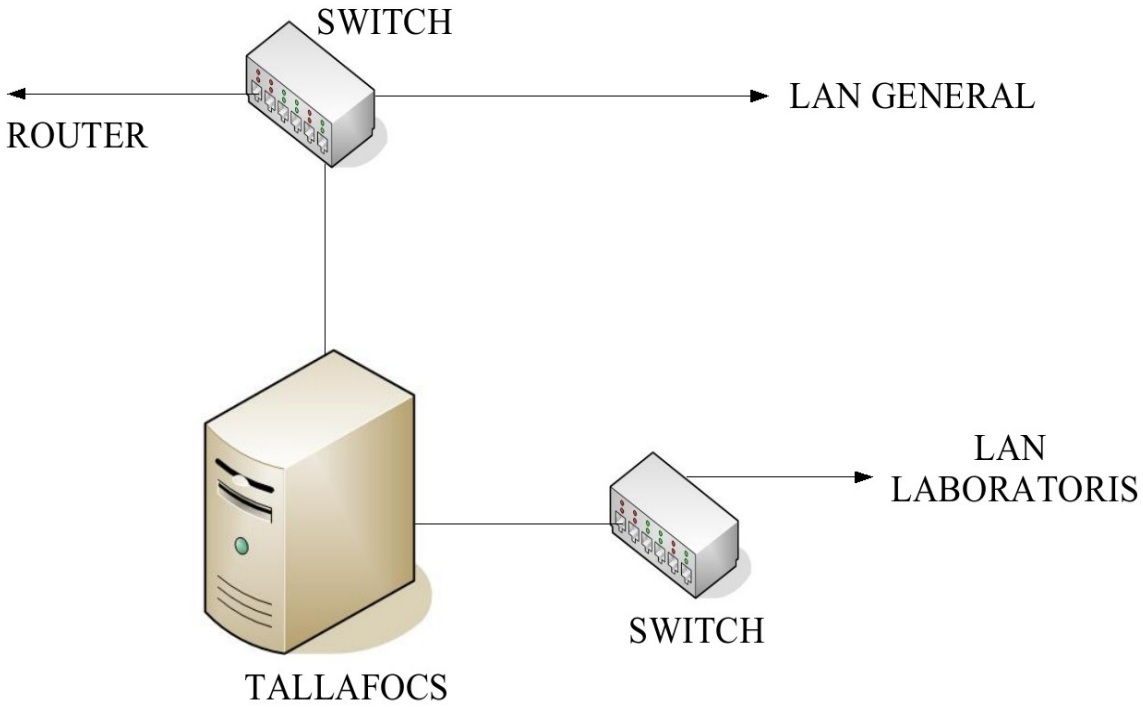
Capítol 7

Tallafocs Linux
Configuració amb IPTABLES
Diferents escenaris amb diferents solucions

7.1 Tallafocs Linux: ús i configuració d'IPTABLES

Un tallafocs es defineix com un dispositiu que filtra el tràfic entre dues xarxes. Podem entendre les xarxes diferenciades com dues porcions diferents d'una mateixa xarxa interna (LAN-LAN) o entre una LAN i la xarxa global LAN-WAN. La seva utilitat en cada cas és diferent.

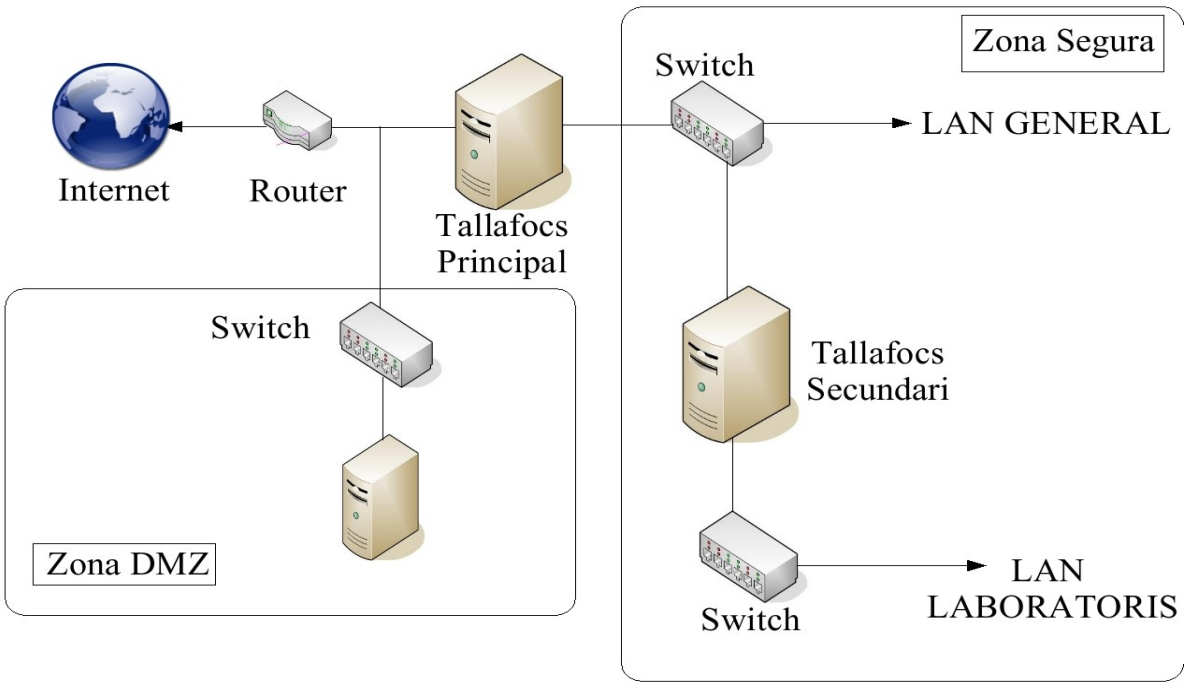
Normalment un tallafocs que separa dues porcions d'una mateixa xarxa interna s'utilitza per motius de privadesa d'una de les xarxes respecte l'altra. L'exemple clar és al centres d'ensenyament on es disposa de seccions de la xarxa interna que per les seves característiques han d'estar emmascarades darrere un tallafocs. Imaginem per exemple un laboratori d'un cicle superior d'informàtica que ha d'estar connectat a la xarxa interna del centre però que no ha d'interferir en el seu funcionament. En aquests laboratoris es fan pràctiques d'instal·lacions de sistemes operatius i de xarxes. Sovint es fan canvis d'IPs i altres modificacions que en estar els ordinadors de prova connectats a la xarxa general del centre implicarien problemes en altres zones de la LAN. La solució és emmascarar tots aquests laboratoris darrere un dispositiu amb una IP única que s'encarregui de dirigir i filtrar adequadament el tràfic de red. Emmascara vol dir que totes les màquines connectades darrere del tallafocs estan representades per la única IP del tallafocs. Evidentment, ha d'haver una separació física entre les xarxes dels laboratoris i la xarxa general perquè això funcioni correctament. Els clients dels laboratoris hauran de ficar una IP dins del tram que marqui el tallafocs i com a passarel·la la IP del mateix. Podem representar aquest cas de manera gràfica amb el següent esquema:



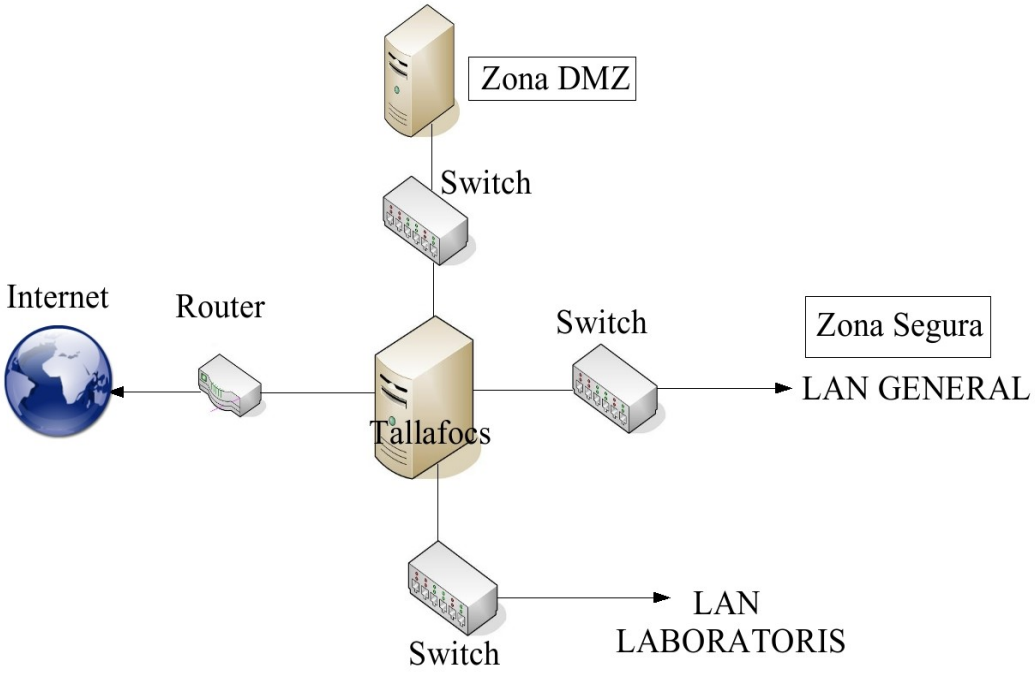
L'altra visió d'un tallafocs és la d'un dispositiu que s'utilitza per filtrar “tot” el tràfic de xarxa existent entre la red interna i Internet. Això ens permet dues coses:

- Filtrar les connexions des de la nostra LAN a Internet evitant d'aquesta manera un ús “poc ètic” de l'ample de banda per part d'algun client.
- Filtrar i redirigir les connexions des de Internet a la nostra LAN, que ens permet augmentar el nivell de seguretat i distribuir les connexions que es reben a ports concrets cap a IPs concretes de la nostra LAN (NAT).

Les dues visions són compatibles i moltes vegades complementàries, com es pot observar en el següent esquema:



La zona marcada com a DMZ (zona desmilitaritzada) és en la que les connexions són lliures i no hi cap mena de filtratge. La resta de la xarxa es converteix en una zona segura (o protegida) per la presència del tallafocs principal i finalment, la zona dels laboratoris es converteix en una LAN privada. Podem definir i intercalar tants de tallafocs com siguin necessaris però cal recordar que un sistema de tipus UNIX suporta múltiples connexions de xarxa (2, 3, 4 ...) i l'eina que utilitzarem per filtrar i reenviar els paquets de xarxa (IPTABLES) permet escollir la destinació i l'origen de les transmissions. Això vol dir que un sol tallafocs ben configurat i unes connexions de xarxa realitzades de la forma correcta poden definir aquesta estructura amb un sol tallafocs.



Amb aquest esquema present el que farem serà veure les possibilitats que ens ofereix un sistema Linux per configurar aquests sistemes de seguretat. L'eina que ens permet fer això és un paquet de programari que s'anomena IPTABLES.

7.2 IPTABLES configuració i nomenclatura

El paquet de programari IPTABLES correspon a una aplicació de tallafocs vinculada al kernel a partir de la versió 2.4 del sistema operatiu. El fet que estigui integrat al sistema operatiu vol dir que no és un "servei". Tècnicament parlant IPTABLES no és cap "dimoni" que escolti en un port determinat per comunicar-se amb cap client ni amb cap procés. IPTABLES està integrat al kernel i el que fem és passar les regles(crear, esborrar o modificar) amb una sèrie d'ordres del sistema (iptables i les seves opcions). Això vol dir que per configurar un tallafocs l'únic que cal fer és escriure un shell-script i executar-lo. El que farem serà ficar el shell-script acabat sota el directori /etc/rc.d per fer que s'engegui en arrancar el sistema ... es a dir que crearem el "procés" d'arrancada del tallafocs per la nostra pròpia mà. El fet que no escolti en cap port fa que sigui més complicat d'explotar qualsevol vulnerabilitat del sistema.

Abans de continuar un comentari, com sempre obligat, sobre com ha de ser el servidor que fa de tallafocs: no fa falta una gran màquina, amb qualsevol ordinador que suporti una instal·lació mínima de Linux i IPTABLES hi ha prou; no ens calen gràfics ja que el que s'ha de fer es col·locar aquest tallafocs en un armari tancat sense teclat, ratolí ni pantalla. Un Pentium II amb 2 Gby de HD, 64 de RAM i tantes targetes de xarxa (el més ràpides possible) com ens calgui. No és aconsellable ficar cap servei ni cap procés addicional en un tallafocs. Això és la teoria, en la pràctica es solen aprofitar servidors ja configurats per crear tallafocs. De totes formes l'avís està escrit, cadascú que faci el que més convingui.

Mirem la nomenclatura que utilitzarem en els següents apartats. IPTABLES té tres tipus de taules per emmagatzemar les regles que han de tractar els datagrames (paquets) que es passen al kernel de Linux i es conserven en unes taules dedicades per cada tipus de regla:

1. FILTER, del que existeixen 3 tipus de regles:

    a) INPUT: que s'apliquen als datagrames que entren al tallafocs destinades a la pròpia màquina.
    b) OUTPUT: que s'apliquen als datagrames que es generen al tallafocs per ser servides a l'exterior.
    c) FORWARD: que s'apliquen a datagrames destinats a altres màquines o xarxes que han de travessar la màquina.

2. NAT, que serveixen per fer redireccions dels paquets entre ports i IPs d'origen i destí amb tres tipus de regles:

    a) PREROUTING: que s'apliquen als datagrames tan prompte arriben al tallafocs.
    b) OUTPUT: que s'apliquen als datagrames generats al tallafocs que s'han de redirigir cap a altres màquines de la xarxa.
    c) POSTROUTING: que s'apliquen als datagrames en el moment de sortir del tallafocs cap a altres destinacions.

3. MANGLE que és un conjunt de regles que permeten modificar els paquets que travessen el kernel. Té cinc tipus de regles definides que són: INPUT, OUTPUT, FORWARD PREROUTING i POSTROUTING. El seu ús és molt particular i únicament necessari en casos específics que no tractaré al curs.

Aquestes regles s'escriuen en taules (en memòria) amb la comanda del sistema *iptables* com ja s'ha comentat amb una sèrie d'opcions i paràmetres. Podem veure els principals paràmetres i opcions si ens mirem el manual en línia de IPTABLES (recordeu # *man iptables*). Els conceptes més importants els resumeixo tot seguit amb la sintaxi de la comanda:

iptables -A <taula> -i <interfície d'entrada> -o <interfície de sortida> -s <IP d'origen> -d <IP de destí> -p <protocol> --sport <port d'origen> --dport <port de destí> -j <acció>

Els paquets poden tenir tres destinacions finals en una regla (l'acció que es fa) :

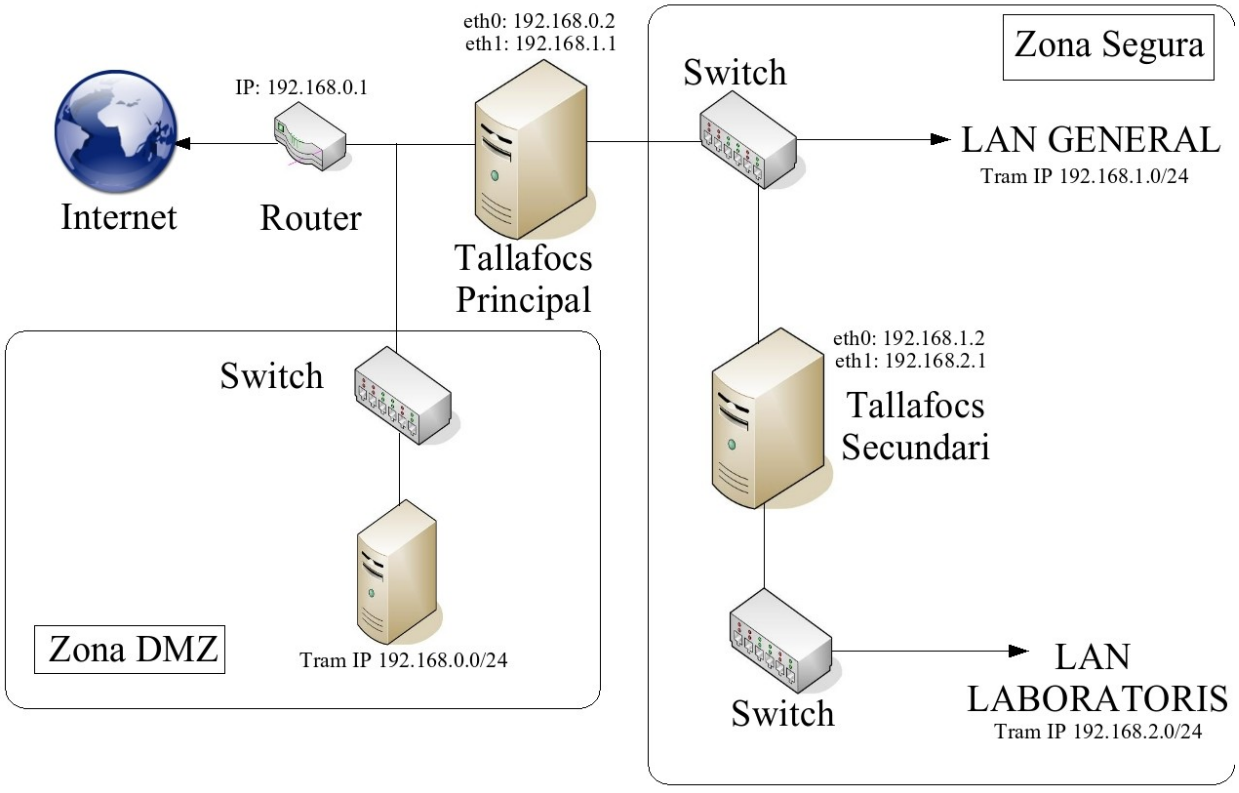
- ACCEPT: es deixa passar el datagrama.
- REJECT: es denega el pas del datagrama però no hi ha cap avís al emissor del paquet.
- DROP: s'ignora el datagrama com si l'ordinador de destí estigues apagat.

Per esborrar totes les regles d'una taula s'utilitzen tres opcions -F, -X i/o -Z. La primera opció esborra les regles una per una, -X esborra les cadenes de regles pròpies de l'usuari (aquelles que no estan definides al kernel) i -Z fica a zero els comptadors de les regles.

Aquestes opcions s'apliquen per defecte a les taules INPUT, OUTPUT i FORWARD de la taula FILTER. Si volem netejar les regles de les taules NAT o MANGLE ens cal especificar-ho explícitament amb l'opció -t: # *iptables -t NAT -F*. Si volem veure les regles aplicades en totes les taules utilitzem les opcions -L -n: # *iptables -L -n*.

7.3 Diferents escenaris i les seves solucions

Recuperem el cas de la xarxa definida anteriorment amb un tallafocs principal i altre de secundari i definim els trams de xarxa que correspon a cada secció de la LAN:



El nostre tallafocs principal, a més a més de tallafocs, té altres funcions (ja sé que em contradic a mi mateix, però us descric un cas real i que funciona força bé ... de moment):

1. És un servidor PROXY (port 3128). Servei restringit a la xarxa interna.
2. És un servidor WEB (port 80 i 443). Servei global.
3. És un servidor SAMBA i WINS (ports 137 i 138). Servei restringit a la xarxa interna.
4. És un servidor de correu SMTP i POP3 (pots 25 i 110). Servei global.
5. Permet connexions segures SSH (port 22). Servei global.
6. Té un WEBMIN per l'administració remota (port 10000). Servei restringit a la xarxa interna.
7. És un encaminadorde la part segura de la xarxa. Servei restringit a la xarxa interna.

El tallafocs secundari únicament fa d'encaminador per la xarxa privada dels laboratoris. Existeixen dos esquemes per plantejar la configuració de tallafocs:

1. Política de acceptació per defecte: els paquets que arriben al kernel “sempre” porten l'etiqueta d'acció ACCEPT, a excepció d'aquells que es deneguen de manera explícita. Podem plantejar un joc d'axiomes per descriure aquesta situació:

    a) Tots els datagrames que arriben de la xarxa local cap al tallafocs pels ports especificats: ACCEPTAR. La resta denega: DENEGAR.
    b) Tots els datagrames que arriben de la xarxa local cap al tallafocs però van cap a l'exterior: EMMASCARAR.
    c) Tots els datagrames que arriben de la xarxa local cap al tallafocs i que van cap a l'exterior pels ports 80 i 443: ACCEPAR.
    d) Tots els datagrames que arriben de l'exterior cap al tallafocs pels ports 22, 25, 80, 110, 443: ACCEPTAR.
    e) Tots els datagrames que arriben de l'exterior cap al tallafocs pels ports 1 a 1024: DENEGAR.
    f) Tots els datagrames que arriben de l'exterior cap al tallafocs pel port 10000: DENEGAR.

2. Política de denegació per defecte: els paquets que arriben al kernel “sempre” porten l'etiqueta d'acció DROP, a excepció d'aquells que s'accepten de manera explícita. Això implica una sèrie de conseqüències: les connexions permeses s'han d'explicitar en dos sentits (doble feina) encara que resulta un tallafocs molt segur.

Mirem quines són les regles que aplicarem en el primer cas de política d'acceptació per defecte. Abans de filtrar esborrarem totes les regles de les taules existents i definirem quina és la política per defecte en cada una de les taules utilitzades:

```
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

Ara comencem a filtrar els datagrames que arriben al tallafocs i són per al tallafocs (INPUT). Introduïm les regles a la taula INPUT per els datagrames que provenen de la mateixa màquina o de

la nostra xarxa interna com les que segueixen:

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -i eth1 -j ACCEPT
```

Ara mirem com filtrem els datagrames que venen de qualsevol altra xarxa:

```
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 22 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 25 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 80 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 110 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 137 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 138 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p udp  -dport 137 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p udp  -dport 138 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -p tcp  -dport 443 -j ACCEPT
iptables -A INPUT -s 0.0.0.0/0 -i eth0 -p tcp -dport 1:1024 -j DROP
iptables -A INPUT -s 0.0.0.0/0 -i eth0 -p udp -dport 1:1024 -j DROP
iptables  A INPUT  -s 0.0.0.0/0 -i eth0 -p tcp  -dport 10000 -j DROP
```

Fins aquí s'han filtrat els datagrames destinats al nostre tallafocs. Ara mirem què fem amb els datagrames que rep el tallafocs des de la xarxa interna cap a Internet (FORWARD):

```
iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p tcp  -dport 80 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -p tcp -dport 443 -j ACCEPT
iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -j DROP
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Amb aquesta configuració per el tallafocs ja ens funcionaria raonablement bé. Però, en realitat, com que tenim un proxy funcionant i escoltant al port 3128 el que volem és que els nostres clients passin tots ells pel proxy (creem un proxy transparent). Ens cal afegir una redirecció a la taula NAT:

```
iptables -t nat -A PREROUTING -i eth1 -s 192.168.1.0/24 -d ! 192.168.1.0/24 -p tcp --
dport 80 -j REDIRECT --to-port 3128
```

A l'annex 3 es pot veure el shell-script d'una sola tirada i amb comentaris. A partir d'ara, en els exemples que segueixen, únicament ficaré una còpia del shell-script i faré una explicació prèvia de l'escenari al que s'ha d'aplicar el shell-script. Part del material del curs consisteix en un conjunt de shell-script on es poden trobar entre altres els que aquí us proposo per als escenaris que s'indiquen en cada cas.

La meva intenció no és ficar una biblioteca de shell-script per configurar tallafocs, ja que molt sovint els problemes i les seves solucions no es poden transportar d'una xarxa a altra. En canvi, si que intento exposar casos concrets amb solucions concretes que poden donar una pista de com resoldre escenaris semblants o que donin solució parcial a casos més generals.

Mirem ara quina hauria de ser el shell-script per el tallafocs secundari. Recordem que aquest sí que és una caixa “negra” que l'únic que ha de fer és rebre els datagrames de la xarxa privada dels laboratoris i encaminar-la cap a la resta de la xarxa. No té cap servei en marxa i ningú ha de treballar en ell a excepció de l'administrador que es connectarà “sempre” via SSH (en línia de comandes) des del tallafocs principal. Per fer aquesta configuració partirem de la segona política: DENEGAR per defecte.

Com abans, netegem les regles de les diferents taules i marquem la política per defecte:

```
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP
```

Comencem a marcar les regles per acceptar connexions. Cal fixar-se en el detall de que s'han de doblar aquestes regles. Primer indicarem al tallafocs que la connexió des del tallafocs principal (192.168.1.1) pel port 22 (SSH) està permesa:

```
iptables -A INPUT -s 192.168.1.1/0 -p tcp  -dport 22 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.1/0 -p tcp  -dport 22 -j ACCEPT
```

Ara ens cal emmascarar la xarxa dels laboratoris i permetre que passin datagrames cap a la xarxa externa i des de la xarxa externa (en els ports que necessitem 80 i 443):

```
iptables -A FORWARD -s 192.168.2.0/24 -i eth1 -p tcp  -dport 80 -j ACCEPT
iptables -A FORWARD -s 192.168.2.0/24 -i eth1 -p tcp -dport 443 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Aquesta seria la versió restrictiva (molt i molt) ja que des dels laboratoris pràcticament no podrien fer cap connexió que no fos pels ports 80 i 443. Per donar més flexibilitat a aquesta proposta faríem una barreja amb l'anterior: les taules INPUT i OUTPUT amb política de denegació per defecte i la taula FORWARD amb política de ACEPTACIÓ per defecte. A l'annex X hi ha el shell-script resultat per aquest cas.

Referències:

[1] Projecte IPTABLES. Pàgina oficial: http://www.iptables.org