran accedir a la xarxa privada interior en les respostes (NAT) o si hi ha port forwarding.

Exemples de filtrar tràfic forward són:

- Permetre o no tràfic de una xarxa a una altra (passant pel router)
- Permetre o no tràfic de un host a un altre (passant pel router)
- Filtrar també per servei. Els de la xarxa NetA poden accedir a internet però els de la xarxa NetB no, però el host B2 si, etc.

Port forwarding

Fer port forwarding és fer redirecció de ports. En el host-aula que fa de router s'obren ports que en realitat no corresponen a serveis del propi host-aula sinó que es redirigeixen a seveis d'altres hosts (de fet també podria ser redirigits al propi host-aula a un altre port).

Així per exemple imaginem que A1 és un servidor web, A2 és un servidor SMTP, host B1 un servidor ldap i host B2 un servidor kerberos. Podem obrir els port 2080 de host-aula i fer port forwarding al port 80 de A1. Obrir el port 2025 de host-aula que redirigeixi al port 25 de A2, and so on.

La redirecció de ports amb **PORT FORWARDING** s'aplica com a **PREROUTING DNAT**. Abans d'aplicar-se cap de les chains input / output / forward es fa una transformació de la connexió modificat el destí al host:port requerit.

Per exemple un client d'internet connecta al port 2025 del host-aula, la connexió és de client:dinàmic1 ---- > host-aula:2025. Com que el port 2025 és un PORT FORWARDING el sistema aplica PREROUTING DNAT abans que qualsevol altra regla i modifica la ip:port destí. De manera que la connexió queda client:dinàmic ---- > A2:25. Ara sí que un cop feta la transformació de prerouting el paquet entra a l'enrutament i se li aplica FORWARD (perquè prové de client i va destinat a A2).

Un cas estrany però vàlid és fer port forwardind d'un port de host-aula a un altre-port de host-aula. En aquest cas un cop aplicat el prerouting s'aplicaria el chain input perquè el destí seria el propi host-aula.

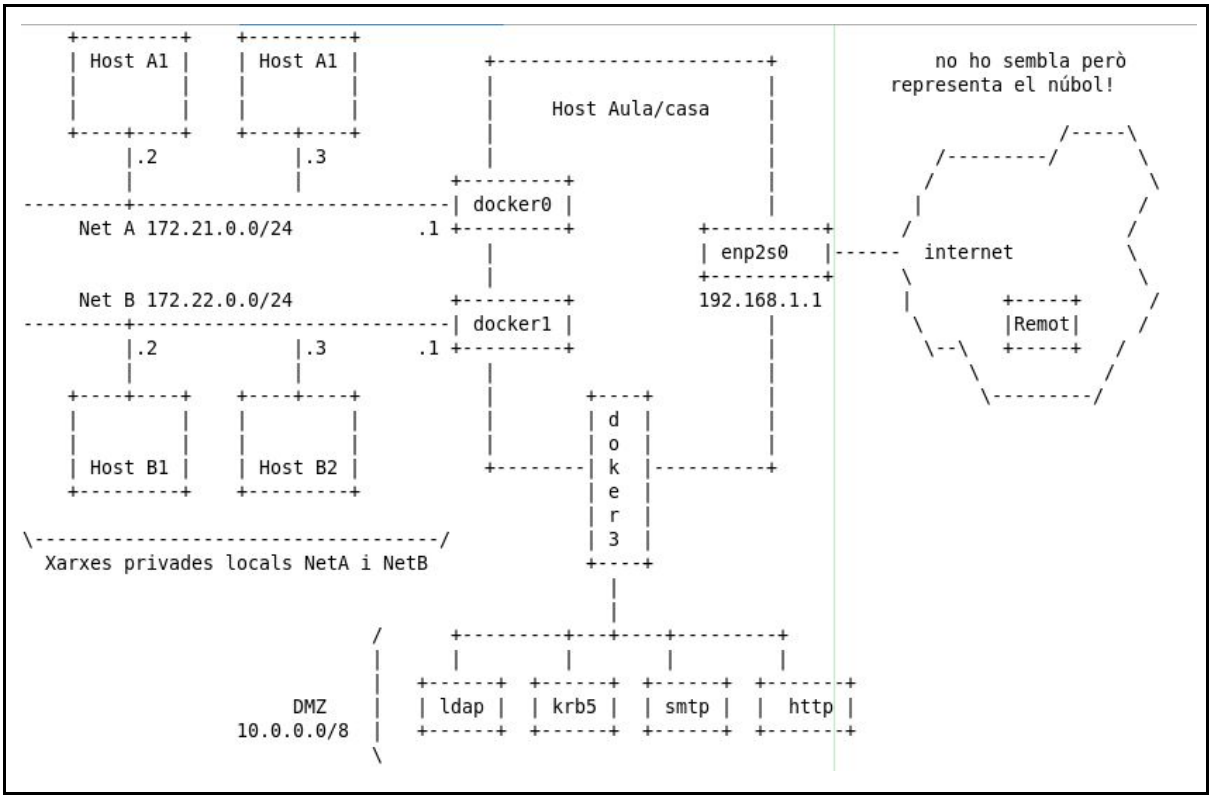
DMZ

Implementar una DMZ DeMilitarized Zone (que sembla que és el contrari que es fa en certs països per les emergències sanitàries!) és en una infraestructura privada destinar una xarxa a servidors segregats de les xarxes de hosts d'usuaris i de l'exterior.

Hi poden haver varis tipus de tipologies diferents, per exemple posar la DMZ entre dos firewalls, un que separa de l'exterior i l'altre de l'interior.

L'objectiu és tenir tots els servidor corporatius en una sola xarxa segregada de la resta de xarxes locals i protegida de l'accés extern. Les regles al firewall determinaran qui pot accedir a quins serveis, tant des de l'exterior com des de les xarxes privades locals.

En l'exemple veiem que hi ha una xarxa segregada 10.0.0.0/8 que conté els servidors ldap, smtp, kerberos i http. En el router host.aula s'estableixen les regles FORWARD i PORT FORWARDING per determinar qui pot accedir a aquests serveis.



Drop

La mare dels ous! La política drop per defect és la política més segura que hi ha, tot el tràfic està denegat excepte aquell que està permès. La dificultat d'implementar aquesta política és:

- Cal que prèviament s'analitzi tot el tràfic per determinar quin és el tràfic que cal permetre. S'ha d'obrir tot allò necessari per al bon funcionament del host (per exemple DHCP, DNS, CHRONY, etc).
- Quan un nou servei o una nova aplicació genera un nou tipus de tràfic (utilitza un port, etc) cal modificar el firewall per permetre aquest nou tràfic.