Sistemes tallafoc

Guillermo Navarro Arribas

PID_00191679

Universitat Oberta de Catalunya

Índex

Introducció

Avui dia, un dels components més importants que ens trobem quant a la seguretat en xarxes informàtiques són els sistemes tallafoc. El seu ús s'ha estès a tot tipus de xarxes i fins i tot als ordinadors personals. Un tallafoc proporciona un mecanisme molt important de control d'accés a la xarxa, mitjançant el filtratge de paquets. L'objectiu principal d'un tallafoc és servir de barrera entre un entorn protegit i un entorn hostil. L'entorn protegit sol ser una xarxa interna d'una organització (generalment privada) o un conjunt d'equips informàtics, i l'entorn hostil solen ser xarxes públiques, com Internet.

Cheswick, Bellovin i Rubin, en el seu influent llibre *Firewalls and Internet Security. Repelling the Wily Hacker*, fan una llista de diverses màximes sobre la seguretat informàtica, les quals reproduïm a continuació:

"La seguretat absoluta no existeix".
"La seguretat és sempre una qüestió econòmica".
"Mantingueu totes les vostres defenses al mateix nivell".
"Un atacant no travessa la seguretat, la rodeja".
"Poseu les vostres defenses en capes".
"No és bona idea confiar en la «seguretat per foscor»".
"Heu de conservar la simplicitat".
"No doneu a cap persona o programa més privilegis que els estrictament necessaris".
"La programació és difícil".
"La seguretat hauria de ser una part integral dels dissenys originals".
"Si no executeu un programa, no importa si té errors de seguretat".
"Un programa o protocol és insegur fins que no es demostri el contrari".
"Una cadena és tan forta com el seu enllaç més feble".
"La seguretat comporta un compromís amb la comoditat".
"No subestimeu el valor dels vostres recursos".

Creiem que aquestes són una bona introducció a la seguretat informàtica i, més concretament, al tema que tractem en aquest mòdul. Moltes d'aquestes frases es consideren principis fonamentals de la seguretat informàtica, en general, i del disseny i configuració de sistemes tallafoc en particular.

En aquest mòdul presentem una introducció als sistemes tallafoc. La nostra intenció és oferir un material inicial que us serveixi per iniciar-vos en el tema i que us permeti endinsar-vos pel vostre compte en el complex món dels tallafocs. Aquest mòdul assumeix que teniu coneixements bàsics del funcionament de les xarxes d'ordinadors i certes nocions de seguretat en les xarxes. Més precisament, i encara que sense necessitat de coneixements exhaustius, sí que considerem que esteu familiaritzats amb la família de protocols TCP/IP.

En aquest mòdul repassem què és un sistema tallafoc. Veurem quins tipus n'hi ha i revisarem les arquitectures més utilitzades avui dia. Dediquem també un apartat introductori al filtratge de paquets, amb exemples de configuracions típiques. Finalment repassem alguns aspectes relacionats amb els tallafocs que us poden ser d'interès.

Objectius

Els objectius que es persegueixen amb l'estudi dels materials d'aquest mòdul són els següents:

1. Conèixer què és un sistema tallafoc i com es pot utilitzar per proporcionar seguretat a una xarxa informàtica.
2. Conèixer i entendre estratègies i arquitectures diferents de tallafocs per a la protecció de xarxes d'ordinadors.
3. Comprendre les polítiques de seguretat i el funcionament del filtratge de paquets en els sistemes tallafoc.

1. Sistemes tallafoc

Els **sistemes tallafoc*** són components de maquinari o programari que controlen el trànsit d'entrada i sortida d'una xarxa. D'aquesta manera, proporcionen un mecanisme de control d'accés sobre la capa de xarxa, que permet, per exemple, separar la nostra xarxa (on els equips que hi intervenen són de confiança) dels equips situats en xarxes de l'exterior (potencialment hostils).

*** En anglès, els sistemes tallafoc s'anomenen *firewall*.**

Un **tallafoc** és un sistema de xarxa encarregat de separar xarxes informàtiques, en controlar el trànsit que transcorre entre aquestes. Aquest control consisteix, en última instància, a permetre o denegar el pas de la comunicació d'una xarxa a una altra mitjançant el control dels protocols de xarxa.

Un tallafoc serveix de barrera en una xarxa, pot bloquejar el trànsit d'entrada o sortida, prevenir accessos no autoritzats i, en general, permet implementar la política de seguretat del sistema. En aquest context, el concepte de *política de seguretat* és important.

Una **política de seguretat** és el conjunt de regles i pràctiques que defineixen i regulen els serveis de seguretat d'una organització o sistema amb el propòsit de protegir els seus recursos crítics i sensibles. En altres paraules, és la declaració del que està permès fer i el que no ho està.

La política de seguretat és la base de la seguretat d'un sistema. S'hi detallen els serveis de seguretat del sistema, es determina què es pot fer o no amb els recursos del sistema, i qui ho pot fer, i generalment s'especifica com s'implementen aquests serveis. La implementació concreta d'una política de seguretat es porta a terme mitjançant **mecanismes de seguretat**. La política no ha de ser per força una declaració formal; de vegades es tracta de simples directrius sobre la seguretat del sistema en llenguatge informal.

En aquest sentit, un tallafoc és un mecanisme de seguretat que permet implementar les regles de la política de seguretat relatives al control d'accés en el nivell de xarxa.

A l'hora d'instal·lar i configurar un sistema tallafoc en una xarxa, hem de tenir present el següent:

1) Tot el trànsit que surt o entra a la xarxa ha de passar pel tallafoc. Això es pot aconseguir bloquejant físicament tot accés a l'interior de la xarxa a través del sistema.

2) Només el trànsit autoritzat, definit en les polítiques de seguretat locals del sistema, podrà traspassar el bloqueig.

3) El tallafoc mateix ha d'estar protegit contra possibles atacs o intrusions.

Els tallafocs, com els coneixem en l'actualitat, van aparèixer a final dels vuitanta, desenvolupats per les empreses DEC i AT&T, i el 1991 va aparèixer el primer tallafoc comercial, el DEC SEAL. Actualment els tallafocs són un element molt important no solament en dispositius de xarxa, sinó fins i tot en ordinadors personals. Hi ha diferents tecnologies per a implementar tallafocs i, sobretot, hi ha moltes arquitectures o maneres de configurar tallafocs en una xarxa. En aquest mòdul en veurem algunes de les més destacades. És important assenyalar que ens centrarem en l'ús de tallafocs en xarxes TCP/IP, tot i que l'ús de tallafocs no és exclusiu d'aquests protocols concrets.

Lectures complementàries

L'article següent (disponible en línia) comenta els orígens dels sistemes tallafoc:
F. Avolio (1999). "Firewalls and Internet Security, the Second Hundred (Internet) Years". *The Internet Protocol Journal* (vol. 2, núm. 2).

Així mateix, és important tenir sempre present què es vol obtenir amb un sistema tallafoc. L'ús més comú és el dirigit a controlar el trànsit d'entrada i sortida d'una xarxa a una altra. Generalment, es tracta de protegir la xarxa interna d'una organització davant d'un xarxa hostil, com Internet. A la xarxa interna podem trobar des d'equips d'ordinadors personals, impressores, dispositius mòbils (telèfons intel·ligents, etc.) o servidors. La presència de servidors, si ofereixen serveis a la xarxa externa, pot requerir un tracte especial en els sistemes tallafoc. Ens referim, per exemple, a servidors web, de correu electrònic o de compartició de fitxers que l'organització vol oferir a Internet. En general, aquests servidors no es tracten com els ordinadors de caràcter personal a l'hora de dissenyar-ne la protecció.

Un tipus d'equip important que es té en compte en el disseny de sistemes tallafoc són els anomenats equips bastió*.

*** En anglès, *bastion hosts*.**

Un **equip bastió** és un sistema informàtic que s'ha protegit molt per a suportar atacs des d'un lloc hostil (en aquest cas, Internet) i que sol actuar com a punt de contacte entre l'interior i l'exterior d'una xarxa.

L'equip bastió està contínuament exposat a atacs, per la qual cosa és necessari que estigui molt protegit. Sol proporcionar serveis que, per exemple, l'organització vol fer disponibles a l'exterior (web, correu electrònic, DNS, etc.), o proporciona serveis de xarxa crítics (encaminament, tallafoc, etc.).

Com veurem en els apartats següents, tot i que els tallafocs proporcionen moltes mesures de seguretat, cal tenir en compte que no són una solució definitiva ni única al problema de la seguretat en xarxes. Hi ha moltes amenaces que no es poden cobrir amb sistemes tallafoc. En aquest sentit, un aspecte molt important, com anirem veient, és que resulta difícil protegir contra un atacant intern amb un tallafoc. El mateix tallafoc, com tot sistema informàtic, pot presentar vulnerabilitats de dia-zero, o ser vulnerable a programes maliciosos i virus del sistema operatiu en què s'executa. A més, els sistemes tallafoc poden tenir certa mala premsa entre els usuaris de la xarxa, ja que moltes vegades aquests els veuen com a contrapartida a la seva comoditat o facilitat d'ús dels serveis de la xarxa.

2. Tipus de tallafocs

Tres de les tecnologies més usades a l'hora de construir sistemes tallafoc són les següents:

- encaminadors amb filtratge de paquets,
- passarel·les en el nivell de circuit, i
- passarel·les en el nivell d'aplicació.

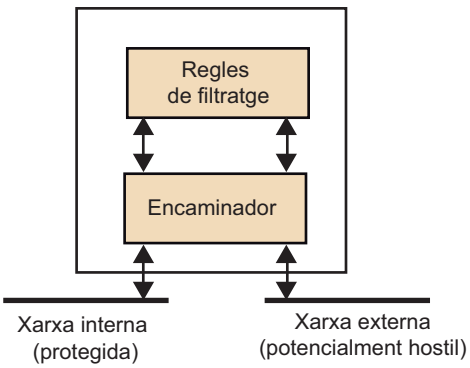
De vegades, aquests tipus de tallafoc reben el nom de *tallafoc de primera*, *tallafoc de segona* i *tallafoc de tercera generació*, respectivament, a causa de l'ordre en què han aparegut al llarg de la història. De manera molt genèrica, podem dir que la seva diferència rau en el nivell en què realitzen el filtratge, és a dir, a la capa de xarxa sobre la qual actuen. Així mateix, avui dia hi ha sistemes tallafoc que poden combinar el filtratge de paquets en capes diverses. Aquest tipus de filtratge multicapa s'anomena *stateful multi layer inspection*.

2.1. Encaminadors amb filtratge de paquets

Un encaminador amb filtratge de paquets (figura 1) és un dispositiu que encamina el trànsit TCP/IP (encaminador o *router* de TCP/IP) segons unes regles de filtratge que decideixen quins paquets s'encaminen a través d'aquest i quins es descarten.

En anglès, s'anomenen *packet filtering firewall*, i l'encaminador que fa aquest filtratge se sol anomenar *screening router*.

Figura 1. Encaminador amb filtratge de paquets



Les **regles de filtratge** s'encarreguen de determinar si a un paquet li està permès passar de la part interna de la xarxa a la part externa, i viceversa.

Aquestes regles de filtratge utilitzen informació que està present en els paquets de xarxa que travessen el tallafoc. Poden acceptar o denegar paquets fixant-se en les capçaleres dels protocols (per exemple, IP, UDP, TCP, etc.), com ara:

- adreces d'origen i de destinació,
- tipus de protocol i indicadors (*flags*) especials,
- ports d'origen i de destinació o tipus de missatge (segons el protocol),
- contingut dels paquets, i
- mida del paquet.

Cada paquet que arribi al dispositiu s'ha de comparar amb les regles de filtratge, començant pel principi de la llista de regles i fins que es trobi la primera coincidència. Si hi ha alguna coincidència, s'activa l'acció indicada per la regla.

Per contra, si no hi ha cap coincidència, es consulta la "política per defecte" per a saber quina acció cal prendre (deixar passar el paquet, descartar-lo, redireccionar-lo, etc.). Si es tracta, per exemple, d'una política de denegació per defecte, en el cas que no hi hagi cap coincidència amb el paquet, aquest es descarta.

Una política de denegació per defecte sol ser més costosa de mantenir, ja que serà necessari que l'administrador indiqui explícitament tots els serveis que han de romandre oberts (els altres, per defecte, es denegaran tots).

Polítiques per defecte

Una política de denegació per defecte també s'anomena *deny all* o *closed policy*, mentre que la política d'acceptació per defecte també s'anomena *allow all* o *open policy*.

En canvi, una política d'acceptació per defecte és més senzilla d'administrar, però incrementa el risc de rebre atacs contra la xarxa, ja que requereix que l'administrador indiqui explícitament els paquets que cal descartar (la resta, per defecte, s'acceptaran en la seva totalitat).

En la majoria d'ocasions s'opta per una política de denegació per defecte com a mesura de seguretat. Aquesta estratègia de vegades s'anomena *principi de seguretat en fallades* o *fail-safe*.

Un sistema tallafoc compleix el principi de seguretat en fallades si rebutja un esdeveniment no previst, com per exemple un paquet relatiu a un nou servei.

2.2. Passarel·les en el nivell de circuit

Les passarel·les en el nivell de circuit no encaminen paquets en el nivell d'enllaç de xarxa, sinó que actuen com a retransmissors (o *relays*) a nivell de transport. Aquests dispositius poden retenir paquets de xarxa fins a obtenir informació suficient sobre l'estat de la comunicació i decideixen si permeten la connexió o l'enviament de dades, o no ho permeten. Per això es diu que realitzen un filtratge amb estat o *stateful packet inspection*.

Vegeu també

Sobre el filtratge amb estat podeu veure el subapartat 4.2. d'aquest mòdul.

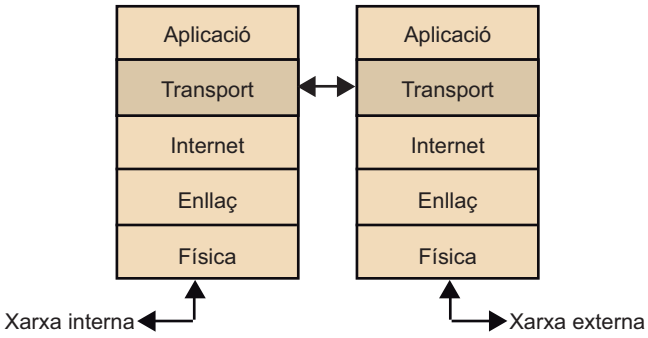
Una **passarel·la en el nivell de circuit** és un dispositiu que fa de passarel·la en el nivell de capa de transport entre dos extrems. Estableix una connexió amb cadascun d'aquests i retransmet les dades entre les dues connexions.

Una passarel·la en el nivell de circuit actua en la capa de transport de TCP/IP, o capa 4 del model OSI, com es mostra en la figura 2. No s'inspecciona el contingut dels paquets en el nivell d'aplicació, el que fa que siguin sistemes més eficients que les passarel·les en el nivell d'aplicació, encara que no tant com els encaminadors amb filtratge de paquets.

Vegeu també

Les passarel·les en el nivell d'aplicació s'estudien en el subapartat 2.3. d'aquest mòdul. Els encaminadors amb filtratge de paquets s'estudien en el subapartat 2.1.

Figura 2. Pasarel·la en el nivell de circuit



Aquest tipus de passarel·les se sol utilitzar per a connectar xarxes aïllades. Les connexions es poden establir automàticament per a determinats serveis TCP o s'hi poden usar protocols específics. Com exemple del segon cas tenim el protocol SOCKS (*SOCKet Secure*), el qual permet l'ús de TCP i UDP, i consta d'un client i un servidor. El servidor SOCKS s'executa en la passarel·la i el client en els ordinadors amfitrions *hosts* interns de la xarxa. Així, els clients de protocols d'aplicació solen incorporar suport per a SOCKS.

En el cas de TCP, per exemple, el client estableix una connexió amb el servidor SOCKS situat en el tallafoc (passarel·la en el nivell de circuit en aquest cas). El servidor autentica el client, avalua la petició de connexió i, si aquesta es permet, estableix una connexió amb el servidor extern mentre fa de *relay* (retransmissor) entre el client i el servidor en el nivell de TCP. Així, les passarel·les en el nivell de circuit també oculten en el nivell d'IP els clients davant el servidor extern.

SOCKS

La versió 5 de SOCKS està definida en l'RFC 1928 i actualment es considera un estàndard *de facto* per a implementar passarel·les en el nivell de circuit.

2.3. Pasarel·les en el nivell d'aplicació

Una passarel·la en el nivell d'aplicació, coneguda també com a servidor intermediari (*proxy*), actua com a retransmissor (*relay*) en el nivell d'aplicació. Els usuaris de la xarxa contacten amb el servidor intermediari, el qual, al seu torn, ofereix un servei intermediari (*proxy*) associat a una o més aplicacions determinades.

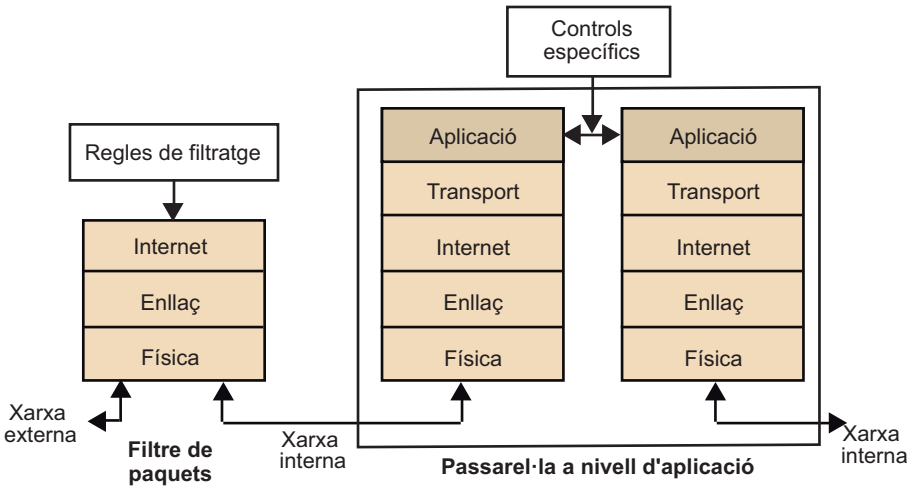
El servei intermediari s'encarrega de realitzar les connexions sol·licitades amb l'exterior i, quan rep una resposta, s'encarrega de retransmetre-la a l'equip que havia iniciat la connexió. Així, el servei intermediari executat a la passarel·la aplica les normes per decidir si s'accepta o es rebutja una petició de connexió.

De la mateixa manera que les passarel·les en el nivell de circuit, separa completament l'interior de l'exterior de la xarxa. Però, a diferència de les primeres, ho fa en el nivell de la capa d'aplicació i ofereix únicament un conjunt de serveis en el nivell d'aplicació. Això permet l'autenticació dels usuaris que realitzen peticions de connexió i l'anàlisi de connexions en el nivell d'aplicació.

Les passarel·les ofereixen més seguretat respecte als filtres de paquets, i per tant presenten un interval de possibilitats molt alt. Per contra, la penalització introduïda per aquests dispositius és molt més gran. Les passarel·les a nivell d'aplicació han de realitzar una inspecció de paquets detallada, que en anglès se sol anomenar *deep packet inspection*. En cas que hi hagi una gran càrrega de trànsit a la xarxa, el rendiment es pot arribar a reduir dràsticament. Una manera de millorar-ne el rendiment és l'ús de sistemes *proxy cache*, que mantenen una còpia local de dades rebudes.

A la pràctica, les passarel·les i els dispositius de xarxa amb filtratge de paquets són complementaris. Aquests dos sistemes es poden combinar, i així proporcionen més seguretat i flexibilitat que si només se n'utilitza un, com es mostra en la figura 3.

Figura 3. Filtratge de paquets i pasarel·la en el nivell d'aplicació



L'ús de les passarel·les proporciona diversos beneficis. D'entrada, una passarel·la podria permetre l'accés només als serveis per als quals hi ha un servidor intermediari habilitat. Així, si una passarel·la conté serveis intermediaris únicament per als serveis HTTP i DNS, llavors només HTTP i DNS estaran permesos a la xarxa interna. La resta dels serveis es rebutjaria completament.

Un altre benefici de l'ús de passarel·les en el nivell d'aplicació és que el protocol d'aplicació també es pot filtrar, de manera que es prohibeix l'ús de diferents subserveis dins d'un mateix servei permès. Per exemple, amb una passarel·la que filtrés connexions FTP, seria possible prohibir únicament l'ús de la comanda PUT d'FTP, i habilitar la resta d'ordres. Aquesta funció no és possible si únicament s'usen filtres de paquets.

Tot i obtenir més control global sobre els serveis vigilats, les passarel·les també presenten alguns problemes. Un dels primers inconvenients que cal destacar és la necessitat d'haver de configurar un servidor intermediari per a cada servei de la xarxa que s'ha de vigilar (HTTP, DNS, SSH, FTP, etc.). A més, en el cas de protocols client-servidor, com per exemple l'FTP, poden arribar a ser necessaris alguns passos addicionals per a connectar el punt final de la comunicació.

3. Arquitectures de tallafoc

Un aspecte molt important a l'hora de dissenyar un sistema tallafoc per a protegir una xarxa és decidir l'estratègia o arquitectura del sistema. És necessari decidir, a més del tipus de tallafoc que s'utilitza, on se situa aquest en la xarxa i com hi proporciona la seguretat perimetral.

En aquest aspecte hi ha nombroses arquitectures i tipus de xarxa, a més de moltes estratègies. En general, com i on s'instal·la un tallafoc depèn molt del tipus de xarxa que volem protegir i del tipus de protecció que hi volem aportar. Actualment no hi ha cap classificació consensuada, però sí que hi ha algunes estratègies comunes que revisarem a continuació.

Per a facilitar-ne l'explicació, dividirem les arquitectures en dos tipus:

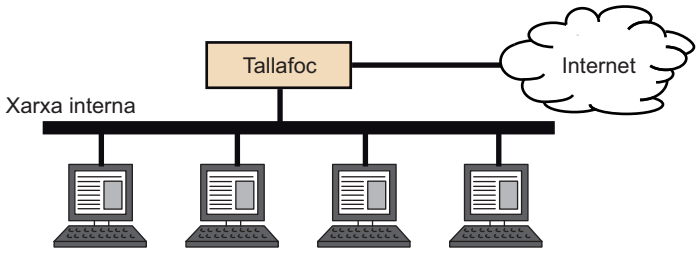
- arquitectures d'un sol punt, que també es coneixen amb el terme anglès *single-box*, i
- arquitectures de xarxa perimetral o subxarxa filtrada (*screened subnet*).

En general, l'objectiu d'implantar un sistema tallafoc és protegir una xarxa interna de l'exterior, que normalment és Internet. No obstant això, en altres casos es poden emprar tallafocs per a separar les parts d'una mateixa xarxa interna, com ara les estacions de treball d'un laboratori de proves.

3.1. Arquitectures d'un sol punt

Aquest tipus d'arquitectures és el més senzill, ja que consisteix a separar la xarxa que es vol protegir de l'exterior amb un sol dispositiu tallafoc (figura 4). Depenent de quin dispositiu faci de tallafoc, podem obtenir diferents solucions.

Figura 4. Arquitectura *single-box*



En general, aquestes arquitectures presenten un sol punt de configuració, cosa que les fa més senzilles d'implantar i administrar, tot i que alhora aquest punt es converteix en un punt crític del sistema. Si un atacant aconsegueix comprometre qualsevol dels servidors que hi ha darrere d'aquest punt únic, les altres màquines podran ser atacades sense cap restricció des de l'equip que ha estat posat en situació critica.

3.1.1. Encaminador amb filtratge de paquets

Aquesta situació és probablement la més senzilla, amb un encaminador amb filtratge de paquets o *screening router* que separa la xarxa interna de l'exterior. És a dir, es fa un filtratge de paquets de xarxa en un sol punt. Generalment és una solució de baix cost i la seva implantació és senzilla.

Vegeu també

El filtratge de paquets s'estudia en el subapartat 2.1. d'aquest mòdul.

Pot ser adequada en situacions en què es requereix eficiència i es considera que els equips de la xarxa ja disposen d'un grau de protecció considerable. És a dir, quan no es requereix un filtratge gaire sofisticat.

3.1.2. Tallafoc *dual-homed*

En aquest cas, el punt que separa la xarxa interna de l'externa és un equip *dual-homed*. Un equip *dual-homed* és un equip amb almenys dues interfícies de xarxa, cadascuna associada a una xarxa, que pot actuar com encaminador entre les xarxes. Els sistemes tallafoc *dual-homed* utilitzen aquest tipus d'equips, encara que no ho fan com a simples encaminadors.

Una **arquitectura de tallafocs *dual-homed*** es construeix amb un equip *dual-homed* amb la capacitat d'encaminament desactivada. D'aquesta manera, els paquets IP d'un extrem de la xarxa (la part hostil) no s'encaminaran cap a la part protegida, i viceversa, llevat que s'indiqui el contrari.

Amb aquesta arquitectura, els equips de la xarxa interna i de la xarxa externa es poden comunicar amb l'equip *dual-homed*, però no entre ells. Els equips de la xarxa interna i externa no es poden comunicar directament, sinó que un servidor intermediari s'encarrega de realitzar les connexions en nom d'aquestes dues parts.

Els tallafocs *dual-homed* proporcionen un grau de control alt sobre el trànsit que entra i surt de la xarxa, ja que els paquets externs no entren a la xarxa interna. L'equip *dual-homed* fa de passarel·la intermediària.

Un dels inconvenients principals d'aquesta arquitectura és que els equips *dual-homed* no són gaire eficients, sobretot si el trànsit és alt.

També és possible combinar el filtratge en el nivell de paquets en aquest tipus d'arquitectures, i permetre d'aquesta manera el filtratge a nivells diversos: Internet, transport o aplicació.

Vegeu també

Quant al filtratge en el nivell d'Internet, de transport o d'aplicació podeu consultar, respectivament, els subapartats 2.1., 2.2. i 2.3. d'aquest mòdul.

És molt comú implementar l'arquitectura *dual-homed* amb un equip bastió.

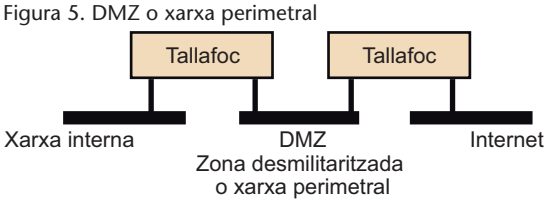
3.2. Arquitectures amb xarxes perimetrals

Vegeu també

L'equip bastió s'estudia en l'apartat 1 d'aquest mòdul.

Per a afegir un nivell addicional de seguretat a les arquitectures d'un sol punt tenim les arquitectures conegudes com a *xarxa filtrada* o *xarxa perimetral* (*screened subnet*). En aquest cas, la idea és afegir una **subxarxa** entre la xarxa interna i l'externa perquè actuï de barrera davant possibles atacs i intrusions. Aquesta xarxa perimetral se sol anomenar **zona desmilitaritzada** o *demilitarized zone* (**DMZ**).

Figura 5. DMZ o xarxa perimetral



DMZ i xarxa perimetral

No està clara la diferència entre DMZ i xarxa perimetral i moltes vegades es fan servir els dos termes indistintament. De vegades, es considera la DMZ com el conjunt de xarxes perimetrals del sistema tallafoc. És a dir, una DMZ pot estar formada per una o més xarxes perimetrals.

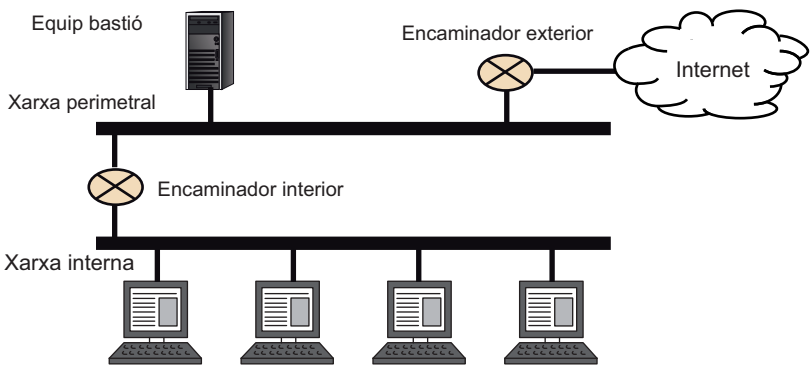
Aquesta xarxa perimetral o DMZ generalment alberga equips bastió, la qual cosa proporciona un nivell de seguretat addicional, i una separació de la xarxa interna. Aquests equips solen tenir servidors públics que han de ser accessibles des de l'exterior. En cas que un atacant aconsegueixi eludir la seguretat del primer tallafoc (o tallafoc exterior) i introduir-se en un servidor de la DMZ, no podrà atacar immediatament els equips situats en la xarxa interna, ja que estan protegits pel segon tallafoc (o tallafoc interior).

En la figura 6 veiem amb més detall una arquitectura de xarxa perimetral construïda amb encaminadors amb filtratge de paquets. La xarxa perimetral de la figura conté un equip bastió, encara que n'hi podria haver més d'un. A més de proporcionar serveis a l'exterior, aquests també es poden destinar a tasques de filtratge en el nivell d'aplicació o circuit.

Vegeu també

Els encaminadors amb filtratge de paquets s'estudien en el subapartat 2.1. d'aquest mòdul.

Figura 6. Exemple d'arquitectura amb xarxa perimetral



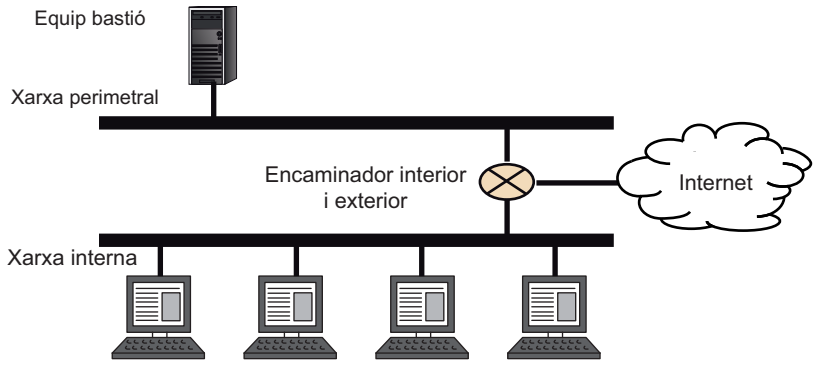
La funció de cadascun dels dos encaminadors és diferent:

- **Encaminador interior** (o ***choke router***). Protegeix la xarxa interna d'Internet i de la xarxa perimetral. Realitza la major part del filtratge de sortida i d'entrada a la xarxa interna, respecte a l'exterior. Així mateix, controla el trànsit entre la xarxa interna i l'equip bastió. Generalment, el trànsit entre la xarxa interna i l'equip bastió és extremadament limitat per a evitar que el compromís d'un bastió comporti la possibilitat d'atacar la xarxa interna.

- **Encaminador exterior** (o ***access router***). Protegeix la xarxa interna i la perimetral de l'exterior. Són menys restrictius que els interiors, i les seves regles de filtratge estan especialment pensades per a protegir l'equip bastió de l'exterior. De vegades, l'encaminador exterior pot estar controlat per una organització externa (per exemple, el proveïdor de serveis d'Internet).

En cas que es disposi d'un encaminador amb filtratge de paquets adequat, es pot utilitzar aquest encaminador per a realitzar les tasques d'encaminador interior i exterior, com mostra la figura 7, i així se simplifica el sistema.

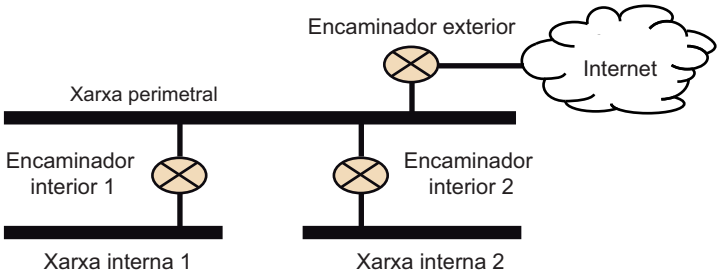
Figura 7. Exemple d'arquitectura amb xarxa perimetral i un sol encaminador



En general, en aquestes arquitectures es pot combinar l'ús d'encaminadors amb filtratge de paquets amb l'ús de passarel·les en el nivell d'aplicació o circuit, segons es consideri oportú. Per exemple, es pot substituir l'encaminador exterior per un equip *dual-homed*; concretament, l'equip bastió de la xarxa perimetral pot fer d'encaminador exterior amb el propòsit de simplificar i reduir els costos del sistema. Encara que l'equip bastió queda més exposat, no hi ha un augment significatiu de la vulnerabilitat. No obstant això, no es recomana utilitzar l'equip bastió com a encaminador intern, ja que precisament una funció important d'aquest encaminador és protegir la xarxa interna en cas que el bastió quedi compromès.

En cas que tinguem dues xarxes internes independents, aquestes poden compartir la mateixa xarxa perimetral o DMZ, com es mostra en la figura 8, mitjançant dos encaminadors interiors.

Figura 8. Exemple de arquitectura amb xarxa perimetral i dues xarxes internes



És important remarcar que no se sol recomanar l'ús de diversos encaminadors interiors per a una sola xarxa interna. Això implica més càrrega administrativa i requereix una configuració acurada dels encaminadors. Pot ser una solució acceptable si l'objectiu és proporcionar redundància, però fins i tot en aquest cas se sol desaconsellar, ja que generalment es recomana proporcionar redundància també en la xarxa perimetral.

Vegeu també

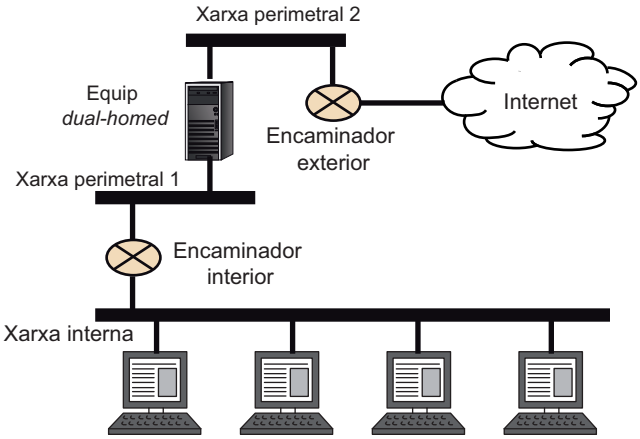
La redundància en el nivell de xarxa perimetral es tracta en el subapartat 3.2.1. d'aquest mòdul.

D'altra banda, l'ús de diversos encaminadors exteriors pot tenir sentit en cas que es vulgui introduir redundància (no implica tants problemes com el cas anterior de diversos encaminadors interiors), o simplement perquè es vol donar sortida o entrada a dues xarxes externes diferents.

3.2.1. Múltiples xarxes perimetrals

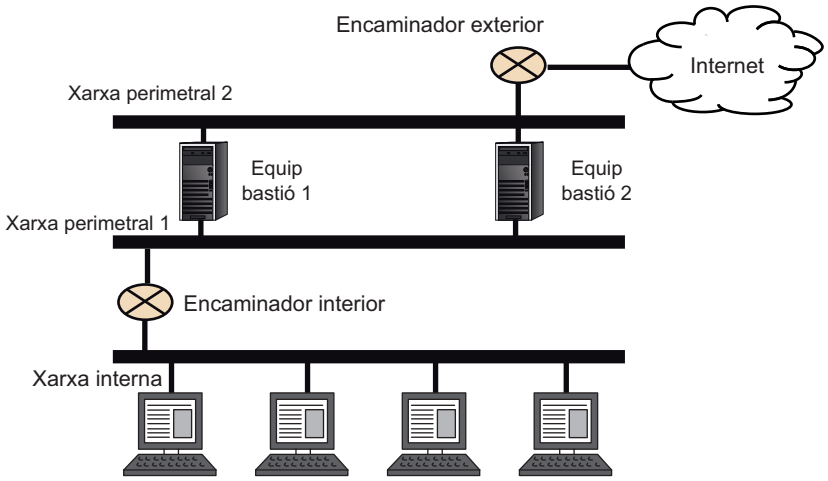
Encara que l'esquema que es mostra en la figura 6 és bastant comú, hi ha arquitectures basades en xarxes perimetrals més sofisticades. Un exemple d'això és l'ús d'un equip *dual-homed* que divideix la xarxa perimetral o DMZ, com es mostra en la figura 9. Aquest tipus d'arquitectura, també coneguda com *split-screened subnet* o *belt-and-suspenders firewall*, vol proporcionar més seguretat i capacitat de defensa. Els encaminadors protegeixen l'equip *dual-homed* que realitza funcions de *proxy*. Proporciona un nivell de seguretat molt alt, però requereix una configuració més detallada i complexa.

Figura 9. Exemple d'arquitectura de xarxa perimetral dividida



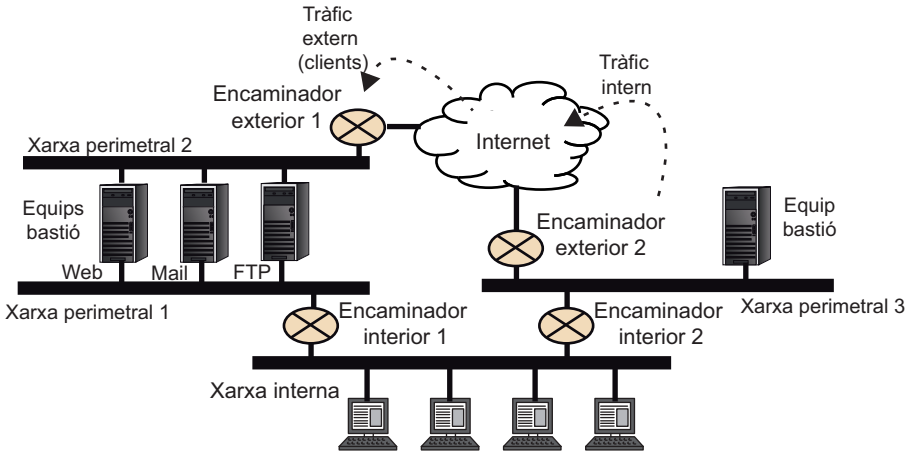
Un ús típic d'aquest esquema és el destinat a controlar l'accés administratiu als serveis allotjats en equips bastió de la DMZ. Per a això se separa el trànsit administratiu (originat a la xarxa interna) del trànsit extern, com es mostra en la figura 10.

Figura 10. Exemple d'arquitectura de xarxa perimetral dividida amb equips bastió



També hi ha arquitectures en les quals les diferents xarxes perimetrals són totalment independents. És a dir, múltiples encaminadors exteriors i interiors que separen per complet les xarxes perimetrals. Aquest tipus d'arquitectura se sol aplicar per a proporcionar redundància per mitjà de dos accessos diferents a Internet. També es pot usar com a mesura de privacitat i separar el trànsit entre una xarxa perimetral o una altra en funció del seu grau de confidencialitat; o per a separar el trànsit d'entrada a servidors de l'organització del trànsit de sortida de l'organització mateixa. Aquest tipus d'arquitectura més elaborada sol proporcionar un grau de protecció més alt, però tenen l'inconvenient que la seva administració és molt més complexa. En la figura 11 veiem un exemple d'arquitectura complexa amb múltiples xarxes perimetrals.

Figura 11. Exemple d'arquitectura complexa de xarxes perimetrals



Basat en: Zwicky, E. D.; Cooper, S.; Chapman, D. B. (2000). *Building Internet Firewalls*. 2a ed. O'Reilly Media.

4. Mecanismes i regles de filtratge

Un dels aspectes més importants d'un sistema tallafoc és com s'aconsegueix implementar la política del sistema o organització amb regles concretes de filtratge. L'administració i configuració de tallafocs és, de vegades, complexa i es considera un art en si mateixa. En aquest apartat us mostrarem tècniques genèriques de filtratge. Cal tenir en compte que cada sistema tallafoc utilitza regles diferents, amb format diferent i que es poden aplicar de maneres diferents.

Considerem el filtratge de paquets com un mecanisme de seguretat en xarxes que té l'objectiu de controlar el flux de dades d'entrada i sortida d'una xarxa.

Un bon mecanisme de filtratge de paquets pot permetre un control molt detallat i sofisticat de les dades que es transmeten per la xarxa. Tanmateix, és important ser conscients del grau de dificultat de tot plegat. Hi ha tasques molt més senzilles que altres, és a dir, que es poden dur a terme més eficientment i amb un cost més baix que altres. Per exemple, una regla que necessiti informació sobre el funcionament d'un protocol concret serà més complexa que una que no necessiti aquesta informació. Així mateix, si cal inspeccionar dades pròpies de l'aplicació, n'estem augmentant la complexitat. Aquests dos últims casos s'acostumen a fer amb passarel·les, mentre que els encaminadors amb filtratge de paquets realitzen un filtrat més senzill i, per tant, molt eficient.

4.1. Filtratge de paquets bàsic

El filtratge bàsic de paquets es fa a partir d'informació disponible a les capçaleres del protocol IP i protocols de transport, i es tracta de manera independent a cada paquet. Aquesta informació sol ser relativament reduïda:

- Adreça IP d'origen i destinació.
- Port d'origen i destinació de la capa de transport.
- Protocol: aquest camp fa referència al camp *Protocol* de la capçalera del datagrama IPv4 o *Next Header* en el cas d'IPv6.

Next Header

En IPv6, *Next Header* identifica l'extensió de capçalera següent. En cas que no hi hagi cap extensió o es tracti de l'última extensió, el camp indica el protocol encapsulat pel datagrama, i utilitza el mateix identificador que IPv4.

Aquest tipus de filtratge permet especificar regles del tipus "Permetre tot el trànsit de sortida destinat al port 80 (HTTP)", però no permet expressar regles del tipus "Permetre tot el trànsit HTTP únicament si no s'està utilitzant per a descarregar arxius de MS Word".

Cada regla de filtratge té associada una *acció* o *target* que determina què es fa amb el paquet que compleix amb la regla. Les principals accions que es poden realitzar amb el paquet són *acceptar* (*ACCEPT*) el paquet i, per tant, permetre el seu pas pel tallafoc, o bé *rebutjar* (*DENY*) el paquet i descartar-lo. Hi pot haver accions addicionals, com ara l'acció *LOG*, que fa que el tallafoc generi un arxiu *log* sobre el paquet, o la que es discuteix en el subapartat següent. Accions del tipus *ACCEPT* o *DENY* provoquen que es realitzi l'acció sobre el paquet i s'acabi el procés de filtratge; en canvi, accions com *LOG* generen l'acció, però en general es continuen processant regles de filtratge.

4.1.1. Com es rebutja un paquet

En cas que es rebutgi un paquet, hi ha la possibilitat de generar un missatge d'error ICMP per a notificar a l'origen que s'ha descartat aquest paquet. Generalment es tracta de missatges ICMP de tipus 3 (*Destination Unreachable*), amb els codis que es mostren en la taula 1. Per a diferenciar-les, és habitual anomenar *DROP* a l'acció de descartar un paquet i *REJECT* quan es descarta i es genera l'ICMP d'error.

Taula 1. Codis d'error ICMP que solen enviar els tallafocs en descartar un paquet

Tipus	Codi	Descripció
3	0	*Destination network unreachable*
3	1	*Destination host unreachable*
3	9	*Network administratively prohibited*
3	10	*Host administratively prohibited*

Els codis 9 i 10 es van afegir especialment a l'especificació d'ICMP per a utilitzar-los amb sistemes de filtratge. Tot i això, molts d'aquests sistemes continuen utilitzant els codis 0 i 1, els quals es van pensar inicialment per a altres propòsits.

Generar un missatge d'error ICMP o no generar-lo quan es descarta un paquet té avantatges i inconvenients:

- El fet d'enviar el missatge ICMP d'error fa que l'origen pugui tancar la connexió immediatament, sense necessitat d'esperar cap timeout, i sense intentar cap retransmissió.

- El missatge ICMP concret que s'envia pot ser interpretat de diferents maneres pels equips d'origen que el reben.

- La generació d'aquests missatges pot comportar una penalització en el rendiment del tallafoc.

- L'enviament d'aquests missatges pot fer que atacants potencials obtinguin informació del filtratge de paquets.

Generalment, es considera més segur no enviar aquest tipus de missatges d'error, però pot haver casos en què sigui convenient fer-ho. Alguns sistemes tallafoc poden incorporar mecanismes addicionals. Per exemple, permetre tancar connexions TCP immediatament responent amb un *reset* de TCP.

4.1.2. Organització de les regles de filtratge

L'ordre amb què es miren les regles de filtratge és molt important, ja que és el mecanisme principal per a resoldre els conflictes. És a dir, si hi ha dues regles contradictòries, la primera que es consulti és la que s'ha d'executar.

En general, és l'administrador qui decideix l'ordre de les regles, que sol ser l'ordre en què s'introdueixen. No obstant això, alguns tallafocs poden modificar aquest ordre per a millorar-ne l'eficiència.

En molts casos les regles s'agrupen per tipus o taules i hi ha un ordre predefinit entre els tipus de regles. Per exemple, el tallafoc *Windows Firewall with Advanced Security* agrupa les regles en els sis tipus que es mostren en la taula 2.

Taula 2. Tipus de regles de filtratge de Window Firewall with Advanced Security

Ordre	Tipus	Descripció
1	*Windows Service Hardening*	Impedeixen que els serveis estableixin connexions per a les quals no van ser dissenyats.
2	*Windows Service Hardening*	Defineixen l'autenticació amb IPSec.
3	*Authenticated bypass rules*	Permeten que cert trànsit se salti restriccions (regles) que el bloquegi si ha estat autenticat amb IPSec.
4	*Block rules*	Regles que bloquegen trànsit.
5	*Allow rules*	Regles que permeten trànsit.
6	*Default rules*	Accions per defecte.

Windows Firewall

Windows Firewall és el tallafoc que incorporen els sistemes operatius Microsoft Windows (Windows 7, Windows Server 2008, Windows Server 2008 R2 i Windows Vista). Anteriorment s'anomenava ICS (*Internet Connection Firewall*).

Aquest tallafoc, a més d'oferir un filtratge de paquets com el que veiem en aquest mòdul, permet gestionar IPSec. Com veiem, totes les regles relacionades amb IPSec tenen preferència sobre la resta. És interessant veure en aquest cas com se separen les regles que bloquegen trànsit de les que el permeten. Això vol dir que es rebutjarà el trànsit que coincideixi amb dues regles contradictòries (una que el permet i una altra que el rebutja). El fet que les regles que rebutgen trànsit tinguin precedència es pot veure com una mesura de seguretat: en cas de dubte, no es permet el trànsit en qüestió.

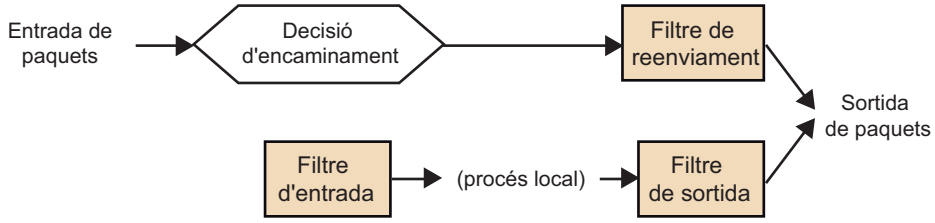
Un altre exemple de sistema tallafoc molt usat avui en dia és Netfilter/iptables, que forma part del nucli de Linux. Iptables permet configurar el tallafoc des de la línia d'ordres. Netfilter/iptables utilitza la taula *filter* per a realitzar el filtratge de paquets, on les regles s'organitzen en cadenes. Hi ha cadenes predefinides i l'administrador pot definir cadenes noves si ho considera convenient. Les cadenes predefinides per al filtratge de paquets són:

Netfilter/iptables disposa de més taules per a fer altres tasques com NAT.

- *INPUT*: afecta paquets destinats al sistema local.
- *FORWARD*: paquets que passen a través del dispositiu (són encaminats pel sistema).
- *OUTPUT*: per a paquets generats pel mateix sistema.

L'ordre d'aquestes cadenes, bastant intuïtiu, ve determinat per la decisió d'encaminament del paquet (si la destinació és el sistema local o no), com es mostra en la figura 12.

Figura 12. Cadenes de la taula de filtratge de Netfilter/iptables



Cada cadena predefinida té una acció per defecte que especifica l'administrador. Dins de cada cadena, l'ordre en què es revisen les regles és el que determina l'administrador del sistema en introduir-hi les regles. D'aquí ve el nom de *cadena*, perquè una cadena no és res més que un conjunt seqüencial de regles.

4.2. Filtratge dinàmic

El filtratge dinàmic o *stateful filtering* utilitza informació de l'estat de la connexió o sessió a l'hora de filtrar paquets. Permet associar paquets a sessions concretes i estats de protocols. En aquest sentit, el tallafoc ha de seguir l'estat de les transaccions de paquets i el seu comportament pot variar en funció del trànsit que hi va passant.

Exemple d'ús de filtratge dinàmic

Aquest tipus de filtratge permet establir regles com "Permetre l'entrada de missatges UDP únicament si es reben com a resposta a una petició UDP originada a la xarxa interna". Per exemple, la taula 3 mostra tres paquets UDP que podrien passar pel tallafoc. Considerem que la nostra xarxa interna és la 230.0.113.0/24. Segons la regla descrita anteriorment, els paquets 1 i 2 s'acceptarien, mentre que el paquet 3 no. Aquest paquet està intentant entrar a la nostra xarxa i, al contrari que el paquet 2, no es correspon a la resposta d'un paquet originat a la nostra xarxa, i es pot tractar d'un paquet fals.

Taula 3. Exemple de paquets UDP

1	IP origen	230.0.113.1	IP destinació	192.0.2.1
	P. origen	43321	P. destinació	7
2	IP origen	192.0.2.1	IP destinació	230.0.113.1
	P. origen	7	P. destinació	43321
3	IP origen	192.0.2.1	IP destinació	230.0.113.1
	P. origen	7	P. destinació	34511

Cal tenir en compte que aquest tipus de filtratge no és perfecte i pot ser vulnerable a atacs de falsejament d'identitat (*IP spoofing*), que falsegen l'adreça IP i el port d'origen perquè sembli que el paquet és la resposta esperada.

El principal problema d'aquest tipus de filtratge és la seva eficiència. El tallafoc necessita recursos de memòria i de processament per a mantenir l'estat del trànsit que veu. Això no solament significa una càrrega important, sinó que obre la possibilitat de rebre atacs de denegació de servei.

L'exemple anterior és molt simplista i actualment hi ha sistemes tallafoc dinàmics molt elaborats que permeten realitzar moltes comprovacions, a tots els nivells, de la pila de protocols xarxa i dades d'aplicació.

Per exemple, es poden utilitzar tècniques de **comprovació de protocol**. Un paquet UDP destinat al port 53 se sol considerar com una petició a un servidor DNS, però podria ser un intent d'emmascarar un paquet maliciós. La comprovació de protocols permet al tallafoc inspeccionar el paquet i veure si realment es tracta d'una petició de DNS. És a dir, comprova que el datagrama UDP contingui un missatge de petició DNS amb la capçalera i la informació corresponents.

Mecanismes més avançats permeten ara inspeccionar les dades del protocol d'aplicació. Avui dia no és estrany disposar de passarel·les en el nivell d'aplicació que puguin filtrar continguts de pàgines web o connexions FTP segons el nom d'usuari.

De vegades, la qualificació de filtratge dinàmic o amb estat no està clara. Per exemple, alguns tallafocs permeten establir regles de filtratge de trànsit TCP en funció dels indicadors (*flags*) actius en el segment TCP, com per exemple SYN o ACK. Això permet distingir si el paquet és l'inici de connexió TCP (no té l'ACK actiu) o forma part d'una connexió ja existent (amb l'ACK actiu). No obstant això, aquest tipus de comprovació es realitza a partir de cada segment TCP de manera independent. És a dir, el tallafoc no necessita mantenir l'estat de la connexió TCP. Per aquest motiu, aquest tipus de filtratge no se sol considerar com filtratge amb estat o dinàmic.

4.3. Exemples de filtratge

A continuació veurem dos exemples* de regles de filtratge per a dos escenaris diferents. El primer exemple considera una arquitectura d'un sol punt, mentre que el segon correspon a una arquitectura de xarxa perimetral. En ambdós casos es tracta de trànsit de filtratge bàsic sense estat. El filtratge amb estat no és tan genèric i depèn molt del producte concret que l'implementa.

*** Aquests exemples estan inspirats llunyanament en l'obra de Zwicky *et al.* (2000).**

Vegeu també

L'arquitectura d'un sol punt s'estudia en el subapartat 3.1.1. d'aquest mòdul, mentre que l'arquitectura de xarxa perimetral s'estudia en el subapartat 3.2.

4.3.1. Exemple 1: tallafoc d'un sol punt

Com a primer exemple podem pensar en la xarxa que es mostra en la figura 13. En aquesta xarxa es determina la política següent:

1) Es permet que els usuaris de la xarxa interna puguin accedir a qualsevol servei TCP d'Internet.

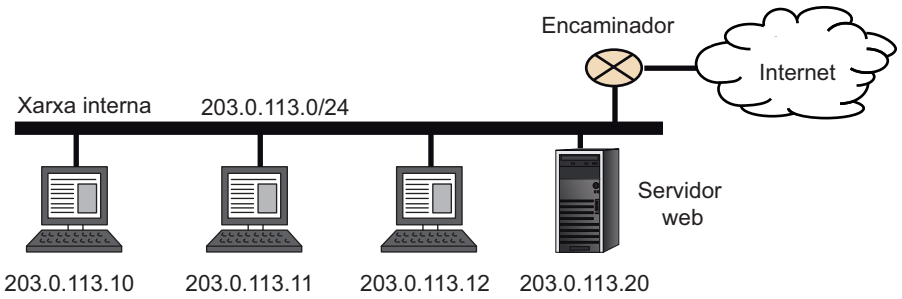
2) Es permet que els usuaris de la xarxa que facin connexions UDP a l'exterior, però només per a realitzar peticions DNS.

3) Es permet el trànsit ICMP de sortida (originat a la xarxa interna).

4) Des de l'exterior només es pot accedir al servidor web, no a la resta d'equips.

5) La resta de trànsit per defecte no es permet.

Figura 13. Exemple de filtratge



En aquest cas tenim un encaminador amb filtratge de paquets. La informació que pot obtenir aquest encaminador per a determinar les regles de filtratge són les adreces IP d'origen i destinació, els ports d'origen i destinació, i el protocol.

Si considerem un filtratge de paquets bàsic, hi podem afegir les regles que es mostren en la taula 4.

Taula 4. Regles d'exemple per a l'escenari de la figura 13

Regla	Acció	IP origen	P. origen	IP destinació	P. destinació	Protocol
1	*ACCEPT*	203.0.113.0/24	> 1023	*	53	UDP
2	*ACCEPT*	*	53	203.0.113.0/24	> 1023	UDP
3	*ACCEPT*	203.0.113.0/24	> 1023	*	*	TCP
4	*ACCEPT*	*	*	203.0.113.0/24	> 1023	TCP
5	*ACCEPT*	203.0.113.0/24	-	*	-	ICMP
6	*ACCEPT*	*	-	203.0.113.0/24	-	ICMP
7	*ACCEPT*	*	> 1023	203.0.113.20	80	TCP
8	*ACCEPT*	203.0.113.20	80	*	> 1023	TCP
9	*DENY*	*	*	*	*	*

Com que es tracta d'una política tancada o *deny all*, s'ha de rebutjar tot el trànsit per defecte. Això s'aconsegueix mitjançant la regla 9, que rebutja tot i és l'última. La resta de les regles són les següents:

- **Regles 1 i 2**: es permet la sortida de trànsit UDP destinat al port UDP 53, que correspon a DNS. La regla 2 és necessària per a permetre l'entrada de la resposta a la petició de DNS. El port d'origen de la regla 1 es restringeix a ports > 1023. És una bona idea restringir totes les regles tant com sigui possible per a evitar accions no desitjades fruit de situacions imprevistes.

- **Regles 3 i 4**: permeten la sortida de trànsit TCP des de ports no privilegiats a qualsevol part d'Internet. Així mateix, es permet l'entrada de trànsit TCP a aquests mateixos ports no privilegiats. Aquí s'ha optat per restringir el port d'origen a un port de client.

- **Regles 5 i 6**: permeten la sortida de trànsit ICMP i l'entrada. Ha calgut incloure la regla 6, que permet l'entrada de paquets ICMP, ja que, per exemple, si permetem que els usuaris de la xarxa enviïn un *ICMP echo request* (*ping*), no té sentit que no en permetem la resposta (*echo replay*).

- **Regles 7 i 8**: permeten connexions exteriors cap al servidor web pel port TCP 80 i la seva resposta.

S'ha hagut de permetre tot el trànsit d'entrada ICMP, cosa que contradiu la política de seguretat. Aquest és un cas en què la informació bàsica que hem usat per a definir les regles no és suficient per a implementar la política. Cal introduir-hi més detalls que ens permetin discernir quins casos concrets de missatges ICMP deixem que entrin a la xarxa (missatges de resposta a peticions iniciades a la xarxa interna). La majoria dels tallafocs actuals permeten detallar el tipus de missatges ICMP en la regla.

Una altra observació important en relació amb l'exemple és que sempre s'ha intentat restringir al màxim l'aplicabilitat de les regles. Per exemple, es restringeix l'ús de ports *well known* (< 1024), sempre que sigui possible. El seguiment del principi de mínim privilegi és una pràctica molt comuna i recomanada en el disseny de les regles de tallafocs.

El **principi de mínim privilegi** (o *least privilege principle*) determina que cada acció de sistema es realitzi amb el mínim conjunt de privilegis possible, esdir, els estrictament necessaris per a dur a terme aquesta acció.

4.3.2. Exemple 2: xarxa perimetral

En aquest cas considerem un exemple de xarxa perimetral com el de la figura 14, en què la xarxa perimetral (198.51.100.0/24) compta amb quatre equips bastió, cadascun dels quals està dedicat a un servei concret. Així mateix, la xarxa interna (192.0.2.0/24) té un servidor de DNS i un altre de correu electrònic per a ús intern.

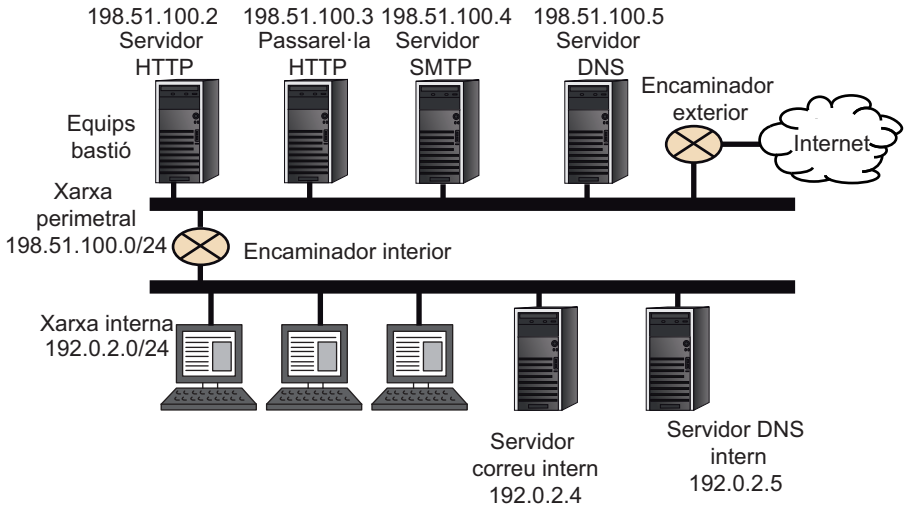
Les regles utilitzades pels encaminadors contenen més informació que en l'exemple anterior. Aquesta informació addicional és l'adreça (orientació) del paquet, que pot ser d'entrada o sortida. Fins ara hem considerat que les adreces IP d'origen i destinació ens proporcionaven aquesta informació. Tanmateix, això no ha de ser cert per força, ja que les adreces IP d'un datagrama po-

den no ser legítimes. La majoria dels tallafocs permeten fer aquesta distinció explícitament o bé indicant la interfície de xarxa per la qual es rep el paquet. A més, hi introduïm una condició relativa a segments TCP que indica si el segment té el *flag* ACK actiu o no.

Vegeu també

El *flag* ACK s'estudia en el subapartat 4.2. d'aquest mòdul.

Figura 14. Exemple de filtratge amb xarxa perimetral



A continuació descrivim la política del sistema:

- **Web**. L'equip bastió 198.51.100.3 fa de passarel·la d'aplicació dels protocols HTTP i HTTPS per als equips de la xarxa interna.

- **Servidor web**. L'equip bastió 198.51.100.2 alberga el servidor web de l'organització, que ofereix exclusivament serveis per HTTP (Port 80 de TCP) a l'exterior.

- **SSH**. Es permet accés per SSH a qualsevol equip de la xarxa interna des d'Internet o la xarxa perimetral, i també l'accés des de la xarxa interna a qualsevol equip d'Internet o xarxa perimetral. En relació amb la xarxa perimetral, es permet l'accés des d'Internet a aquesta xarxa per a administrar remotament els equips bastió.

  Encara que SSH és un servei important i generalment considerat segur, és important tenir en compte que en permetre el trànsit SSH en totes dues direccions, estem dipositant una confiança important en els usuaris. Permetre l'establiment de connexions SSH des de l'exterior pot introduir-hi vulnerabilitats, sobretot en presència d'usuaris maliciosos. Aquests usuaris poden executar altres serveis en el port 22 o realitzar *port forwarding* o túnels sobre SSH.

  Vegeu també

  Els túnels s'estudien en el subapartat 5.1. d'aquest mòdul.

  Una opció més segura és permetre únicament connexions SSH a la xarxa interna des de la xarxa perimetral (no des de tot Internet), i concretament

des d'un equip bastió que faria de passarel·la SSH. Llavors, els usuaris han d'establir primer una connexió amb l'equip bastió i, des d'aquest, a l'equip desitjat de la xarxa interna.

- **SMTP**. Tenim un servidor SMTP a l'equip bastió 198.51.100.4 de la xarxa perimetral, que pot rebre trànsit SMTP d'entrada i sortida, des de i cap a Internet. Així mateix, aquest servidor SMTP farà el mateix vers un servidor SMTP de la xarxa interna, el 192.0.2.4.

  Aquesta configuració és molt típica per als servidors SMTP, en la qual els usuaris de la xarxa interna utilitzen el servidor intern, però es limita l'accés d'aquest des de l'exterior mitjançant un equip bastió. Aquest equip bastió fa en certa manera de passarel·la SMTP i evita que possibles atacants puguin accedir directament al servidor intern que utilitzen els usuaris. La redirecció del correu electrònic extern cap a l'equip bastió se sol fer mitjançant registres MX al DNS.

- **DNS**. Hi ha un servidor intern de DNS (192.0.2.5) que utilitzen els equips de la xarxa interna. Al seu torn, aquest servidor realitza les peticions i rep respostes d'un servidor DNS situat en un equip bastió de la xarxa perimetral (198.51.100.5), que al seu torn utilitzarà servidors externs d'Internet. Qualsevol petició de DNS externa serà rebuda pel servidor a l'equip bastió i no podrà accedir directament a la xarxa interna. Així mateix, es permetran les transferències de zona (mecanisme per a la replicació de bases de dades DNS) entre aquests dos servidors.

  El trànsit DNS sol tenir certa complexitat i convé entendre bé com funcionen els protocols DNS. Recordem breument que els missatges de petició i resposta poden anar sobre TCP o UDP, el port del servidor és el 25. En cas que sigui entre servidors, la petició i la resposta es fan per UDP al port 25 (tots dos utilitzen el mateix port).

Lectures complementàries

Podeu trobar informació detallada sobre el funcionament dels protocols de DNS en els RFC 1034 i 1035, i sobre la transferència de zones, en el RFC 5936.

A continuació procedim a mostrar una possible configuració de regles per als encaminadors interior i exterior. A part de regles relatives a cada protocol i servei, els dos encaminadors incorporen regles per defecte al final que rebutgen qualsevol paquet. En aquest cas, cal especificar una regla per defecte per a l'entrada i una altra per a la sortida.

L'ús de l'orientació del paquet també ens permet introduir regles per a rebutjar directament paquets amb informació errònia, i així evitem possibles atacs de falsejament d'identitat (*IP spoofing*). Per exemple, l'encaminador interior no hauria de deixar entrar trànsit per al qual 'adreça d'origen sigui de la xarxa interna (regla X_1 de l'encaminador interior). De la mateixa manera, l'encaminador exterior no hauria de deixar entrar paquets des de l'exterior amb una adreça d'origen que sigui de la xarxa interna o perimetral (regles X_1, X_2 de l'encaminador exterior).

En la taula 5 veiem les regles corresponents a l'encaminador interior.

Taula 5. Regles per a l'encaminador interior

Regla	Acció	Dir.	IP origen	P. origen	IP destinació	P. destinació	Prot.	ACK
X_1	*DENY*	In	192.0.2.0/24	*	*	*	*	*
H_1	*ACCEPT*	Out	192.0.2.0/24	>1023	198.51.100.3	80	TCP	*
H_2	*ACCEPT*	In	198.51.100.3	80	192.0.2.0/24	>1023	TCP	*
S_1	*ACCEPT*	Out	192.0.2.0/24	*	*	22	TCP	*
S_2	*ACCEPT*	In	*	22	192.0.2.0/24	*	TCP	Si
S_3	*ACCEPT*	In	*	*	192.0.2.0/24	22	TCP	*
S_4	*ACCEPT*	Out	192.0.2.0/24	22	*	*	TCP	Si
M_1	*ACCEPT*	Out	192.0.2.4	>1023	198.51.100.4	25	TCP	*
M_2	*ACCEPT*	In	198.51.100.4	25	192.0.2.4	>1023	TCP	Si
M_3	*ACCEPT*	In	198.51.100.4	>1023	192.0.2.4	25	TCP	*
M_4	*ACCEPT*	Out	192.0.2.4	25	198.51.100.4	>1023	TCP	Si
D_1	*ACCEPT*	Out	192.0.2.5	53	198.51.100.5	53	UDP	-
D_2	*ACCEPT*	In	198.51.100.5	53	192.0.2.5	53	UDP	-
D_3	*ACCEPT*	Out	192.0.2.5	>1023	198.51.100.5	53	TCP	*
D_4	*ACCEPT*	In	198.51.100.5	53	192.0.2.5	>1023	TCP	Si
D_5	*ACCEPT*	In	198.51.100.5	>1023	192.0.2.5	53	TCP	*
D_6	*ACCEPT*	Out	192.0.2.5	53	198.51.100.5	>1023	TCP	Sí
F_1	*DENY*	Out	*	*	*	*	*	*
F_2	*DENY*	In	*	*	*	*	*	*

A continuació es detallen aquestes regles:

- H_1, H_2: permeten la sortida de trànsit HTTP i HTTPS de la xarxa interna cap a l'equip bastió que fa de passarel·la d'aplicació per a aquests protocols i permet la recepció de la seva resposta. És important assenyalar que els clients han de configurar aquesta passarel·la en els seus navegadors i que no cal habilitar el trànsit per al port 443 (HTTPS), ja que aquesta connexió la realitza la passarel·la, i no pas el client (la connexió entre el client i la passarel·la sempre és pel port 80).

- S_1, S_2: permeten establir connexions des de la xarxa interna a servidors SSH de l'exterior (incloent-hi la xarxa perimetral).

- S_3, S_4: permeten establir connexions SSH des de l'exterior a servidors situats a la xarxa interna.

- M_1, M_2: permeten la sortida del correu electrònic des del servidor de correu intern cap al servidor de l'equip bastió a la xarxa perimetral.

- M_3, M_4: permeten l'entrada de correu des del servidor de la xarxa perimetral al servidor intern.

- D_1: permet peticions i respostes DNS per UDP des del servidor intern al situat en l'equip bastió.

- D_2: com l'anterior, però des de l'equip bastió cap al servidor intern.

- D_3, D_4: permeten peticions DNS per TCP des del servidor intern al de l'equip bastió. Aquestes regles també permeten la transferència de zona des del servidor de l'equip bastió (primari) al de la xarxa interna (secundari).

- D_5, D_6: equivalents a les anteriors, però intercanviant els servidors.

De la mateixa manera, la taula 6 mostra les regles de l'encaminador exterior. A continuació es comenten i es justifiquen:

Taula 6. Regles per a l'encaminador exterior

Regla	Acció	Dir.	IP origen	P. origen	IP destinació	P. destinació	Prot.	ACK
X_1	*DENY*	In	192.0.2.0/24	*	*	*	*	*
X_2	*DENY*	In	168.51.100.0/24	*	*	*	*	*
H_1	*ACCEPT*	Out	198.51.100.3	>1023	*	*	TCP	*
H_2	*ACCEPT*	In	*	*	198.51.100.3	>1023	TCP	Si
H_3	*ACCEPT*	In	*	>1023	198.51.100.2	80	TCP	*
H_4	*ACCEPT*	Out	198.51.100.2	80	*	>1023	TCP	Si
S_1	*ACCEPT*	Out	192.0.2.0/24	*	*	22	TCP	*
S_2	*ACCEPT*	In	*	22	192.0.2.0/24	*	TCP	Si
S_3	*ACCEPT*	In	*	*	192.0.2.0/24	22	TCP	*
S_4	*ACCEPT*	Out	192.0.2.0/24	22	*	*	TCP	Si
S_5	*ACCEPT*	In	*	*	198.51.100/24	22	TCP	*
S_6	*ACCEPT*	Out	198.51.100/24	22	*	*	TCP	Si
M_1	*ACCEPT*	Out	198.51.100.4	>1023	*	25	TCP	*
M_2	*ACCEPT*	In	*	25	198.51.100.4	>1023	TCP	Si
M_3	*ACCEPT*	In	*	>1023	198.51.100.4	25	TCP	*
M_4	*ACCEPT*	Out	198.51.100.4	25	*	>1023	TCP	Si
D_1	*ACCEPT*	Out	198.51.100.5	53	*	53	UDP	-
D_2	*ACCEPT*	In	*	53	198.51.100.5	53	UDP	-
D_3	*ACCEPT*	In	*	*	198.51.100.5	53	UDP	-
D_4	*ACCEPT*	Out	198.51.100.5	53	*	*	UDP	-
D_5	*ACCEPT*	Out	198.51.100.5	>1023	*	53	TCP	*
D_6	*ACCEPT*	In	*	53	198.51.100.5	>1023	TCP	Sí
D_7	*ACCEPT*	In	*	>1023	198.51.100.5	53	TCP	*
D_8	*ACCEPT*	Out	198.51.100.5	53	*	>1023	TCP	Sí
F_1	*DENY*	Out	*	*	*	*	*	*
F_2	*DENY*	In	*	*	*	*	*	*

- H_1, H_2: permeten la sortida i l'entrada posterior de trànsit TCP de l'equip bastió que fa de passarel·la HTTP, cap a qualsevol servidor d'Internet en qualsevol port. Això permet connexions a servidors web en ports 80 (HTTP) i 443 (HTTPS) i a ports no estàndard. Són unes regles molt laxes en relació amb la restricció del port. Aquest tipus de laxitud és relativament normal en un encaminador exterior, com es va discutir en el subapartat 3.2. Com a mesura addicional, només es permet l'establiment de connexions cap a l'exterior, ja que la regla d'entrada requereix que el segment tingui el *flag* ACK actiu, és a dir, es descartarà si es tracta d'un inici de sessió (primer segment SYN de l'establiment de connexió TCP).

- H_3, H_4: permeten l'entrada de trànsit TCP a l'equip bastió que fa de servidor web. Només es permet l'accés al port 80 i només es permet l'establiment de connexió des de fora cap a dins (ACK).

- S_1, S_2, S_3, S_4: equivalents a les regles respectives en l'encaminador interior.

- S_5, S_6: permeten connexions SSH des de l'exterior a la xarxa perimetral per a administrar remotament els equips bastió.

- M_1, M_2: connexions SMTP des de l'equip bastió cap a Internet.

- M_3, M_4: connexions SMTP des d'Internet cap a l'equip bastió.

- D_1: peticions i respostes UDP des del servidor DNS de l'equip bastió a servidors d'Internet.

- D_2: peticions i respostes UDP des de servidors d'Internet al servidor de l'equip bastió.

- D_3, D_4: permet a clients DNS d'Internet preguntar al servidor de l'equip bastió i rebre'n les respostes. En aquest cas, la regla D_3 fa que la regla D_2 sigui redundant; s'ha inclòs la D_2 a tall il·lustratiu (amb tot, no és mala pràctica permetre aquesta redundància amb el propòsit de facilitar l'administració i lectura de les regles de filtratge).

- D_5, D_6: peticions del servidor de l'equip bastió a servidors d'Internet (i les seves respostes respectives). També permet transferència de zona.

- D_7, D_8: equivalents a les anteriors, però intercanviant els servidors.

5. Més enllà del filtratge de paquets

Avui dia els sistemes tallafoc realitzen força tasques que van més lluny del mer filtratge de paquets. Exemple d'això són la creació de xarxes privades virtuals o de NAT. També incorporen tècniques addicionals de seguretat, com ara *port knocking*. En aquest apartat repassem ràpidament aquests conceptes.

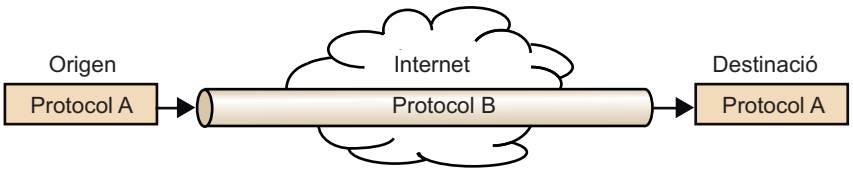
5.1. Túnels i xarxes privades virtuals

En molts casos en què s'opta per l'ús de sistemes tallafoc molt restrictius ens trobem amb la necessitat d'establir connexions segures entre punts concrets d'Internet que puguin saltar-se les regles del tallafoc. Aquí entra en joc el concepte de *túnel*.

Un **túnel** és l'encapsulació d'un protocol en un altre, i es pot veure com un cable virtual que enllaça dos punts d'Internet.

Un túnel pot permetre saltar-se la regles d'un tallafoc, la qual cosa pot tenir aplicacions avantatjoses en alguns casos. En l'origen, un protocol s'encapsula en un altre que pot travessar qualsevol xarxa. En la destinació, el protocol original es pot desencapsular (figura 15).

Figura 15. Túnel



En principi, hi ha molts tipus de túnels que poden tenir com a propòsit saltar-se les regles d'un tallafoc. En l'exemple del subapartat 4.3.2. teníem un sistema tallafoc amb xarxa perimetral en el qual es permet la connexió SSH directa entre la xarxa interna i l'externa. Per això es permetia la connexió TCP al port 22 o cap al port 22. No obstant això, el trànsit HTTP havia de passar per la passarel·la d'apliació situada a la xarxa perimetral.

Davant d'aquesta situació, un usuari malintencionat podria establir un túnel TCP pel port 22 entre el seu equip de la xarxa interna i un equip exterior.

És a dir, encapsular en TCP qualsevol protocol i dirigir-lo al port 22. Si ho fa adequadament, podria per exemple accedir a servidors externs HTTP des de l'interior sense necessitat d'utilitzar la passarel·la HTTP i saltar-se així la política del sistema i el filtratge que realitzaria la passarel·la. En aquest cas podria, fins i tot, encapsular HTTP en SSH i establir-hi un túnel SSH. No solament és molt senzill fer-ho, ja que la majoria de les implementacions actuals d'SSH incorporen aquesta funcionalitat directament, sinó que a més el trànsit aniria xifrat. El protocol encapsulat no seria detectable per cap tipus de filtratge pel qual passés el túnel.

Actualment hi ha molts tipus de túnels i possibilitats d'encapsulament, sobre DNS, HTTP, FTP, etc. Aquest tipus de túnels es pot emprar per a violar la política implementada per un tallafocs. Per aquest motiu es considera que és molt difícil protegir una xarxa dels seus usuaris interns mitjançant sistemes tallafoc. En general, un tallafoc ens permet protegir una xarxa davant d'una amenaça externa, però no d'una interna.

Lectura complementària

Com a curiositat, l'RFC 1149 defineix l'encapsulament d'IP en coloms missatgers.

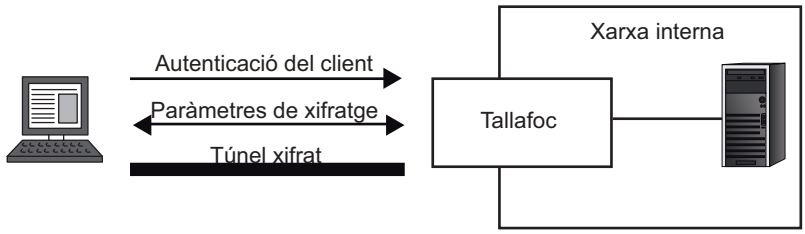
Malgrat els seus possibles usos maliciosos, els túnels poden tenir aplicacions positives. Es poden utilitzar per a unir dues xarxes separades per una xarxa hostil, com Internet. Cada xarxa està fortament protegida amb un sistema tallafoc i el túnel permet unir-les com si hi hagués un enllaç físic entre elles. En aquest cas, és convenient que el trànsit del túnel estigui xifrat. Aquest tipus de túnels sol rebre el nom de *xarxa privada virtual*.

Una xarxa privada virtual (VPN, *Virtual Private Network*) és una xarxa privada que interconnecta punts o xarxes remotes a través de xarxes públiques com Internet.

Una VPN utilitza túnels xifrats i mecanismes d'autenticació per a garantir la seguretat de la xarxa virtual. Els usuaris de la VPN tenen la sensació d'estar en una xarxa privada quan, en realitat, estan separats per una xarxa pública. Hi ha molts tipus de VPN, els quals poden utilitzar molts tipus de protocols per a establir el túnel a diferents nivells de xarxa. És comú l'ús de protocols genèrics com IPSec o SSL/TLS per sí sols o en combinació amb protocols més específics, com ara *Layer 2 Tunneling Protocol* (L2TP), que encapsula IP sobre protocols que suporten lliurament punt-a-punt, com IP, ATM o Frame Relay.

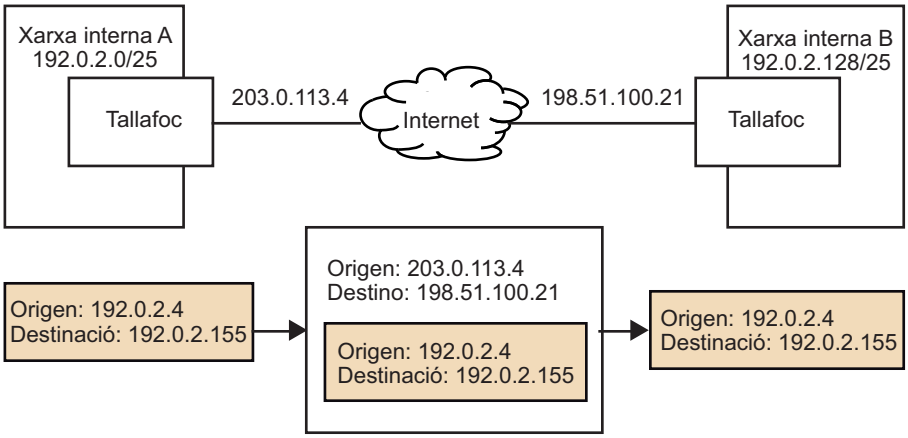
A més del tipus de túnel utilitzat, una VPN pot proporcionar diversos serveis. Generalment, una VPN es pot configurar, per exemple, per a permetre que els empleats de l'empresa accedeixin a la xarxa corporativa des de casa, per mitjà d'Internet. L'usuari s'autentica i s'estableix un túnel xifrat (després d'establir o negociar els paràmetres necessaris) entre el client que té l'usuari i la xarxa interna de l'empresa (figura 16).

Figura 16. VPN per a la connexió d'un client



Una altra possibilitat, també força comuna, consisteix a unir amb un túnel dues xarxes separades geogràficament, i per una xarxa pública. En aquest cas, l'objectiu és que es tingui la percepció que les dues xarxes són una de sola. Aquest tipus de VPN se sol anomenar *branch office*. La figura 17 mostra un exemple molt simplificat en què els datagrames IP s'encapsulen per a passar per Internet.

Figura 17. VPN per a la connexió de dues xarxes corporatives



5.2. *Port knocking*

Port knocking és una tècnica que va aparèixer l'any 2003 com un mecanisme d'autenticació davant d'un tallafoc.

Port knocking permet la comunicació autèntica de dades a través d'un sistema tallafoc amb els ports tancats. O, dit d'altra manera, permet oferir un servei per un tallafoc que té els ports tancats per defecte.

Lectura recomanada

La primera publicació que fa referència a la tècnica del copejament de ports és la següent: M. Krzywinski (2003). "Port Knocking: Network Authentication Across Closed Ports". *SysAdmin Magazine* (núm. 12, p. 12-17).

La idea consisteix a oferir un servei protegit per un tallafoc que no permet el pas de cap paquet, és a dir, que té tots els ports tancats. El client realitza una sèrie d'intents de connexió a una seqüència de ports concreta. Si aquesta seqüència és la correcta, el sistema tallafoc obrirà el port que permetrà al client accedir al servei protegit. Un intent de connexió pot ser, per exemple, l'enviament d'un segment de sincronització de TCP (SYN) amb el propòsit d'i-

niciar una connexió. La seqüència de ports és la clau (compartida pel client i el servidor) que permetrà que el client s'autentiqui.

Per a detectar la seqüència de ports, els sistemes de *port knocking* poden monitorar els fitxers de registre del sistema tallafoc o, simplement, capturar paquets abans que arribin al tallafoc. Actualment també hi ha sistemes tallafoc, com ara Netfilter/iptables, que incorporen suport per a *port knocking*.

Knockd

Knockd és un servidor de *port knocking* que analitza el trànsit en la de capa d'enllaç per a detectar seqüències de ports. Aquestes seqüències es poden fer mitjançant l'enviament de paquets TCP o UDP als ports corresponents. Knockd està disponible per a Linux, Window i OSX a zeroflux.org.

La versió bàsica de *port knocking*, i la més comuna, estableix una seqüència de ports compartida entre el servidor i el client com a clau. Tanmateix, actualment hi ha modalitats més sofisticades. Un cas més extrem consisteix a xifrar informació de la connexió desitjada: IP d'origen, port, etc., amb un xifratge simètric. Aquesta informació xifrada es pot dividir en bytes: cada byte s'interpreta com un nombre decimal (de 0 a 255) i a cada número se li suma, per exemple, 24000. Al final tenim una seqüència de nombres en el rang de 24000 a 24255 que serà la seqüència de ports utilitzada. El servidor rep la seqüència i la pot desxifrar, i així obté la IP d'origen*, el port i el servei que ha de facilitar al client. En aquest cas, cal que el client i el servidor comparteixin una clau simètrica, però el mètode és molt més segur que el mode bàsic, ja que pot evitar atacs de repetició. En l'exemple anterior estem enviant un byte d'informació amb cada paquet. Atès que el port són 16 bits, es podrien enviar un màxim de 2 bytes.

*** L'adreça IP dels paquets que fan el *port knocking* acostuma a ser falsa per a evitar possibles espies.**

Hi ha una variant de *port knocking*, coneguda com *single packet authorization* (SPA), que permet fer l'autenticació amb un sol paquet. La idea és enviar un paquet que contingui com a dades la informació d'autenticació xifrada. Aquesta variació aconsegueix enviar la informació en un sol paquet.

fwknop

fwknop (*FireWall KNock OPerator*) és un servidor disponible per a Linux, BSD i OSX que permet implementar *port knocking* i SPA.

L'ús d'aquestes tècniques afegeix un grau de seguretat defensiva al sistema que ja estava protegit pel sistema tallafoc. El fet que el tallafoc estigui tancat totalment per defecte pot evitar, per exemple, molts problemes derivats de vulnerabilitats de dia-zero. En el camp de la seguretat informàtica s'utilitza el principi de *defense in depth* (defensa en profunditat), el qual ve a dir que la superposició de múltiples mecanismes defensius millora la seguretat d'un sistema.

5.3. Ús de NAT

NAT (*Network Address Translation*) permet usar internament, en una xarxa, un conjunt d'adreces i, per a l'exterior, unes adreces diferents. S'usa més freqüentment per a compartir una mateixa adreça IP pública entre diversos dispositius que internament utilitzen adreces privades.

El funcionament dels dispositius NAT té moltes similituds amb el dels sistemes tallafoc, fins al punt que molts sistemes tallafoc poden realitzar també NAT. És el cas de Netfilter/iptables, per exemple.

L'ús de NAT pot tenir avantatges addicionals des del punt de vista de la seguretat i els sistemes tallafoc:

- En assignar adreces IP privades a dispositius de la xarxa, ens assegurem que aquestes es comuniquin amb l'exterior per mitjà del dispositiu NAT, el qual pot estar fent també funcions de tallafoc. Si un equip intern intenta saltar-se el tallafoc, no podrà fer-ho amb la seva adreça IP privada, ja que no es pot encaminar a Internet.

- Ajuda a limitar el trànsit d'entrada. Depenent del tipus de NAT que s'estigui fent, aquest deixarà passar només el trànsit d'entrada que formi part d'una comunicació iniciada des de l'interior.

- També pot ajudar a ocultar informació sobre la xarxa interna a possibles atacants externs.

Aquestes són indicacions generals, ja que en funció de quin tipus de NAT s'utilitzi tindrem més avantatges o desavantatges. Per exemple, es pot fer NAT amb el mapeig de ports (d'adreces internes); aquest tipus de NAT pot, en alguns casos, interferir amb el sistema de filtratge, ja que per exemple es modifica el port d'origen del datagrama.

Resum

Un sistema tallafoc permet establir una barrera de seguretat entre xarxes informàtiques. Amb tallafocs podem protegir una xarxa, o part d'aquesta, dels entorns hostils que siguin una possible font d'atacs. Hi ha diverses tecnologies i arquitectures de sistemes tallafoc, i cadascuna té la seva aplicabilitat, amb avantatges i desavantatges.

Els tallafocs controlen el flux de xarxa en filtrar els paquets que hi passen. Aquest filtratge pot tenir diversos graus de complexitat i, conseqüentment, d'eficiència. Des d'un filtratge senzill en què només es considera informació de les capçaleres dels protocols principals, fins a sistemes sofisticats de filtratge continu de continguts.

Activitats

1. Els codis 9 i 10 es van afegir especialment a l'especificació d'ICMP per a utilitzar-los amb sistemes de filtratge. Tot i així, molts segueixen utilitzant els codis 0 i 1 que inicialment es van pensar per a altres propòsits. Per què creieu que es van haver d'introduir els codis nous? Quines contraindicacions pot tenir l'ús dels codis 0 i 1?

2. Hi ha un sistema de filtratge de grans dimensions a Internet conegut com a *The Great Firewall of China*. Busqueu informació sobre aquest sistema. Què és i quin és el seu propòsit? Com aconsegueix aquest sistema bloquejar el trànsit? O, dit d'altra manera, com rebutja paquets? Com es pot evitar?

Pista: podeu consultar l'article següent: R. Clayton; S. J. Murdoch; R. N. M. Watson (2006). "Ignoring the Great Firewall of China" (en línia). A: *6th Workshop on Privacy Enhancing Technologies*.

3. En aquest mòdul es comenta que hi ha sistemes tallafoc, com Netfilter/iptables, que incorporen *port knocking*. Definiu el conjunt de regles d'iptables que necessiteu per a definir un *port knocking* que obri el port 23 si es rep la seqüència de ports *port knocking*: 1000, 2314, 4132, 2222.

4. En aquest mòdul es comenta que la modalitat de xifratge de *port knocking* pot evitar atacs de repetició. En què consisteixen aquests atacs en el context de *port knocking*? Fins a quin punt el xifratge evita aquests atacs? SPA també és vulnerable a atacs de repetició?

Glossari

adreça IP *f* Adreça utilitzada pel protocol IP.

amenaça *f* Violació potencial de la seguretat, que existeix sobre la base d'unes circumstàncies, capacitats, accions o esdeveniments que puguin arribar a causar una infracció de la seguretat o causar algun dany en el sistema.

atac *m* Agressió a la seguretat d'un sistema fruit d'un acte intencionat i deliberat que viola la política de seguretat d'aquest sistema.

bastion host *m* Vegeu **equip bastió**.

DNS *m* Vegeu ***domain name system***.

domain name system *m* Sistema de noms, jeràrquic i distribuït, que permet associar noms de domini a adreces IP.
sigla **DNS**

equip bastió *m* Sistema informàtic que ha estat fortament protegit per a suportar atacs des d'un lloc hostil.
en **bastion host**

equip *dual-homed* *m* Equip amb almenys dues interfícies de xarxa, cadascuna associada a una xarxa, que pot actuar com a encaminador entre les xarxes.

ICMP *m* Vegeu ***internet control message protocol***.

internet control message protocol *m* Protocol de control, principalment per a enviar missatges d'error, de TCP/IP.
sigla **ICMP**

internet protocol *m* Protocol per a interconnectar xarxes.
sigla **IP**

IP *m* Vegeu ***internet protocol***.

passarel·la en el nivell de circuit *f* Dispositiu que fa de passarel·la en el nivell de la capa de transport entre dos extrems. Estableix una connexió amb cadascuna i retransmet les dades entre les dues connexions.

política de seguretat *f* Conjunt de regles i pràctiques que defineixen i regulen els serveis de seguretat d'una organització o sistema amb el propòsit de protegir els seus recursos crítics i sensibles. En altres paraules, és la declaració de què està permès fer i què no ho està.

port knocking Tècnica que permet la comunicació autèntica de dades a través d'un sistema tallafoc amb els ports tancats.

TCP *m* Vegeu **transmission control protocol**.

transmission control protocol *m* Protocol de transport (extrem-a-extrem) de TCP/IP.
sigla **TCP**

túnel *m* Encapsulació d'un protocol en un altre. Es pot considerar com un cable virtual que enllaça dos punts d'Internet.

UDP *m* Vegeu ***user datagram protocol***.

user datagram protocol *m* Protocol de transport (extrem-a-extrem) de TCP/IP.
sigla **UDP**

virtual private network *f* Vegeu **xarxa privada virtual**.

VPN *f* Vegeu **xarxa privada virtual**.

xarxa privada virtual *f* Xarxa privada que interconnecta punts o xarxes remotes a través de xarxes públiques com Internet.
sigla **VPN**
en **virtual private network**

vulnerabilitat de dia zero *f* Vulnerabilitat que, en el moment de ser explotada, no se'n té coneixement previ de l'existència.
en **zero-day vulnerability**

vulnerabilitat de seguretat Fallada o debilitat en el disseny, la implementació, l'operació o la gestió d'un sistema, que pot ser explotada per tal de violar la seva política de seguretat.

zero-day vulnerability *f* Vegeu **vulnerabilitat de dia zero**.

Bibliografia

Avolio, Frederic (1999). "Firewalls and Internet Security, the Second Hundred (Internet) Years". *The Internet Protocol Journal* (vol. 2, núm. 2).

Cheswick, William R.; Bellovin, Steven M.; Rubin, Aviel D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (2a ed.). Boston, Massachusetts: Addison-Wesley Professional Computing.

Fraser, B. (1997). *Site Security Handbook*. RFC 2196, IETF. The Internet Society.

García Alfaro, Joaquín (2004). "Mecanismos de prevención". A: Herrera Joancomartí, Jordi (coord.); García Alfaro, Joaquín; Perramón Tornil, Xavier. *Seguridad en redes de computadores*. Barcelona: Fundació Universitat Oberta de Catalunya, 287 pàg.

Microsoft (2010). "Windows Firewall with Advanced Security Getting Started Guide" (en línia). Microsoft TechNet Library.

Rash, Michael (2007). *Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort*. San Francisco, Califòrnia: No Starch Press.

Shirey, R. (2000). *Internet Security Glossary* RFC 2828, IETF. The Internet Society

Zwicky, Elizabeth D.; Cooper, Simon; Chapman, D. Brent (2000). *Building Internet Firewalls* (2a ed.). Sebastopol, Califòrnia: O'Reilly Media.