Universitat de Lleida
Escola Politècnica Superior
Enginyeria Tècnica en Informàtica de Sistemes

Projecte Final de Carrera

Disseny d'una eina visual per a la configuració d'Iptables

Autor: Joel Bernaus Bernaus

Tutor: Francesc Sebé Feixas

6 d'octubre de 2014

Índex

Capítol 1

Introducció

Un tallafocs és un aparell que s'encarrega d'arbitrar el trànsit de dades en una xarxa informàtica, permetent aquelles comunicacions que són autoritzades. En aquest capítol s'explica la importància i necessitat dels tallafocs. Així mateix, també es detalla el propòsit del treball i com s'ha estructurat aquest document.

1.1 Antecedents i Motivacions

Els primers intents de crear una gran xarxa informàtica interconnectada els trobem en ARPANET, una xarxa informàtica militar desenvolupada pel departament de defensa dels Estats Units a partir del 1969. Però no va ser fins l'1 de gener de 1983 que va néixer Internet; quan la National Science Foundation (NSF) dels Estats Units va crear la primera xarxa de llarg abast basada en la tecnologia TCP/IP. Des de llavors, el creixement d'aquesta xarxa ha estat immens. Segons les estadístiques [1], el 30 de juny de 2012 Internet comptava amb 2,405,518,376 usuaris, és a dir, més d'una tercera part de la població mundial. Entre l'any 2000 i el 2012, el nombre d'usuaris ha crescut un 566,4%.

El 2 de novembre de 1988 Robert T. Morris [3], un llicenciat de la Universitat de Cornell, va llençar des del MIT el primer *worm* de la història, conegut com a Morris Worm, amb la intenció de dimensionar el tamany de la xarxa. Aquest s'aprofitava d'uns forats de seguretat en alguns serveis dels sistemes operatius basats en UNIX. Ràpidament va infectar un 7% dels ordinadors d'arreu del món. Donat que les rutines de propagació i encriptació del worm alentien les màquines infectades no es va trigar massa a notar els efectes de la infecció i va causar pèrdues bastant importants. Un grup de voluntaris anomenats VirusNet, van investigar-ho [4] i en 36 hores van trobar la manera de neutralitzar-lo.

El 2005, uns *hackers* van obtenir les dades de pagament de 40 milions de targetes de crèdit comprometent terminals de pagament de diversos cen-

tres comercials i cadenes de botigues. Tot i la obligació de complir amb l'estàndard de seguretat PCI-DSS, que estableix la configuració de seguretat que han de complir els equipaments que realitzen pagaments amb targeta, es van trobar errades en la implementació que els va permetre accedir als registres dels pagaments de la memòria RAM dels Terminals de punt de venda, on la informació no estava protegida. Per solucionar el greu problema de seguretat es van haver de refer els protocols i es va desenvolupar la tecnologia del "chip-and-pin" que permet el xifratge de les dades durant tot el procés del pagament, encara que, per compatibilitat i degut a la complexitat de l'adopció dels nous mètodes, aquestes targetes continuen duent una banda magnètica que en usar-la fa que el sistema continuï sent insegur.

Tenint en compte el creixement en l'ús d'internet per a la vida quotidiana, cada cop és més important disposar de mecanismes que assegurin la privacitat de les comunicacions i la seguretat dels equipaments que emmagatzemen dades sensibles i protegeixen els canals de les comunicacions en que s'empren aquestes dades. Aquesta seguretat s'aconsegueix en diferents nivells i per diferents vies: en el canal, emprant criptografia; en el perímetre, emprant tallafocs i en l'accés, controlant el nivell d'accés a les comunicacions.

Un tallafocs és un dispositiu emprat en les xarxes informàtiques que té com a finalitat comprovar les comunicacions i permetre-les, o no, segons estigui establert en les polítiques de xarxa del sistema. Normalment se situa en el punt de connexió entre la xarxa interna i l'externa, Internet, i s'encarrega de protegir la xarxa local d'intents d'accés no autoritzats des de fora. També es pot utilitzar per connectar una segona xarxa local que aplegui aquells equips que tenen la necessitat d'altres condicions d'accés, per exemple, accés total des de l'exterior. Aquesta segona xarxa local és anomenada llavors *zona desmilitaritzada* (DMZ), on es troben normalment els servidors que han de ser accessibles des de la xarxa exterior o Internet. També es pot connectar un segment de la xarxa amb l'accés totalment restringit des de l'exterior, on es podrien allotjar servidors amb dades sensibles a les quals es pogués accedir només a través d'un servidor allotjat a la DMZ, actuant d'intermediari en la comunicació, el que es coneix com a proxy.

Els tallafocs afegeixen seguretat a la xarxa aïllant els equips i bloquejant les connexions no autoritzades, però només són un nivell més de protecció, i en cap cas es poden considerar suficients. Ja que només protegeixen les connexions que transiten a través d'ells, la xarxa continua essent vulnerable si l'atacant obté accés físic a la xarxa, o si utilitzant IP spoofing es fa passar per un equip autoritzat o si senzillament introdueix un mètode d'intrusió en un equip local, per exemple un cavall de Troia en un USB.

Generalment, les funcions que realitzen els tallafocs són:

- controlar l'accés des de la xarxa interior cap a fora, i viceversa,
- filtrar els paquets que passen per la xarxa,

- emmagatzemar i analitzar els paquets en cas de problemes,
- i monitoritzar el trànsit de dades.

1.2 Propòsit del treball

El propòsit d'aquest treball és desenvolupar una eina visual per a la configuració d'Iptables (el tallafocs per software implementat en Linux). Aquesta tasca s'ha desenvolupat seguint els següents passos:

- Estudi del funcionament d'Iptables: regles, comandes, opcions,... (veure capítol 3)
- Lectura i aprenentatge de les funcions de Java que permeten el disseny gràfic (veure secció 4.2).
- Implementació d'una eina visual que permet dibuixar l'esquema d'una xarxa (veure capítol 4).
- Generació automàtica de les regles bàsiques d'Iptables (veure secció 4.1.6).

La memòria d'aquest treball està estructurada en 5 capítols. En el capítol 2 es fa una breu introducció a les xarxes de comunicacions, tant a nivell d'estructura com de seguretat. En el capítol 3 s'explica el funcionament i configuració d'Iptables. En el capítol 4 es detalla el disseny de l'eina visual, així com la metodologia emprada per la seva implementació. Finalment, en el capítol 5 es llisten les millores que es podrien integrar en un possible treball futur.

Capítol 2

Xarxes de Computadors

En aquest capítol es detallen els elements que conformen una xarxa de comunicacions i els símbols amb els que es representen els seus components en els esquemes. També s'explica el model de comunicacions TCP/IP i l'OSI. Finalment, es parla de la seguretat en les comunicacions i dels tallafocs.

2.1 Model de comunicacions

A mesura que les xarxes informàtiques creixien en complexitat es va anar fent més i més necessari trobar una manera de simplificar i compatibilitzar el seu funcionament. Un model de comunicacions és una forma d'estandarditzar el funcionament d'una xarxa informàtica dividint-lo en diferents nivells, amb la intenció de diferenciar la part lògica de la física. Proporciona, doncs, un model de referència per als fabricants i implementadors, aconseguint d'aquesta manera una major compatibilitat i interoperabilitat entre les diferents xarxes. Això s'aconsegueix establint un conjunt de guies de disseny i de protocols per a que els equips es puguin comunicar entre ells independentment de les seves diferències.

Els models més importants són l'OSI i el TCP/IP. L'especificació d'aquest últim va ser acabada anteriorment a l'OSI i podria arribar a ser considerat més simple. Tot i això, és el que s'utilitza en Internet.

2.1.1 Transmission Control Protocol/Internet Protocol

És el model de xarxa emprat a Internet. Realment s'anomena *Internet Protocol Suite* però és més conegut com a Transmission Control Protocol/Internet Protocol (TCP/IP) pels dos protocols més importants que defineix. Va ser desenvolupat amb finançament del departament de defensa dels EUA presumiblement per articular ARPANET, la precursora d'Internet. Està definit en la norma RFC-1122 [2].

Aquest model consta de 4 capes:

- NIVELL 4, Aplicació: Estableix com un programa d'un ordinador es pot comunicar amb el d'un altre ordinador.

- NIVELL 3, Transport: Incorpora mecanismes de control de flux per assegurar la integritat de les comunicacions entre ordinadors.

- NIVELL 2, Internet: Detalla els mètodes mitjançant els quals diferents xarxes intercanvien informació, assegurant el camí de transmissió de dades entre elles.

- NIVELL 1, Enllaç o capa física: especifica les tecnologies de connexió entre segments de la xarxa.

Quan dos programes de dos ordinadors diferents es connecten, estableixen una comunicació a nivell d'aplicació. El port permet identificar l'aplicació a la que es refereixen les dades. A nivell de transport, s'analitza la quantitat de dades a enviar, es fracciona en paquets més petits i s'afegeix una etiqueta identificativa a cadascun d'aquests. Això permet comprovar la integritat de les dades i proporciona un mecanisme per a que, tant el receptor com l'emissor, puguin identificar els errors que s'hagin pogut produir. A continuació, en el nivell d'Internet, el protocol IP afegeix a cada paquet les adreces de destí (xarxa i encaminador al qual es transmet) i d'origen (xarxa i encaminador des del qual es transmet). Els paquets viatgen per les xarxes d'encaminador a encaminador fins que un d'ells els fa arribar a l'equip al que estan destinats.

2.1.2 Open System Interconnection

El model Open System Interconnection (OSI), fou desenvolupat per la ISO, l'Organització Internacional per a l'Estandardització, i fou publicat el 1980 [7] i, posteriorment, sota la referència ISO/IEC 7498-1:1994 [8]. A diferència del model TCP/IP, utilitza set capes d'abstracció per a definir com s'han d'establir les comunicacions. El model OSI és una potent eina de representació i sovint s'utilitza en l'ensenyament del funcionament de les xarxes.

S'organitza en els següents nivells d'abstracció:

- CAPA 7, Aplicació: Especifica com poden les aplicacions intercanviar dades a través de la xarxa.

- CAPA 6, Presentació: Especifica la codificació i representació de les dades que s'intercanvien, compatibilitzant les comunicacions entre equips que emprin diferents tipus de codificació.

- CAPA 5, Sessió: S'encarrega de controlar i arbitrar l'estat de la transmissió entre els equips.

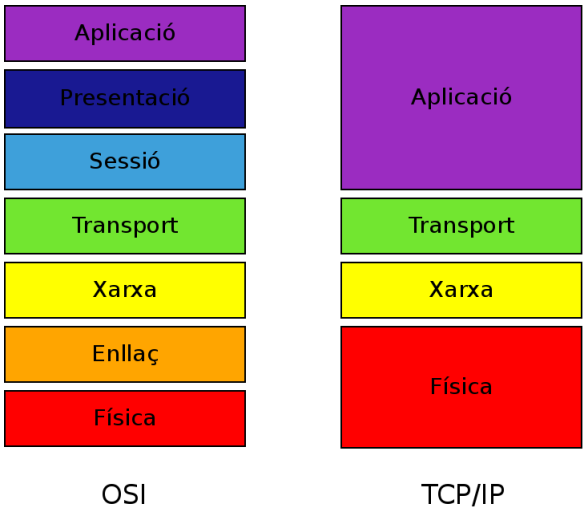

Figura 2.1: Comparació dels diferents nivells d'abstracció dels models OSI i TCP/IP.

- CAPA 4, Transport: Realitza la segmentació i seguiment del transport de les dades entre els equips. Defineix els protocols TCP i UDP.
- CAPA 3, Xarxa: S'encarrega d'encaminar les dades per les diferents xarxes que hi hagi entre els extrems de la comunicació.
- CAPA 2, Enllaç: Defineix com interactuen els equips d'una mateixa xarxa, també permet detectar errors i defineix la "trama", l'estructura de dades bàsica on s'empaqueta la informació rellevant per les altres capes. L'enllaç més habitual és l'*Ethernet*.
- CAPA 1, Capa física: Defineix el mitjà físic per on viatgen les dades i el tipus de senyal elèctric emprat per a la comunicació.

És habitual usar el model OSI per determinar el tipus d'equipament de xarxa. Així quan parlem d'equipament de Nivell 3 ens referim als equips que realitzen encaminament (encaminadors, estacions...), i amb equipament de Nivell 2 als que treballen amb adreces físiques dins una mateixa xarxa (commutadors, concentradors, estacions...).

En la Figura 2.1 podem veure una comparació gràfica entre les capes del model OSI, i les del TCP/IP. Es representa l'equivalència entre les funcions que prenen cada un dels nivells dels models.

2.2 Definició i elements d'una xarxa

Una xarxa informàtica, bàsicament, és un conjunt d'ordinadors connectats entre sí per tal de compartir informació i recursos. Segons la seva dimensió,

aquestes se solen classificar en PAN (xarxa d'àrea personal), LAN (xarxa d'àrea local), MAN (xarxa d'àrea metropolitana) o WAN (xarxa d'àrea extensa). Però normalment és suficient parlar només de dos tipus, que impliquen, a més a més, una certa idea de l'abast:

- LAN: Xarxa Local, normalment tots els equips d'aquesta conformen un entorn controlat. Per exemple, els equips d'una petita empresa, un departament d'una de gran, els d'una casa, etc..
- WAN: Xarxa informàtica que s'estén per una àrea molt gran. No és un entorn controlat i, per tant, es voldrà controlar quins recursos es comparteixen amb ella. L'exemple més conegut d'una xarxa WAN és Internet.

Així doncs, hi han xarxes molt senzilles i d'altres que poden abastar tot el món. Els elements d'una xarxa a nivell 3 són els següents:

- Estació: Un ordinador en concret que necessita ser representat pel fet de tenir alguna condició particular.
- Servidor: Una estació que ofereix un servei, és a dir, comparteix un recurs a la xarxa i, per tant, s'hauran de garantir les condicions necessàries per a que aquest recurs sigui accessible únicament pels equips autoritzats.
- Xarxes: Representen un conjunt indeterminat d'estacions i altres equipaments de xarxa de nivell 2 que permeten la interconnexió entre ells, com per exemple, commutadors (*switch*) i concentradors (*hub*). Se solen representar mitjançant un núvol, degut a la indeterminació del concepte que representen.
- Encaminador o *router*: Permet la interconnexió de dues xarxes, actuant de porta d'accés (*gateway*) per a cada una d'elles. Quan un equip d'una xarxa es vol comunicar amb el d'una altra, l'encaminador s'encarrega de fer de mitjancer en la comunicació, tot encaminant-la per la via més òptima. Se sol representar utilitzant una peça circular amb fletxes en la seva part superior, ressaltant la seva funció de redireccionament de les comunicacions.
- Tallafocs o *firewall*: Filtra la comunicació que passa a través seu i la bloqueja, o la permet, en funció de les regles que s'hagin establert. Pot ser un dispositiu dedicat o pot estar integrat en altres elements de nivell 3. Se sol representar usant un mur.

Els podem veure interconnectats en la figura 2.2, representant una xarxa molt bàsica formada, tan sols, per Internet, un encaminador i tres estacions.

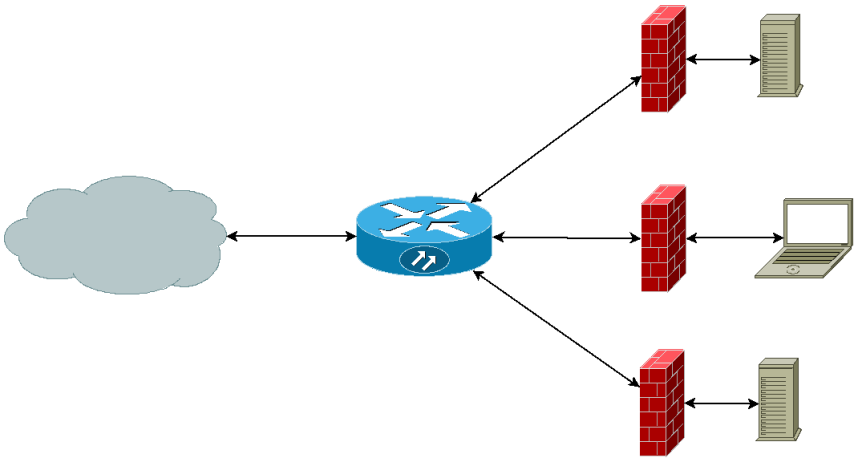

Figura 2.2: Esquema d'una xarxa bàsica

De vegades, en alguns esquemes pot aparèixer representat equipament de nivell 2, com punts d'accés sense fils. Però això es fa per especificar el disseny físic de la xarxa sense que tingui cap importància a nivell IP.

2.3 Seguretat

Un atac informàtic a través de la xarxa pot inutilitzar una xarxa empresarial i causar greus pèrdues econòmiques, o pot facilitar l'accés a informació de gran importància que pot ser usada per obtenir diversos avantatges competitius o fins i tot pot ser venuda en el mercat negre. D'altra banda, altres atacs poden tenir com a objectiu guanyar el control d'una màquina remota, simplement per poder utilitzar els seus recursos amb finalitats delictives. De fet, amb la informatització actual, cada cop és més atractiu realitzar atacs per tal de desestabilitzar les xarxes informàtiques que controlen la infraestructura de territoris o, fins i tot, països sencers que puguin ser considerats enemics, conformant el que es coneix com a guerra cibernètica.

Si bé és cert que no totes les xarxes tindran la mateixa susceptibilitat de ser atacades, la gran quantitat de motivacions que poden suscitar un atac fan que la importància de mantenir segures les comunicacions sigui cabdal.

Els principals riscos en una xarxa són la pèrdua de:

- la integritat de les dades,
- la confidencialitat,
- i la disponibilitat de recursos.

Els atacs més comuns són els següents:

- Virus, cavalls de Troia i *malware*: s'instal·len en el sistema remotament i duen a terme accions no desitjades que poden afectar el funcionament normal dels equips.
- Denegació de servei: Es demanen una gran quantitat de connexions simultànies, els recursos s'esgoten i el trànsit es col·lapsa.
- Pesca o *eavesdropping*: si no s'empra xifratge en les comunicacions, un tercer pot interceptar-les i llegir-les.
- Rastrejadors o sniffers: No només permeten la pesca, sinó que també es poden usar per estudiar el funcionament intern d'una xarxa per tal de trobar-hi forats de seguretat.
- Atacs de contrasenyes: Un atacant pot obtenir accés a contrasenyes d'usuaris vàlids i modificar la configuració de la xarxa per obrir forats de seguretat o per a inutilitzar-la.
- Atacs de man-in-the-middle: un atacant pot interceptar comunicació d'un sistema autoritzat i fer-se passar per ell o modificar el contingut de la comunicació.
- etc...

Degut a la gran diversitat dels atacs, mantenir la seguretat en una xarxa és una tasca costosa que s'ha d'obtenir a través de diferents mecanismes. Serà necessari establir mètodes criptogràfics per assegurar la confidencialitat i la integritat de les comunicacions, instal·lar antivirus per bloquejar les infeccions el més ràpidament possible, i configurar tallafocs per evitar els accessos per canals no controlats, entre d'altres mecanismes.

2.4 Tipus de tallafocs

Els tallafocs no poden ser l'únic mètode de protecció d'una xarxa però, sens dubte, són un element molt important. Els tallafocs han anat evolucionant amb el pas del temps, i és difícil fer-ne una classificació clara ja que poden ser jutjats de moltes maneres diferents. Segons les necessitats de la xarxa, serà més adient un tipus de tallafoc o bé un altre. Pot ser que el flux habitual de la xarxa sigui molt gran per a ser tractat amb un tallafocs de programari o que s'hagi d'utilitzar un equip dedicat enlloc d'un que realitzi vàries tasques. Hi ha encaminadors de gamma alta que poden incloure un tallafocs o la possibilitat d'instal·lar-hi un mòdul que realitzi aquella funció aprofitant la infraestructura del propi equip.

Tot i que s'han de tenir en compte molts aspectes a l'hora de triar un tallafocs: el cabal que poden filtrar, la rapidesa del filtratge... moltes vegades se solen classificar per coses tant simples com:

- el preu: el rang és sorprenent.
- la implementació: en maquinari o en programari.
- el cabal de dades: personals, departamentals o d'empresa.
- la generació/tecnologia: aquest podria ser el punt més rellevant ja que cada generació aporta diferents mètodes.

Generalment, els tallafocs implementats en maquinari solen ser més ràpids i acceptar molt més cabal que els de programari. Disposen de millors algoritmes i més capacitat, poden filtrar inspeccionant la capa de transport dels paquets de la comunicació controlant molts més detalls. Però caldrà balancejar les necessitats reals de la xarxa a l'hora de prendre una decisió. Pot ser que necessitem un tallafocs de maquinari en la porta d'accés per filtrar moltes transmissions si tenim un servidor web molt concorregut, i que alhora ens calgui un tallafocs de programari per assegurar dades sensibles de l'organització que només siguin accessibles pels equips de la xarxa local.

Les diferents generacions de tallafocs representen l'evolució tecnològica que han sofert al llarg dels anys:

- Primera generació: Empren la tecnologia de filtratge de paquets, s'inspeccionen els camps origen, destí, protocol, port, tipus de servei i altres elements de la capçalera IP. Generalment són ràpids i tenen escàs efecte negatiu en la càrrega de la xarxa. Però és possible introduir paquets prefabricats que falsegin aquesta capçalera.
- Segona generació: Tecnologia d'aplicació. Es denominen així ja que treballen en la capa d'aplicació del model OSI. Generalment reben les peticions d'equips externs i, si compleixen els requisits, efectuen la comunicació amb els equips interns transmetent-ne el resultat al sol·licitant. En actuar com a intermediaris entre els equips, afegeixen una capa de protecció important. Mantenen el desconeixement del funcionament intern de la xarxa, però acostumen a ser més lents i necessitar molta memòria per a recordar els estats de les diferents connexions. A més a més, han d'emmagatzemar informació relativa al tipus d'aplicació en concret que han de filtrar.
- Tercera generació: Tecnologia d'inspecció. S'inspecciona la informació de nivell de sessió. Aquesta sol incloure origen, destí, port, numero de seqüència, i alguna informació especifica de nivell d'aplicació. Poden incloure mètodes per inspeccionar les dades en busca de virus, verificar que sigui contingut http legítim... Són més ràpids que els de segona generació i no necessiten tanta memòria.

Tot i això, encara hi ha diferents capacitats que poden tenir els tallafocs de diferents generacions que poden ser el que realment els diferencïi d'un altre tallafoc en el nostre rang pressupostari i segons les necessitats.

Figura 2.3: Diferents models de firewall de CISCO

- Tallafocs *stateful*: Es pot establir regles en funció de l'estat de la connexió, és a dir, no només es pot tractar les comunicacions en funció de l'origen i els destí, sinó que també poden ser gestionades en funció de si les connexions són noves, establertes o relacionades amb alguna connexió anterior.
- NAT (Network Address Translation): Es pot realitzar traducció d'adreces assumint, de cara a l'exterior, un servei que desenvolupi un servidor intern. També pot ser usat per a compartir diverses connexions sortints però sempre en una relació d'un a un.
- PAT (Private Address Translation): Es pot realitzar una traducció de les adreces internes a una única adreça IP pública, això permet que, per exemple, un tallafocs assumeixi com a pròpies les peticions HTTP de diversos equips de la xarxa interna i, en rebre la resposta, la redirigeixi al equip intern sol·licitant. D'aquesta manera els, diferents equips de la xarxa local poden accedir a l'exterior compartint una sola adreça pública.
- etc...

2.5 Tipus de Control o Polítiques

Normalment, els tallafocs es poden configurar per acceptar dos tipus de control: el permissiu i el restrictiu. Aquests estableixen com es tracten per

defecte les connexions que filtren si no compleixen cap regla.

- Control permissiu: Per defecte, es permeten totes les connexions, exceptuant aquelles per les quals creem explícitament regles per rebutjarles.
- Control restrictiu: Per defecte, es prohibeixen totes les comunicacions, exceptuant aquelles per les quals creem explícitament regles per acceptar-les.

Generalment, el control restrictiu és més segur, ja que dificulta que deixem punts oberts per descuit però, en algun cas, pot ser més ràpid establir polítiques permissives i prohibir explícitament les que vinguin de les xarxes externes, o que arribin a través de la porta d'accés. Habitualment, es treballa en control restrictiu.

Capítol 3

Netfilter/Iptables

En aquest capítol es descriu el funcionament de *Netfilter*. També es descriu l'organització de les regles, cadenes i taules del sistema.

3.1 Introducció a Netfilter

Netfilter[12] és un sistema de gestió de les comunicacions a nivell de paquet de dades vinculat al nucli de Linux que permet la configuració del filtratge, manipulació i redireccionament de paquets. Permet especificar si una determinada comunicació és autoritzada i actuar en conseqüència bloquejant-la, transmetent-la, o bé, redirigint-la cap a un equip especific aplicant traducció d'adreces de xarxa (NAT). També pot alterar els camps de direcció per facilitar connexions que, d'altra manera, no es podrien dur a terme mitjançant l'emmascarament.

Iptables és l'eina d'usuari mitjançant la qual, l'administrador de la xarxa, pot configurar les regles que condicionaran les decisions que prendrà *Netfilter* amb les comunicacions, encara que sovint quan es parla d'*Iptables*, hom es refereix al conjunt de les eines que ofereix *Netfilter*.

Netfilter va ser desenvolupat a partir de 1998 i va ser inclòs en el nucli de Linux a partir de l'any 2000 en la versió 2.3 d'aquest nucli. Anteriorment, en Linux, s'havia usat *ipfwadm*, i *ipchains*, aplicacions que realitzaven les tasques de filtratge, però amb *Netfilter* s'introduïa un espai de treball dedicat exclusivament al tractament d'aquest aspecte. Una de les principals novetats, obviant les referents a la implementació, respecte als anteriors sistemes de gestió de les comunicacions de *Linux* va ser millorar la funcionalitat, afegint el filtratge en funció de l'estat de la connexió al sistema.

Com tot tallafocs, en *Iptables* s'utilitza una sèrie de regles que, si van dirigides al paquet que s'està avaluant, estableixen com continuar el processament d'aquest. Aquestes regles estan agrupades en cadenes i taules. Les taules representen un tipus d'operació: filtrat, redireccionament o manipulació. Cada taula conté una sèrie de cadenes.

3.2 Regles i Cadenes

Una regla especifica quina acció ha de prendre el sistema si un determinat paquet compleix les condicions d'origen, destí, tipus de servei i estat de la connexió definides, cosa que es coneix com a fer *matching*. Les cadenes són un conjunt de regles que s'han de comprovar seqüencialment cada cop que un paquet entra al sistema. Quina de les cadenes s'ha de recórrer dependrà del sentit de la comunicació.

Quan un paquet entra al sistema es recorre la cadena associada i, tan bon punt fa *matching* amb una regla, abandona el recorregut i es duu a terme l'acció que aquesta regla estableix. Si, per altra banda, no es troba cap regla que es refereixi a aquest paquet en arribar al final de la cadena, es durà a terme l'acció especificada en les polítiques per defecte. Per això, l'ordre en que afegim les regles a cada cadena és molt important. Si afegim primer les regles d'una xarxa en una cadena i llavors afegim les d'una subxarxa especifica d'aquesta, els paquets, en fer *matching* amb les condicions de la xarxa principal, no seran tractats correctament.

3.2.1 Tipus d'Accions

Les accions, també anomenades *targets*, més habituals que es poden definir en les regles són:

- ACCEPT: el paquet és autoritzat per a realitzar el seu processament.
- DROP: el paquet és descartat.
- REJECT: el paquet es descarta i es retorna un missatge d'error per notificar a l'equip emissor que la comunicació no es pot realitzar.

A banda d'aquestes, hi ha accions que serveixen per desar un registre (LOG), per modificar el paquet (NAT, MASQUERADE...), per redirigir-lo a una cadena d'usuari, etc...

3.3 Taules

Iptables, per defecte, té tres tipus de taules, *Filter*, *NAT* i *Mangle*, tot i que se'n poden afegir més si és necessari. Serveixen per agrupar les cadenes segons les principals funcions que duen a terme:

- FILTER: Tots els paquets que passen per la màquina han de travessar aquesta taula, doncs estableix les regles mitjançant les quals es pot decidir si descartar o acceptar el paquet. Per defecte, conté tres cadenes:
  - INPUT: s'aplica als paquets que van dirigits a la mateixa màquina.

  - OUTPUT: s'aplica als paquets que tenen com origen la màquina i que són enviats a l'exterior.
  - FORWARD: s'aplica als paquets que tan sols passen a través d'aquesta màquina per poder arribar a altres màquines.

- NAT: Serveix per establir com i quan es tradueixen les adreces i els ports de les connexions. El primer paquet de cada connexió passa per aquesta taula establint com s'ha de dur a terme la traducció durant tota la connexió. Donat que per l'encaminament a nivell 3 es fa la mateixa modificació d'adreces, s'ha de tenir en compte que les modificacions s'han de realitzar abans o després que aquest encaminament es dugui a terme, en funció de si són paquets d'entrada o de sortida, respectivament. Per exemple, en un equip que enllaça l'adreça pública de la porta d'accés a Internet amb el servidor de correu de la xarxa local. En donar un servei als equips d'Internet, tant aquests com el servidor local, l'única adreça que coneixen en comú, si no tenen definida una ruta d'encaminament, és la de la porta d'accés; per això, aquesta ha d'introduir la seva adreça local com a origen, en contactar cap al servidor, i en el destí, en els paquets que vagin del servidor cap a l'equipament extern.

  També conté, per defecte, tres tipus de cadenes:

  - PREROUTING: Els paquets entrants passen primer per aquesta taula abans de decidir l'encaminament modificant el camp origen dels mateixos.
  - POSTROUTING: Els paquets sortints passen per aquesta taula després que es decideixi l'encaminament del paquet. Normalment es porta un registre de les traduccions que s'han fet en entrada per tal de saber quina adreça s'ha de ficar en la destinació.
  - OUTPUT: Els paquets sortints de la pròpia màquina passen per aquesta cadena.

- MANGLE: Aquesta taula serveix per realitzar modificacions avançades en els paquets, no només d'origen i destí, sinó també d'aspectes que afectin el servei de transport. Per això, aquesta taula és la que s'avalua abans que cap altra. Inclou cinc cadenes que es corresponen amb els tipus de cadenes ja esmentats en les altres taules: INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING.

En la Figura 3.1 es descriu el flux dels paquets en arribar a una màquina amb *Iptables*, mostrant les cadenes per les quals han de passar.

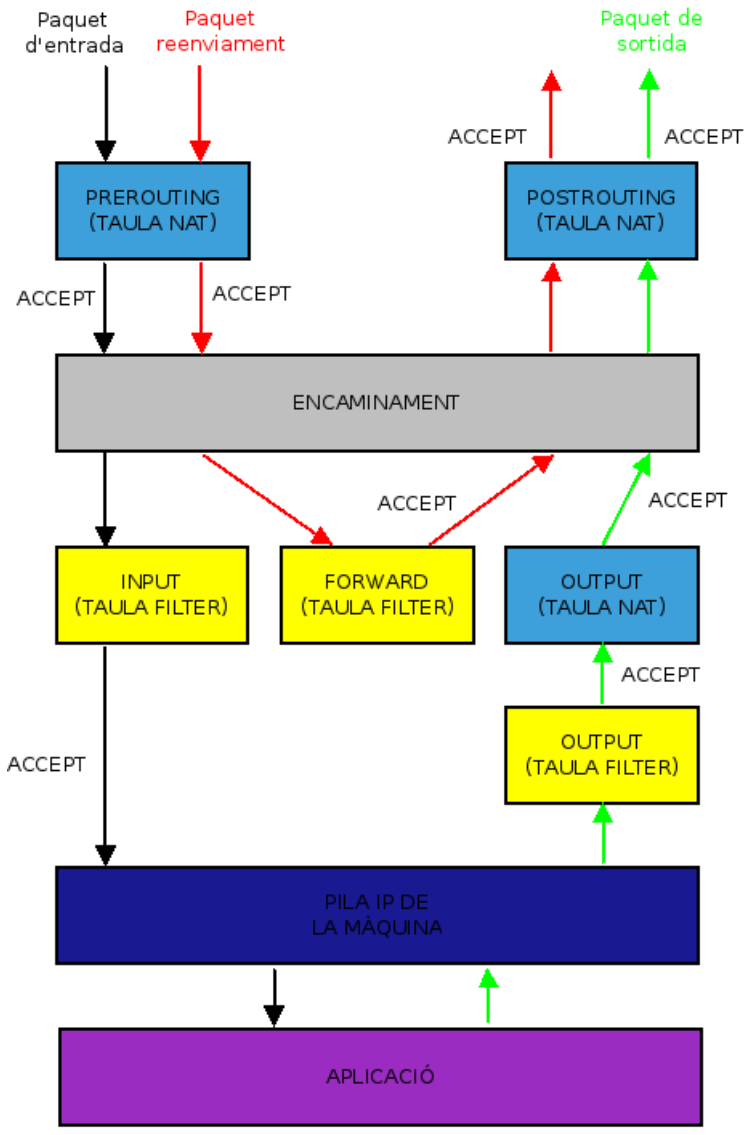

Figura 3.1: Exemple del flux de diferents paquets amb *Netfilter*

3.4 Sintaxi d'Iptables

Amb la comanda de Linux *iptables* es poden afegir, esborrar o modificar regles utilitzant IPv4. Per treballar amb IPv6 cal utilitzar *ip6tables*. A continuació, s'inclouen alguns exemples de comandes d'*iptables* per donar una idea bàsica de la sintaxi d'aquestes.

- **Adjuntar una regla**

  Les regles es poden inserir o adjuntar. En inserir-les podem indicar quina posició en la cadena ocupen, pel que s'acostuma a usar en modificacions puntuals o correccions. En adjuntar s'afegeixen sempre al final de la cadena. Per aquest motiu, en *scripts* se sol usar l'adjunció.

  L'ordre "`iptables -A FORWARD -s 192.168.1.2/24 -m state stablished, related -d 192.168.2.2/24 -p tcp --dport 23 -j ACCEPT`" adjunta una regla en la cadena FORWARD.

  Els arguments especifiquen les condicions de filtratge, en l'exemple apareixen els següents:

  1. Origen (-s), especifica l'adreça IP de l'origen.
  2. *Match* (-m), estableix condicions específiques de filtratge, en l'exemple s'usa per seleccionar els paquets que formin part d'una connexió establerta o relacionada.
  3. Destí (-d), especifica l'adreça IP del destí.
  4. Protocol (-p), selecciona els paquets d'un determinat protocol de transport.
  5. Port de destinació (–dport), defineix el port de destí.
  6. Acció (-j), quina acció s'ha de dur a terme quan un paquet compleixi totes les condicions anteriors.

- **Establir les polítiques per defecte.**

  El tipus de control s'estableix individualment per cada cadena.

  La comanda "`iptables -P INPUT DROP`" estableix la política per defecte de la cadena INPUT com a restrictiva.

  La comanda "`iptables -P OUTPUT ACCEPT`" estableix la política per defecte de la cadena OUTPUT com a permissiva.

- **Esborrar les regles.**

  Es poden esborrar totes les regles, totes les d'una taula i totes les d'una cadena.

  La comanda "`iptables -F`" esborra totes les regles.

La comanda "`iptables -F -t filter` esborra totes les regles de la taula *filter*.

La comanda "`iptables -F INPUT` elimina totes les regles de la cadena *INPUT*.

Capítol 4

Eina visual per a configurar Iptables

En aquest capítol es descriu el funcionament de l'eina desenvolupada i es detallen les parts que la composen. Les diferents seccions conformen, a més a més, un manual d'ús.

4.1 Visió general del disseny

En desenvolupar l'eina es cercava una manera senzilla d'editar diferents esquemes de xarxa, dotant-la d'una certa capacitat de comprensió, que permet la identificació dels elements implicats en les diferents comunicacions que s'hi poden realitzar. Així, si es defineix una regla entre A i B, aquesta es capaç d'identificar els tallafocs que es troben en el camí i establir-ne la configuració, de manera que aquest permeti la transmissió de les dades.

D'aquesta manera, es pot generar un script de configuració amb totes les regles que s'han de configurar en els tallafocs implicats, suposant que aquests fossin implementats mitjançant *iptables*.

Es pressuposa un ús de polítiques restrictives en tots els punts de la xarxa, ja que és la política generalment més adient.

4.1.1 Finestra principal

La part més important de la finestra principal (figura 4.1) és l'àrea de disseny. Al principi sempre disposem d'una figura representant Internet a la que podem connectar portes d'accés de les nostres xarxes o fins i tot un equip remot que hagi de tenir un accés particular a la xarxa, com per exemple, accés per *ssh* als servidors, connexions d'escriptori remot per a *helpdesk*...

En la barra de menús de la finestra principal trobarem els següents components:

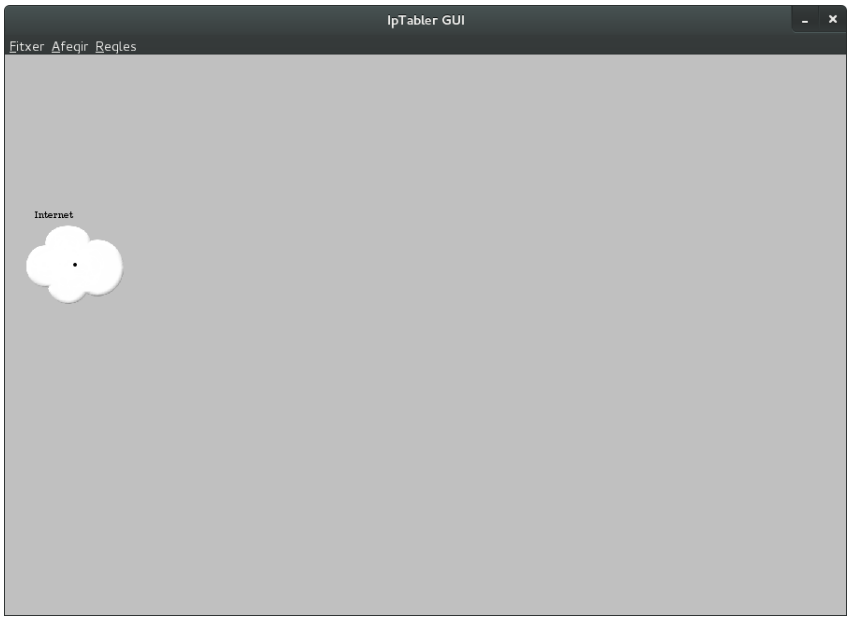

Figura 4.1: Finestra principal de l'eina

- El menú "fitxer", on disposem de les ordres bàsiques per tornar a començar de nou, desar o carregar l'esquema i sortir.
- El menú "afegir", des del que podem seleccionar el tipus de figura que es vulgui afegir i començar l'edició, de la qual en parlarem més endavant.
- El menú "regles", des del qual es poden consultar la llista de ports i la de regles que tenim definides en el projecte. Per defecte, es carrega una sèrie de ports, però se'n pot afegir de nous. La llista de regles és buida i, per tant, les condicions de seguretat de la xarxa dependran de les necessitats de l'usuari.

4.1.2 Elements de l'esquema de xarxa

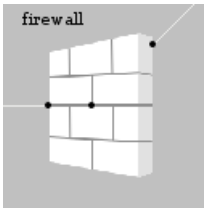

Figura 4.2: Un tallafocs representat en l'àrea de disseny

En l'àrea de disseny, els diferents elements de la xarxa es representen per un dibuix identificatiu i s'indica amb un punt les seves interfícies, tal i com es pot veure en la figura 4.2. Si les interfícies estan connectades a un altre element, aquestes, apareixeran a la vora de la figura i estaran unides per una línia amb l'altre element. En cas que l'element disposi d'interfícies lliures es representarà amb un punt al centre de la figura.

En ser seleccionats, els elements es poden arrossegar a la posició desitjada de l'àrea de disseny, encara que, si està ocupada, es posicionarà en la zona lliure més propera.

En l'esquema de xarxa podran aparèixer xarxes, encaminadors, tallafocs, estacions de treball i servidors, però en funció de l'element hi podrem connectar uns o altres. Per exemple, no podrem connectar dues xarxes sense enllaçar-les a través d'un element capaç d'encaminar entre elles, com un encaminador o un tallafocs.

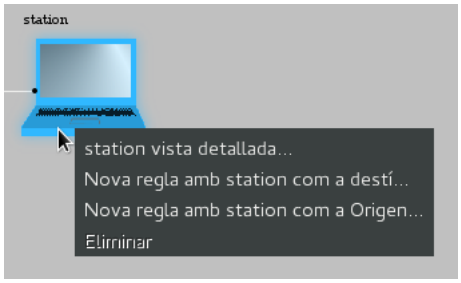

Figura 4.3: El menú contextual dels elements de xarxa

En fer clic amb el botó dret del ratolí desplegarem el menú contextual de l'element (Figura 4.3) que ens permetrà obrir una vista detallada amb les principals propietats de l'element, afegir-lo com a destí o origen de la regla que estem definint o eliminar-lo de l'esquema.

En la finestra de la vista detallada (Figura 4.4) se'ns descriurà diferents aspectes de l'element seleccionat. Les diferents seccions d'aquesta dependran del tipus d'element, però generalment hi apareixerà:

- Detall de les interfícies: Una vista detallada de cada interfície de l'element.

- Propietats de la xarxa: (només en elements de xarxa) On es mostra la IP i la màscara de xarxa i podem editar-les per ajustar-nos a les necessitats.

- Clients de la xarxa: (només en elements de xarxa) Ens mostra les adreces IP de les interfícies connectades a la xarxa, s'actualitzen en canviar les propietats de la xarxa.

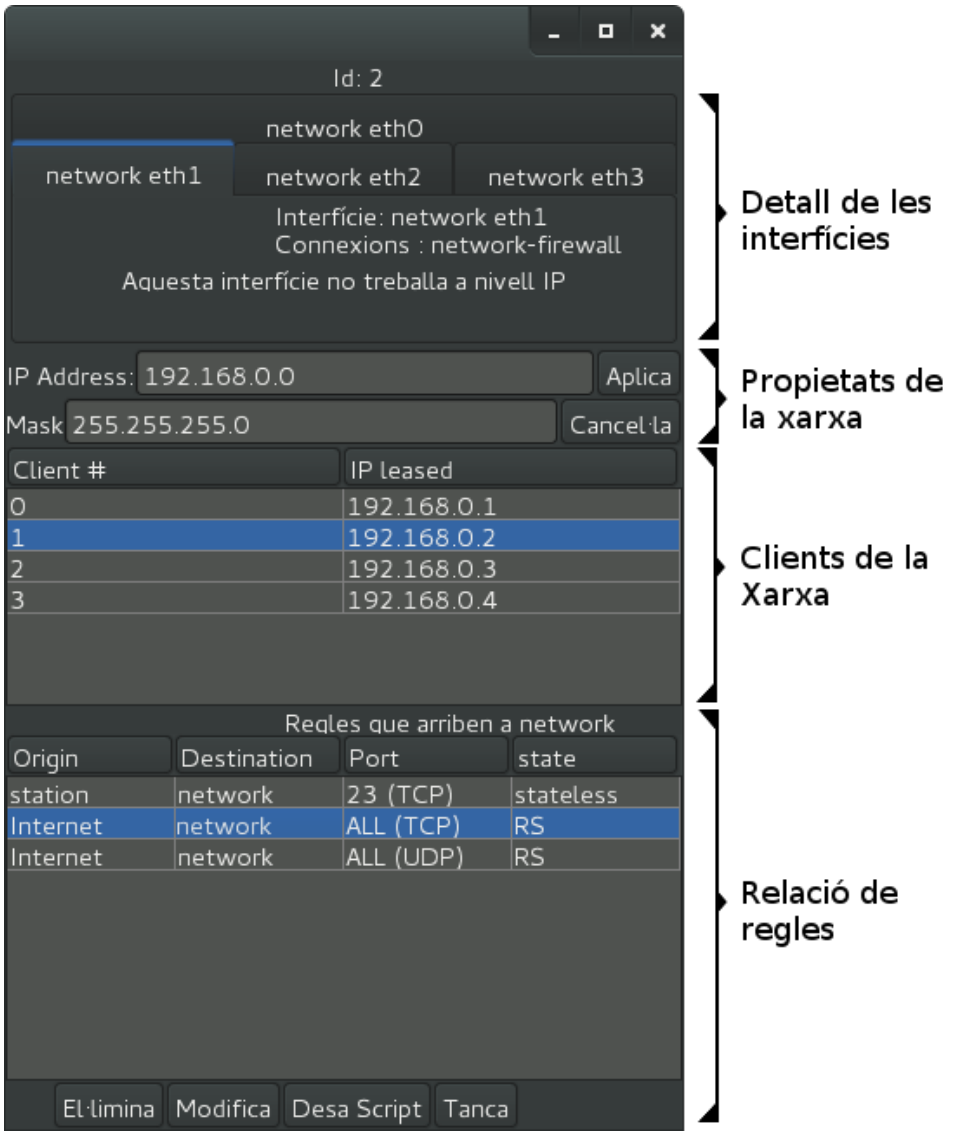

Figura 4.4: Visió detallada d'una xarxa

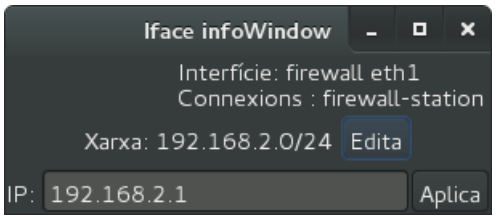

Figura 4.5: Finestra d'informació d'una interfície

Figura 4.6: Menú contextual d'una interfície

- Relació de regles: Es mostren les regles que afecten a l'element, és a dir, les que s'han d'escriure en l'*script* de configuració de l'element. Només apareix en estacions de treball, servidors, xarxes i tallafocs. En estacions i servidors s'inclouen també les regles heretades de la xarxa a la qual pertanyen. També apareixen els botons per eliminar una de les regles, desar l'*script* i tancar la finestra.

4.1.3 Interfícies

En fer clic amb el botó dret del ratolí en una interfície, ens mostra el menú contextual de la interfície, com es mostra en la Figura 4.6. Aquest ens permetrà afegir noves figures connectades a la interfície (quan sigui possible), editar la xarxa implícita en aquelles interfícies que ho requereixen i veure'n les propietats que es mostraran en una breu finestra d'informació (Figura 4.5) amb els connectors, l'adreça IP assignada (si en necessita) i un accés directe a les propietats de la xarxa a que pertany.

4.1.4 Afegir elements a l'esquema de xarxa

Per afegir elements a l'àrea de disseny, i com que no tots els elements accepten les mateixes connexions, es disposa de dos mecanismes per fer-ho: a través del menú "Afegir", o bé, a través del menú contextual de les interfícies que estiguin lliures.

Afegir elements mitjançant el menú Afegir

En seleccionar un tipus de figura en el menú, les interfícies de l'esquema a les que es pugui connectar una figura del tipus seleccionat es ressaltaran en color groc, i en passar el ratolí per sobre d'una d'elles es ressaltarà en verd, com es veu en la Figura 4.7. Fent clic en una d'aquestes interfícies afegirem la figura.

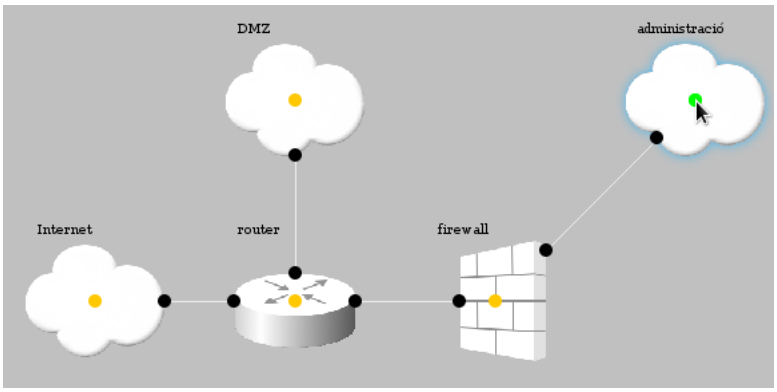

Figura 4.7: Afegint una estació de treball des del menú "Afegir"

Afegir elements a través del menú contextual de les interfícies

Com es pot veure en la Figura 4.8, mitjançant el menú contextual de la interfície es mostraran els tipus d'elements que hi poden ser connectats i, clicant en el tipus que ens interessi, s'afegirà en una zona lliure propera.

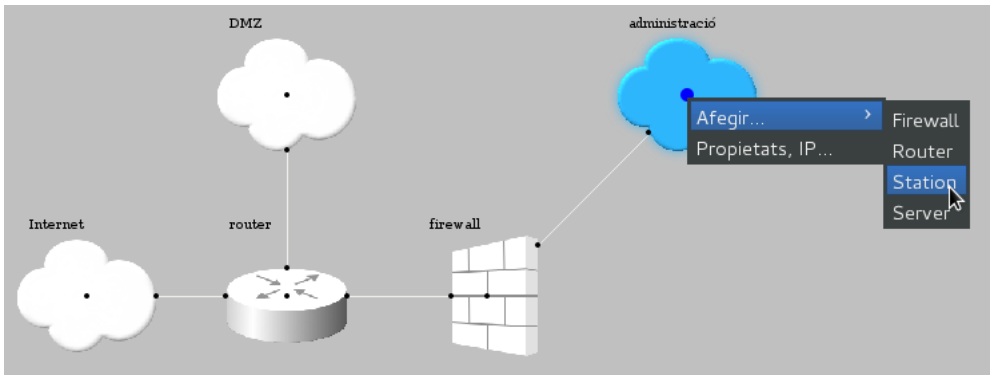

Figura 4.8: Afegint una estació de treball a través del menú contextual

4.1.5 Ports

L'eina treballa amb ports TCP i UDP, que han d'estar carregats prèviament en la llista de ports de l'aplicació. Per accedir a aquesta llista s'ha de

seleccionar l'opció "Mostrar ports" en el menú "regles" de la barra de menús de la finestra principal.

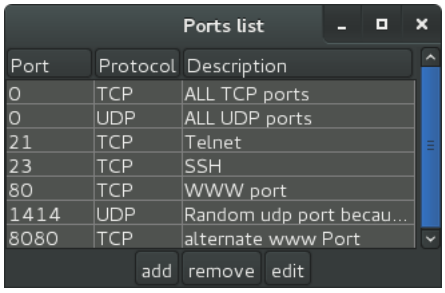

Figura 4.9: Llista de ports

En la llista de ports (Figura 4.9), veurem els ports afegits, que estaran disponibles a l'hora de definir regles. Des d'aquesta finestra es pot afegir, eliminar i modificar qualsevol dels ports existents.

4.1.6 Regles

Creació de regles

En l'eina es poden definir regles filtrant pels protocols TCP i UDP, així com l'adreça de destí, la d'origen i l'estat de la connexió. En afegir una regla, es calcula la trajectòria que hi ha entre l'origen i el destí i s'identifiquen quins tallafocs hi estan implicats.

Per afegir una nova regla haurem de seguir els següents passos:

1. Seleccionar origen i destí. Des del menú contextual de les figures podem definir la figura seleccionada com a origen o com a destí de la nova regla. No importa l'ordre en el que ho fem, un cop seleccionat un extrem de la connexió només podrem seleccionar l'altre, o bé, cancel·lar la creació de la regla des de la barra de menús de regles, seleccionant l'opció "Cancel·la creació de regla". En les figures 4.10 i 4.11 es mostra com seleccionem com a origen i destí, una estació de treball i un servidor respectivament.

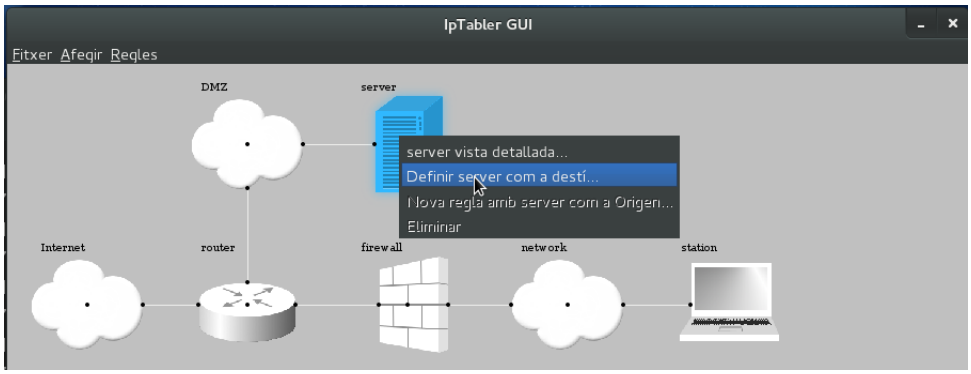

Figura 4.11: Definint un servidor com a destinació de la regla

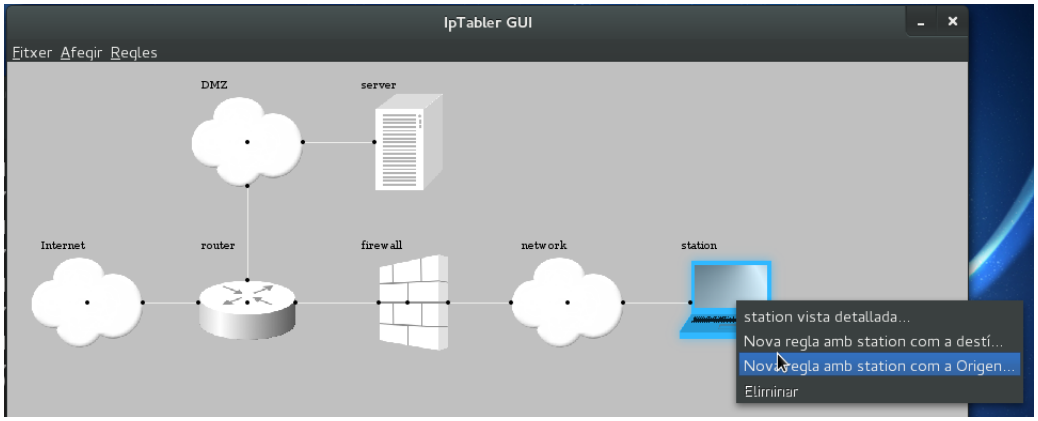

Figura 4.10: Definint una estació de treball com a origen de la regla

2. Seleccionar el port i l'estat de la connexió. Un cop haguem definit els extrems del camí de la regla, apareixerà la finestra de selecció de port, Figura 4.12, on podrem seleccionar el port, d'entre els que haguem afegit, i l'estat de la connexió. En acceptar, la regla s'haurà afegit al projecte.

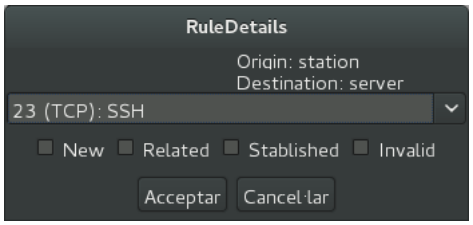

Figura 4.12: Definint els detalls d'una nova regla

Figura 4.14: Vista detallada del servidor amb les regles que l'afecten

Vista general de les regles

Podrem consultar les regles definides sobre l'esquema en que treballem seleccionant l'opció "mostrar regles" del menú de regles de la barra de menús. En la Figura 4.13 es mostra la llista de regles de l'exemple anterior.

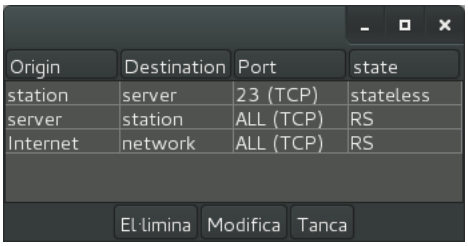

Figura 4.13: Llista de regles

Vista de les regles per figures i creació de l'script de configuració

En canvi, si volem veure les regles que s'aplicaran a cada equip haurem de consultar les vistes detallades de les figures. En les figures 4.14 i 4.15 es mostren les vistes detallades del destí, un servidor, i del tallafocs implicat.

Des d'aquestes vistes detallades podrem generar els scripts de configuració de cada figura, prement el botó "Desa Script" se'ns demanarà el directori de sortida on es desarà un script anomenat "setIptables_ <nom

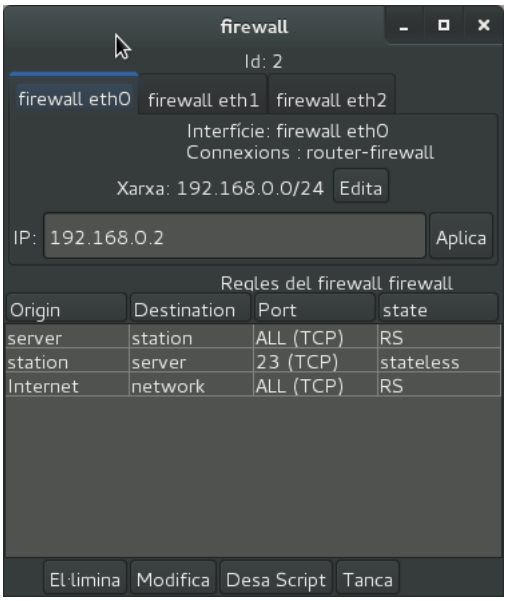

Figura 4.15: Vista detallada del tallafocs implicat en la connexió

de la figura>.sh". En la Figura 4.16 es mostra l'script de configuració de l'exemple anterior.

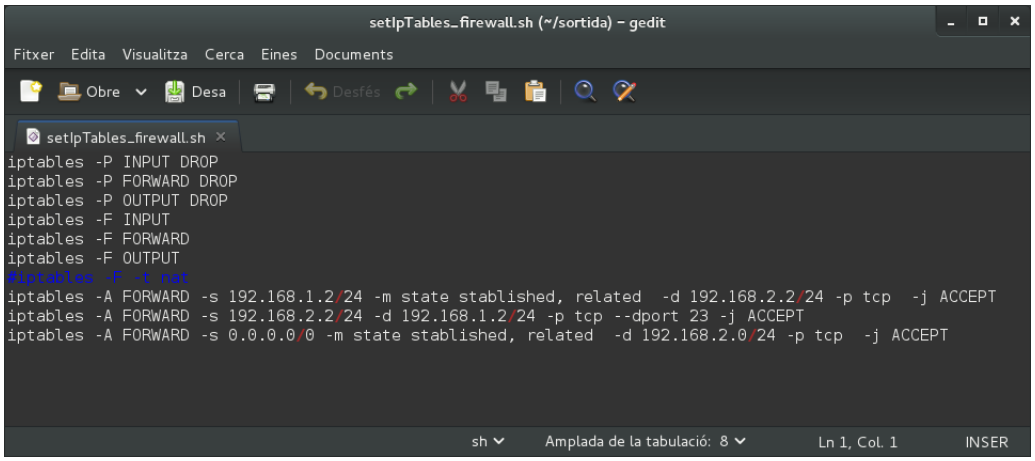

Figura 4.16: Script de configuració generat per l'eina amb les regles de l'exemple

4.2 Tecnologies emprades

L'eina s'implementa en llenguatge *Java*[9]. En un principi, aquesta decisió va venir motivada per les facilitats d'ús i portabilitat que ofereix aquest

llenguatge. *Java* és un llenguatge orientat a objectes que disposa d'una base molt àmplia de llibreries lliures, pel que ofereix una molt bona versatilitat i reutilització de codi.

Per la representació gràfica s'empra la llibreria *swing*, inclosa en les llibreries estàndard de *Java*. Aquesta permet la creació d'aplicacions amb interfície gràfica multi-plataforma d'una manera molt ràpida.

També s'utilitza la llibreria lliure *opencsv*[10], que facilita el treball amb arxius de valors separats per comes.

Per fer el càlcul del posicionament de les interfícies s'utilitza una implementació de la classe *lineIterator*, que inclou la funció de l'algorisme de Bresenham per recórrer els punts d'una recta. La funció s'adapta per a poder acceptar diferents nivells de precisió. La classe va ser publicada pel seu autor, *nikoschwarz*, en la plataforma de distribució de *snippets* (petits fragments de codi): snipt.net.

El treball fou desenvolupat amb la versió 13 de la comunitat de l'entorn intelliJ IDEA.

Capítol 5

Conclusions i treball futur

En aquest capítol es recullen una sèrie de reflexions finals i una proposta de millores que es podrien afegir en un possible treball futur.

5.1 Conclusions

La seguretat en la xarxa té una importància cabdal degut a la creixent informatització que fa que cada cop compartim més informació sensible amb tercers. Els tallafocs tan sols són una de les moltes baules que ens ajudaran a mantenir aquesta seguretat.

Tot i els avantatges, o desavantatges, del diferents tipus de tallafocs, a l'hora d'escollir-ne un, haurem de tenir molt en compte les necessitats de la xarxa ja que per aconseguir un disseny eficient i assequible és possible que ens calgui combinar diferents tecnologies.

Netfilter/Iptables és una solució de seguretat lliure i molt completa, les funcionalitats de la qual s'han explotat a un nivell molt bàsic en aquest projecte. Tot i això, les creixents necessitats fan que el desenvolupament de les eines de seguretat de Linux continuïn evolucionant i ja se'n prepara una nova evolució.

Tot i que *Java* és un llenguatge prou accessible i que la gran quantitat de llibreries disponibles agilitzen molt el desenvolupament, de vegades, les interrelacions entre aquestes llibreries són difícils de dominar. Explotar correctament la multitud de llibreries representa, potser, un dels majors reptes a l'hora d'aprendre i desenvolupar eficientment aplicacions amb aquest llenguatge. Per pal·liar aquesta dificultat existeix, per sort, molta documentació [11].

5.2 Treball futur

- Explotar més les capacitats de l'*Iptables*, implementar mètodes per configurar NAT i regles per al protocol *icmp*.

- Millorar la usabilitat. L'actual disseny de la interfície, de vegades resulta incòmode, una reagrupació de les finestres d'informació i vista detallada en un panell lateral podria resultar més còmode. Altrament, una barra d'eines resultaria atractiva visualment.

- Facilitat d'ús. En afegir una regla proposar la reciproca, per exemple, si afegim accés HTTP de A a B amb estat *related* i *stablished*, tenir l'opció d'afegir automàticament la regla de B a A amb estat *new* sobretot si es dóna el cas que existeixin tallafocs entre A i B.

- Millores en la representació gràfica/reimplementació. En la implementació actual els elements de la xarxa són components gràfics de la llibreria *swing* de *Java*. Això facilita la implementació del dibuixat però, degut al tractament d'events que fa *swing* es produeixen errors de sincronia en algunes operacions, com l'eliminació en cascada.

- Simular camins en encaminadors. Aquesta particularitat facilitaria la creació de xarxes més complexes podent, per exemple, capacitar el programa per augmentar les interfícies dels servidors i connectar-los a més d'una xarxa per a fer balanceig de càrrega, o bé, per protecció complementària contra atacs DOS.

- Sincronització de vistes detallades. Les finestres de vistes detallades són asíncrones, pel que si, per exemple, obrim la vista d'una interfície amb connectivitat IP, i des de la vista de la xarxa que la conté canviem l'adreça de xarxa, aquest canvi no es veu reflectit en la primera finestra fins que la tornem a obrir. Això és corregible implementant un sistema d'events que alerti les finestres dels canvis però per raons de temps no s'afegeix la funcionalitat.

Bibliografia

[1] Estadístiques mundials d'Internet http://www.internetworldstats.com/stats.htm.

[2] Especificació del model TCP/IP http://tools.ietf.org/html/rfc1122.

[3] Notícia del Washington Post sobre el Morris Worm

[4] Code of Morris' worm http://www.foo.be/docs-free/morris-worm/worm/

[5] L'algorisme de Bresenham - Departament de ciencies de la computació de la Universitat de Helsinki http://www.cs.helsinki.fi/group/goa/mallinnus/lines/bresenh.html

[6] NetWorkWorld types of firewalls http://www.networkworld.com/article/2255950/lan-wan/chapter-1--types-of-firewalls.html

[7] Zimmermann, Hubert (April 1980). "OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection". IEEE Transactions on Communications 28 (4): 425–432.

[8] Standard ISO/IEC 7498-1:1994 http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip

[9] Pàgina web de Java http://www.oracle.com/es/technologies/java/overview/index.html

[10] Pàgina de la llibreria opencsv http://opencsv.sourceforge.net

[11] Documentació de Java http://docs.oracle.com/javase/7/docs/api/

[12] Pàgina web del projecte Netfilter http://www.netfilter.org/