Mecanismes de prevenció

Joaquín García Alfaro

P07/05070/02623

UOC
Universitat Oberta de Catalunya

Índex

Introducció

Quan un equip és connectat a una xarxa de computadors, es poden identificar tres àrees de risc:

Primer, el nombre de punts que poden ser utilitzats com a origen per a realitzar un atac contra qualsevol component de la xarxa s'incrementa. En un sistema aïllat (sense connexió), un requisit necessari per ser atacat és forçosament l'existència d'un accés físic cap a l'equip. Però en el cas d'un sistema en xarxa, cadascun dels equips que pugui enviar informació cap a la víctima podrà ser utilitzat per un possible atacant.

Alguns serveis (com per exemple web i dns) necessiten estar oberts públicament, de forma que qualsevol equip connectat a Internet podria ser l'origen d'una possible activitat maliciosa contra ells. Això fa que sigui molt probable l'existència d'atacs regulars contra aquests sistemes.

La segona àrea de risc inclou l'expansió del perímetre físic del sistema telemàtic al qual l'equip acaba de ser connectat. Quan la màquina està aïllada, qualsevol activitat pot ser considerada com a interna a l'equip (i per tant, de confiança). El processador treballa amb les dades que troba a la memòria, que alhora han estat carregades des d'un mitjà d'emmagatzemament secundari. Aquestes dades estan realment ben protegides contra actes de modificació, eliminació, observació maliciosa ... en ser transferides entre diferents components de confiança.

Però aquesta mateixa premissa no és certa quan les dades són transferides a través d'una xarxa. La informació transmesa pel mitjà de comunicació és reenviada per dispositius que estan totalment fora del control del receptor. Aquesta informació podria ser llegida, emmagatzemada, modificada i més tard retransmesa cap al receptor legítim. Especialment en grans xarxes com Internet, no és trivial l'autenticació de l'origen que es presenta com l'emissor d'un missatge.

Finalment, la tercera àrea de risc es deu a l'augment en el nombre de serveis d'autenticació (generalment un servei de Login-Password) que un sistema connectat a una xarxa ha d'oferir, respecte a un sistema aïllat. Aquests serveis no deixen de ser simples aplicacions (amb possibles errors de programació o de disseny) que protegeixen l'accés cap als recursos dels equips del sistema. Un error o vulnerabilitat en alguns d'aquests serveis pot suposar el compromís del sistema al complet.

La prevenció d'atacs és la suma d'una sèrie de mecanismes de seguretat que proporcionen un primer nivell de defensa contra cert tipus d'atacs abans que aquests arribin al seu objectiu.

Objectius

Els objectius a assolir amb l'estudi d'aquest mòdul són:

1. Entendre el funcionament de les tecnologies tallafoc.

2. Veure els diferents mètodes existents per al filtratge de la informació.

3. Comprendre les diferents possibilitats de configuració dels sistemes tallafoc.

1. Sistemes tallafoc

Els sistemes tallafoc* són un mecanisme de control d'accés sobre la capa de xarxa. La idea bàsica és separar la nostra xarxa (on els equips que intervenen són de confiança) dels equips de l'exterior (potencialment hostils).

*** En anglès, *firewall*.**

Un sistema tallafoc actua com una barrera central per reforçar el control d'accés als serveis que s'executen tant a l'interior com a l'exterior de la xarxa. El tallafoc intentarà prevenir els atacs de l'exterior contra les màquines internes de la nostra xarxa denegant peticions de connexió des de parts no autoritzades.

Un tallafoc pot ser qualsevol dispositiu utilitzat com a mecanisme de control d'accés a nivell de xarxa per protegir una xarxa en particular o un conjunt de xarxes. En la majoria dels casos, els sistemes tallafoc s'utilitzen per prevenir accessos il·lícits a l'interior de la xarxa.

Un tallafoc és aquell sistema de xarxa expressament encarregat de separar xarxes de computadors, efectuant un control del trànsit existent entre elles. 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 TCP/IP.

A l'hora d'instal·lar i configurar un sistema tallafoc a la nostra xarxa, s'ha de tenir present el següent:

1) Tot el trànsit que surt de l'interior cap a l'exterior de la xarxa a protegir, i viceversa, ha de passar pel tallafoc. Això es pot aconseguir bloquejant físicament tot l'accés a l'interior de la xarxa a través del sistema.

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

3) El propi tallafoc ha d'estar protegit contra possibles intrusions. Això implica l'ús d'un sistema operatiu de confiança amb suficients garanties de seguretat.

2. Construcció de sistemes tallafoc

En el sentit més general, un sistema tallafoc consta de programari i maquinari. El programari pot ser propietari, *shareware*, o *freeware*. Per altra banda, el maquinari podrà ser qualsevol que pugui suportar aquest programari.

Actualment, tres de les tecnologies més utilitzades a l'hora de construir sistemes tallafoc són les següents:

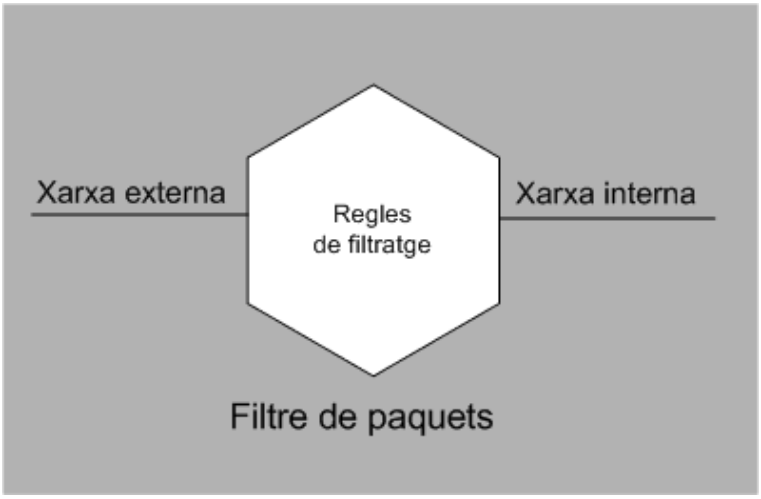
- Encaminadors amb filtratge de paquets.
- Passarel·les a nivell d'aplicació.
- Passarel·les a nivell de circuit.

A continuació estudiarem amb més detall cadascuna d'aquestes categories.

2.1. Encaminadors amb filtratge de paquets

Es tracta d'un dispositiu que encamina el trànsit TCP/IP (encaminador* de TCP/IP) sobre la base d'una sèrie de regles de filtratge que decideixen quins paquets s'encaminen a través seu i quins són descartats.

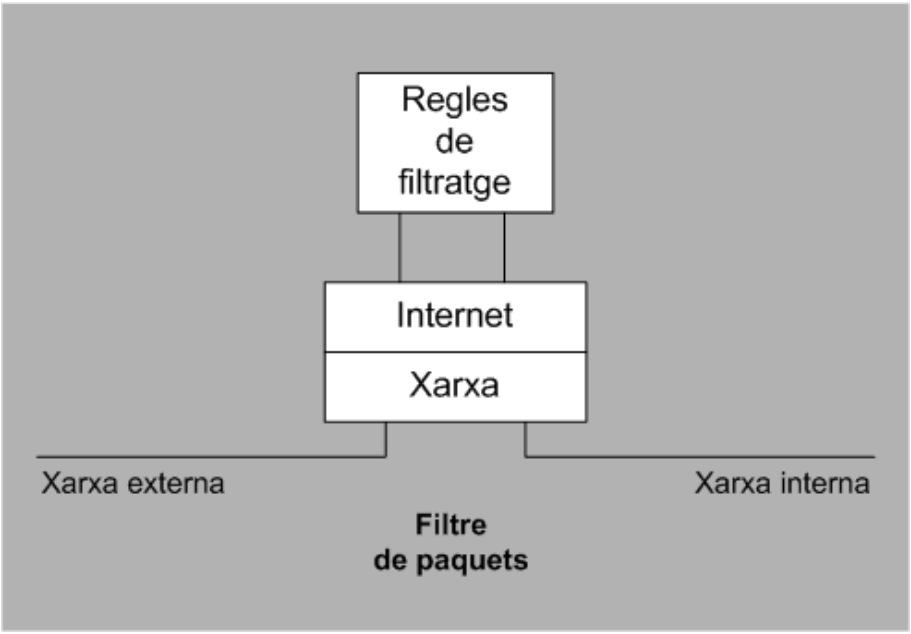
*** En anglès, *router*.**



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, verificant el trànsit de dades legítim entre ambdues parts.

Els encaminadors amb filtratge de paquets, en treballar a nivell de xarxa, poden acceptar o denegar paquets fixant-se en les capçaleres del protocol (tant IP, com UDP, TCP ...), com poden ser:

- Adreces d'origen i de destí.
- Tipus de protocol i indicadors especials.
- Ports d'origen i de destí o tipus de missatge (segons el protocol).
- Contingut dels paquets.
- Mida del paquet.



Les regles estan organitzades en conjunts de llistes amb una determinada política per defecte (denegar-ho tot, acceptar-ho tot ...).

Cada paquet que arribi al dispositiu serà comparat amb les regles, començant pel principi de la llista fins que es trobi la primera coincidència. Si existeix alguna coincidència, l'acció indicada a la regla serà activada (denegar, acceptar, redirigir ...).

Per contra, si no és possible cap coincidència, serà consultada la política per defecte per saber quina acció prendre (deixar passar el paquet, descartar-lo, redireccionar-lo, etc). Si es tracta, per exemple, d'una política de denegació per defecte, en cas de no existir cap coincidència amb el paquet, aquest serà descartat.

Una política de denegació per defecte acostuma a ser més costosa de mantenir, ja que serà necessari que l'administrador indiqui explícitament tots els serveis que han de romandre oberts (la resta, per defecte, seran tots denegats).

En canvi, una política d'acceptació per defecte és més senzilla d'administrar, però incrementa el risc de permetre atacs contra la nostra xarxa ja que requereix que l'administrador indiqui explícitament quins paquets cal descartar (la resta, per defecte, seran tots acceptats).

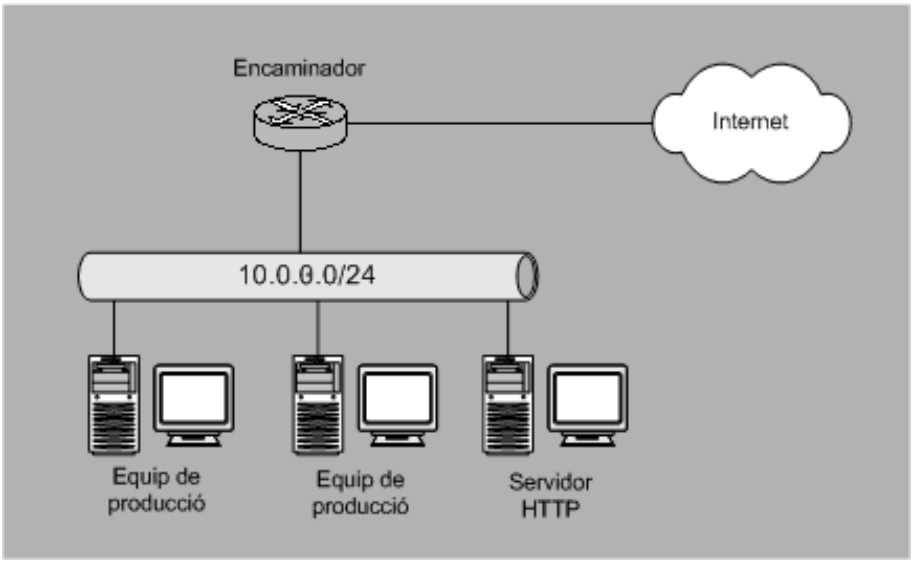
Exemples de configuració

En la figura següent es presenta una possible xarxa a on s'ha implantat la següent política de seguretat mitjançant la configuració d'un conjunt de regles de filtre de paquets aplicades en el mateix encaminador:

- Tots els sistemes de la xarxa interna 10.0.0.0 poden accedir a qualsevol servei TCP de la xarxa Internet.

- El trànsit ICMP només és permès de sortida, no d'entrada (per tal d'evitar l'extracció d'informació mitjançant aquest protocol).

- Els sistemes externs no es poden connectar a cap sistema intern excepte al servidor d'HTTP (10.0.0.1).

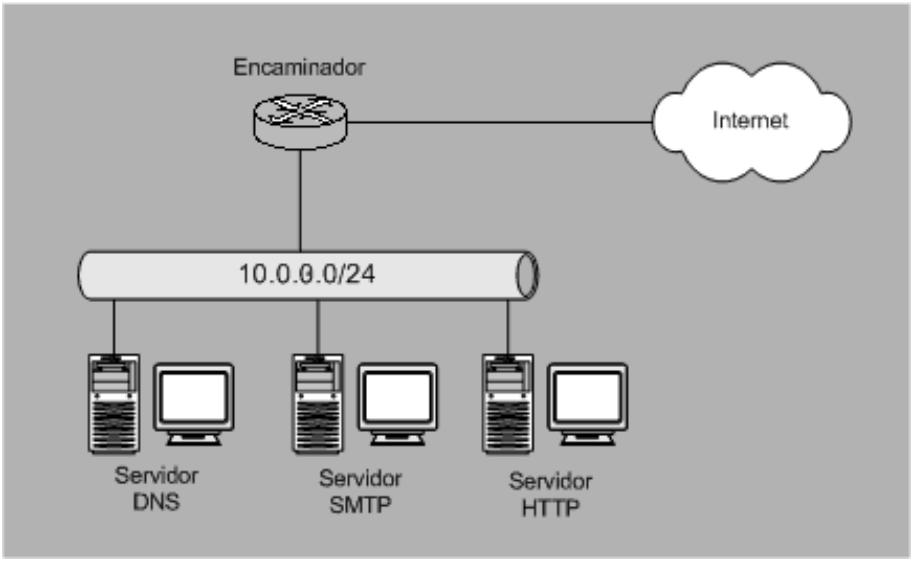


Les regles de filtratge configurades a l'encaminador corresponen a la següent taula:

Regla	Acció	Origen	Port d'origen	Destinació	Port de destinació	Indicador	Descripció
1	Permet	10.0.0.0	*	*	*	TCP	Permet connexions TCP sortints
2	Permet	*	*	10.0.0.1	80	TCP	Permet connexions HTTP entrants
3	Rebutja	*	*	10.0.0.0	*	*	Rebutja qualsevol altra connexió a la xarxa interna

Com a segon exemple, podem pensar en la mateixa xarxa, però amb la següent política de seguretat:

- Tots els sistemes de la xarxa interna 10.0.0.0 poden accedir a qualsevol servei TCP de la xarxa Internet, exceptuant HTTP.
- S'han d'autoritzar accessos al servidor DNS (10.0.0.3).
- Els sistemes externs no poden connectar a cap sistema intern excepte al servidor d'HTTP (10.0.0.1) i SMTP (10.0.0.2).



Les regles de filtratge d'aquest segon exemple podrien correspondre a les expressades en la taula següent:

Regla	Acció	Origen	Port d'origen	Destinació	Port de destinació	Indicador	Descripció
1	Rebutja	10.0.0.0	*	*	80	TCP	Rebutja qualsevol connexió a servidors HTTP
2	Permet	10.0.0.0	*	*	*	TCP	Permet connexions TCP sortints
3	Permet	*	*	10.0.0.1	80	TCP	Permet connexions HTTP entrants
4	Permet	*	*	10.0.0.2	25	TCP	Permet connexions SMTP entrants
5	Permet	*	*	10.0.0.3	53	UDP	Permet connexions DNS entrants
6	Rebutja	*	*	10.0.0.0	*	*	Rebutja qualsevol altra connexió a la xarxa interna

Avantatges i desavantatges dels encaminadors amb filtratge de paquets

La construcció d'un sistema tallafoc mitjançant un encaminador amb filtratge de paquets és realment econòmica, ja que generalment se sol fer amb maquinari ja disponible. A més, ofereix un alt rendiment a xarxes amb una càrrega de trànsit elevada. Un exemple d'encaminador amb filtre de paquets podria ser l'aplicatiu `iptables`, implementat com una part del programari d'encaminament del kernel Linux 2.4.

Addicionalment, aquesta tecnologia permet la implantació de la major part de les polítiques de seguretat necessàries.

Les **polítiques de seguretat** són el resultat de documentar les expectatives de seguretat, intentant plasmar en el món real els conceptes abstractes de seguretat. Poden ser definides de manera processal (plasmant de forma pràctica les idees o filosofies de l'empresa quant a seguretat) o de manera formal (utilitzant un model matemàtic que intenta abastar tots els possibles estats i operacions).

Tot i aquests avantatges, els encaminadors de xarxa amb filtratge de paquets poden presentar algunes deficiències, com per exemple:

- Molts dels encaminadors utilitzats poden ser vulnerables a atacs existents (tot i que la majoria dels distribuïdors tenen els corresponents paquets d'actualitzacions per solucionar-ho). Per altra banda, no solen tenir capacitats de registre*. Això provoca que a l'administrador li sigui difícil saber si el propi encaminador està sent atacat.

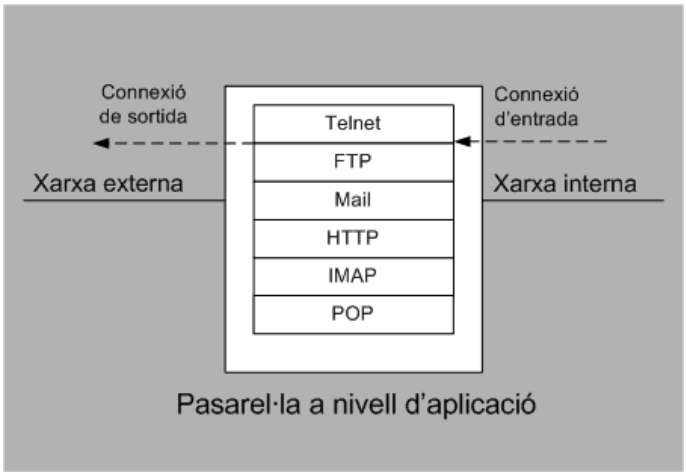
- La seva capacitat d'actuació pot arribar a deteriorar-se a causa de la utilització d'un filtratge excessivament estricte, dificultant també el procés de gestió del dispositiu si aquest nombre de regles arriba a ser molt elevat.

- Les regles de filtratge poden arribar a ser molt complicades, provocant en ocasions que possibles distraccions en la seva configuració siguin aprofitades per un atacant per realitzar una violació de la política de seguretat.

* En anglès, *logging*.

2.2. Passarel·les a nivell d'aplicació

Una passarel·la a nivell d'aplicació, coneguda també com a servidor intermediari (o en anglès *proxy*), no encamina paquets a nivell de xarxa sinó que actua com a retransmissor a nivell d'aplicació. Els usuaris de la xarxa contactaran amb el servidor intermediari, que al seu torn estarà oferint un servei *proxy* associat a una o més aplicacions determinades.

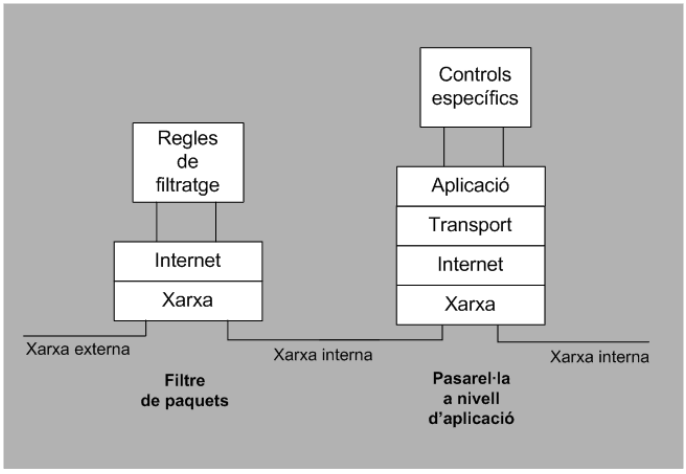


El servei proxy s'encarregarà de realitzar les connexions sol·licitades amb l'exterior i quan rebi una resposta, s'encarregarà de retransmetre-la cap a l'equip que havía iniciat la connexió. Així, el servei proxy executat a la passarel·la aplicarà les normes per decidir si s'accepta o es rebutja una petició de connexió.

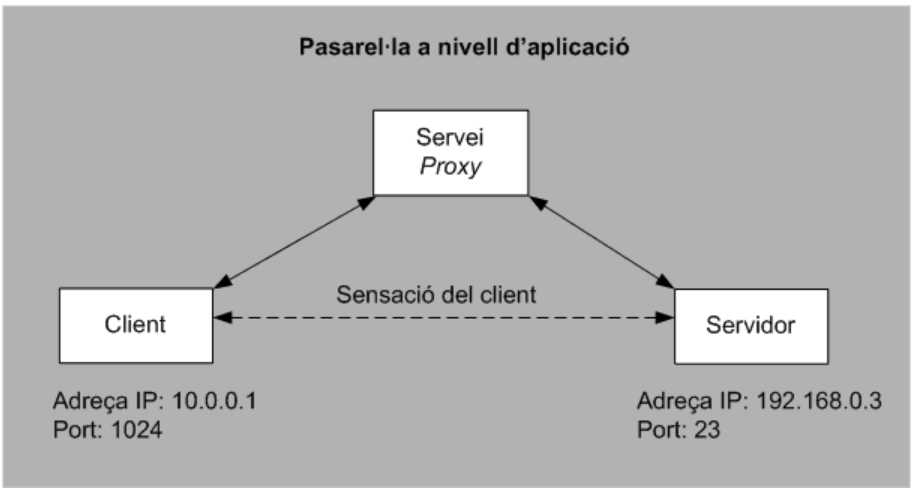
Una passarel·la separa completament l'interior de l'exterior de la xarxa a la capa d'enllaç, oferint únicament un conjunt de serveis a nivell d'aplicació. Això permet l'autenticació dels usuaris que realitzen peticions de connexió i l'anàlisi de connexions a nivell d'aplicació.

Aquestes dues característiques fan que les passarel·les ofereixin una major seguretat respecte als filtres de paquets, presentant un rang de possibilitats molt elevat. Per contra, la penalització introduïda per aquests dispositius és molt major. En cas d'una gran càrrega de trànsit en la xarxa, el rendiment pot arribar a reduir-se dràsticament.

A la pràctica, les passarel·les i els dispositius de xarxa amb filtratge de paquets són complementaris. Així, aquests dos sistemes es poden combinar proporcionant més seguretat i flexibilitat que si només se'n fes servir un, tal com es mostra en la figura següent:



Quan la passarel·la autentica el client, obre una connexió al servidor *proxy*, sent aquest el responsable de transmetre les dades que el client rep del servidor intermediari.



Aquest funcionament particular provoca que les pasarel·les a nivell d'aplicació presentin un rendiment inferior que als filtres de paquets. Per tal d'evitar-ho, els servidors intermediaris fan una còpia de les dades transmeses per a lliurar-les a un altre quan aquest les sol·liciti*.

L'ús de les passarel·les proporciona diversos beneficis. D'entrada, les passarel·les permeten només aquells serveis per als quals hi ha un servidor *proxy* habilitat. Així, si una passarel·la conté serveis intermediaris tan sols per als serveis HTTP i DNS, llavors només HTTP i DNS seran permesos en la xarxa interna. La resta de serveis seran completament rebutjats.

*** Sistemes coneguts com a *proxy cache*.**

Un altre benefici de l'ús de passarel·les és que el protocol també pot ser filtrat, prohibint així l'us de diferents subserveis dins d'un mateix servei permès. Per exemple, mitjançant una passarel·la que filtrés connexions FTP, seria possible prohibir únicament l'ús de l'ordre PUT d'FTP deixant habilitada la resta d'ordres. Aquesta característica no es possible obtenir-la mitjançant l'ús de només filtres de paquets.

Addicionalment, els servidors intermediaris també poden implantar el filtre de connexions per adreça IP de la mateixa manera que els filtres de paquets, ja que l'adreça IP està disponible en l'àmbit d'aplicació en el qual es farà el filtratge.

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

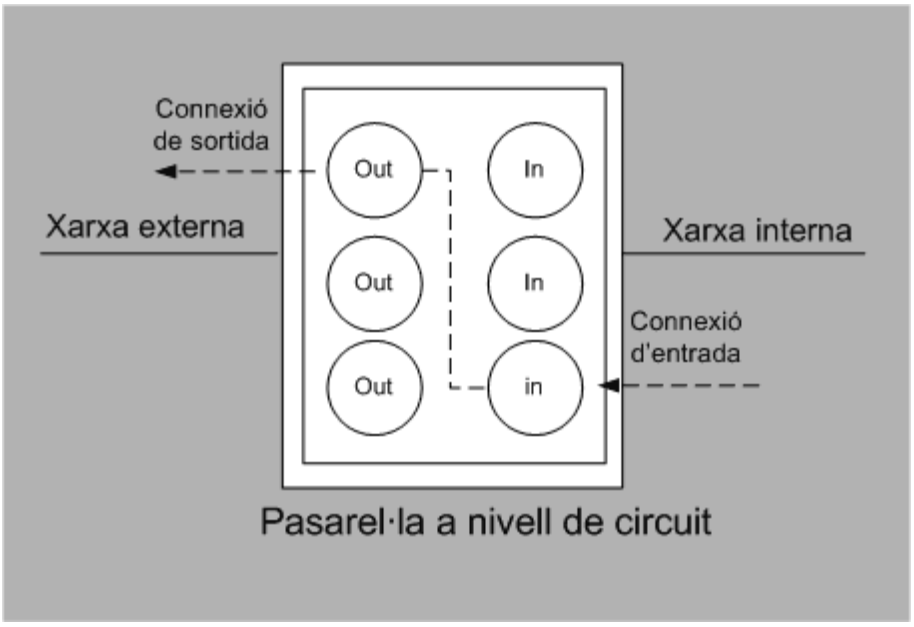
2.3. Passarel·les a nivell de circuit

Les passarel·les a nivell de circuit són un híbrid entre els esquemes de filtratge de paquets i els servidors intermediaris.

Una **passarel·la a nivell de circuit** és un dispositiu similar al de passarel·la a nivell d'aplicació, on l'usuari primer estableix una connexió amb el sistema tallafoc i aquest estableix la connexió amb l'equip de destí.

En contrast amb un servidor intermediari tradicional, una passarel·la a nivell de circuit opera de manera similar a un filtre de paquets a nivell de xarxa una vegada que la connexió ha estat inicialitzada.

Així, una vegada establerta la connexió, el dispositiu s'encarregarà de retransmetre tot el trànsit entre ambdues parts sense inspeccionar el contingut dels paquets a nivell d'aplicació tal com mostra la figura.



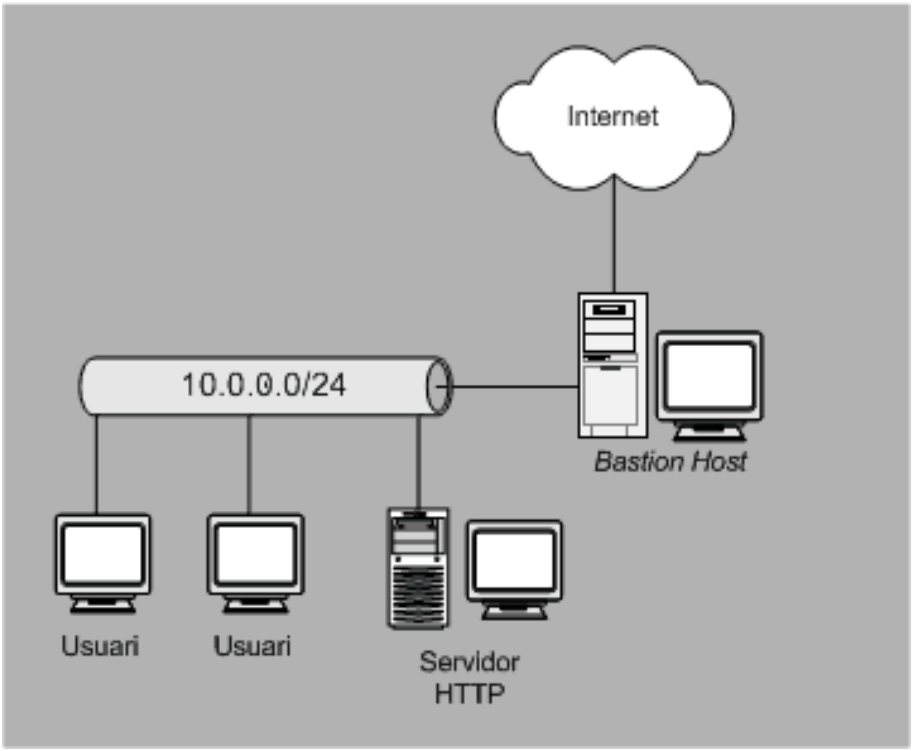
La funció de seguretat que ofereix aquest tipus de dispositiu consisteix a determinar quines connexions estan permeses, abans de bloquejar connexions cap a l'exterior.

Aquesta forma de treballar és molt més ràpida que un sistema tradicional, ja que les connexions poden ser restringides a nivell d'usuari sense necessitat d'analitzar tot el contingut dels paquets transmesos.

3. Zones desmilitaritzades

En certes instal·lacions, un únic dispositiu tallafoc no és suficient. Aquelles xarxes formades per múltiples servidors, accessibles públicament des de l'exterior, juntament amb estacions de treball que haurien d'estar completament aïllades de connexions de l'exterior, es beneficiaran de la separació entre dos grups de sistemes tallafoc.

Suposem, per exemple, la xarxa següent:



En aquesta figura podem veure que hi ha un únic sistema tallafoc com a punt de protecció, implantat mitjançant la utilització d'un equip bastió amb una arquitectura *dual-homed*.

Un **equip bastió** (en anglès *bastion host*) és un equip que ha estat fortament protegit per suportar els suposats atacs des d'un lloc hostil (en aquest cas Internet) i que actua com a punt de contacte entre l'interior i l'exterior d'una xarxa.

Bastion Host

El nom d'equip bastió prové de les muralles fortament protegides que separaven els castells medievals de l'exterior.

Una **arquitectura de tallafoc *dual-homed*** es construeix mitjançant l'ús d'un equip *dual-homed* amb la capacitat d'encaminament desactivada per tal que els paquets IP d'un extrem de la xarxa (la part hostil) no siguin encaminats cap a l'altra banda (la part protegida).

Equip *Dual-homed*

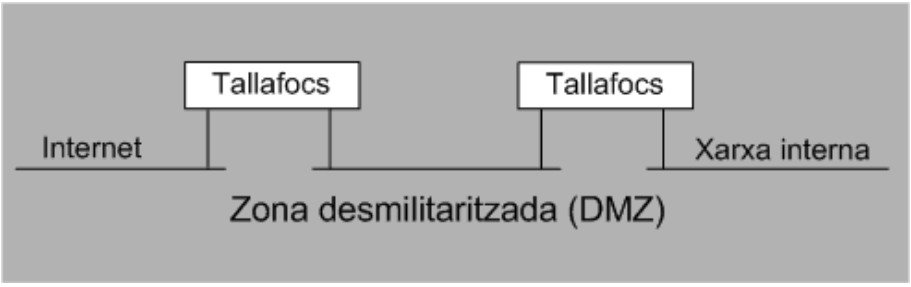
Es tracta d'un equip que té, almenys, dues interfíicies de xarxa (en anglès, *network interfaces* o *homes*).

D'aquesta forma, els equips de la xarxa interna poden comunicar-se amb l'equip *dual-homed*, els equips de la xarxa externa poden comunicar-se amb l'equip *dual-homed*, però els equips de la xarxa interna i externa no es poden posar en comunicació directament, sinó que un servidor intermediari s'encarrega de fer les connexions en nom d'aquestes dues parts.

Això fa que aquest tallafoc amb arquitectura *dual-homed* sigui un punt crític en la seguretat de la xarxa. Si un atacant aconsegueix comprometre qualsevol dels servidors que es troba al darrere d'aquest punt únic, totes les altres màquines podran ser atacades sense cap restricció des de l'equip que acaba de ser compromès.

Per prevenir aquestes situacions, és possible la utilització de dos dispositius tallafoc, introduint el concepte de zona desmilitaritzada o DMZ*.

*** En anglès, *Demilitaritzed Zone.***

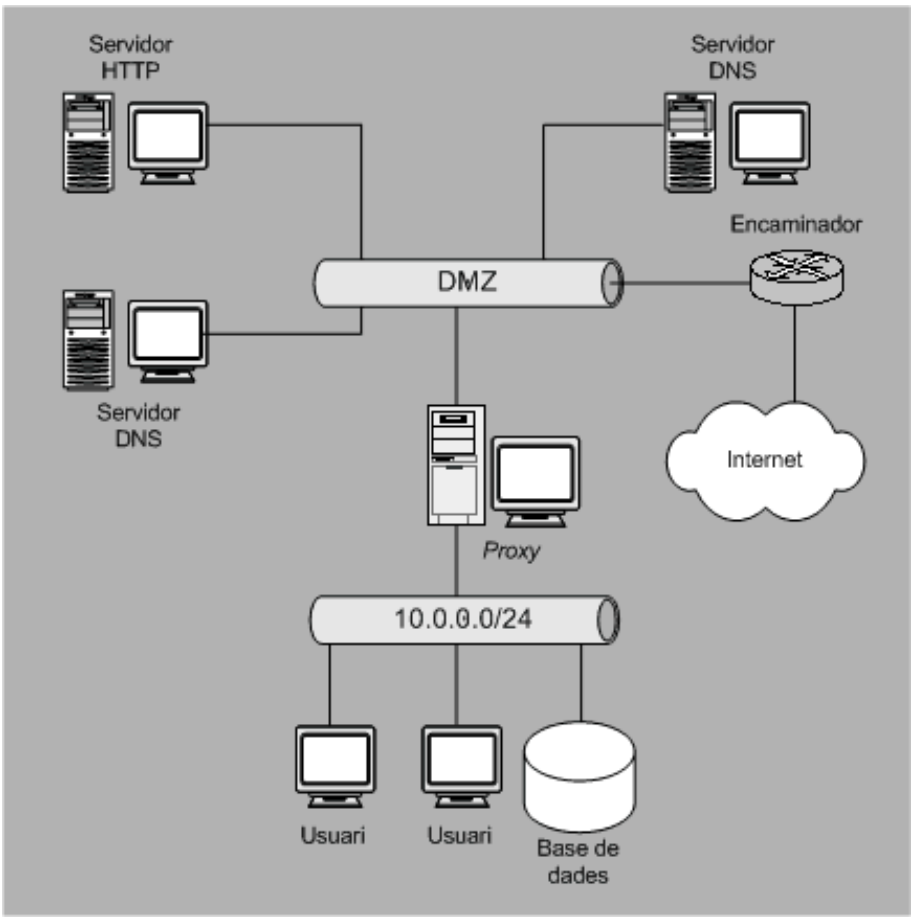


En la instal·lació mostrada a la figura anterior, un tallafoc separa l'exterior de la xarxa del segment desmilitaritzat (la DMZ) i els servidors que han de ser públics des de l'exterior de la xarxa. El segon tallafoc, que fa de punt de contacte entre la xarxa interna i la zona desmilitaritzada, serà configurat per tal que denegui tots els intents de connexió que hi arribin des de l'exterior.

Així, si un atacant aconsegueix introduir-se en un dels servidors de la zona desmilitaritzada, serà incapaç d'atacar immediatament una estació de treball. És dir, encara que un atacant s'apoderi del segment dels servidors, la resta de la xarxa continuarà estant protegida mitjançant el segon dels tallafocs.

Combinació de tecnologies per a la construcció d'una DMZ

A la figura següent podem veure l'ús d'un encaminador amb filtratge de paquets, juntament amb la utilització d'un servidor intermediari per a l'establiment d'una zona desmilitaritzada.



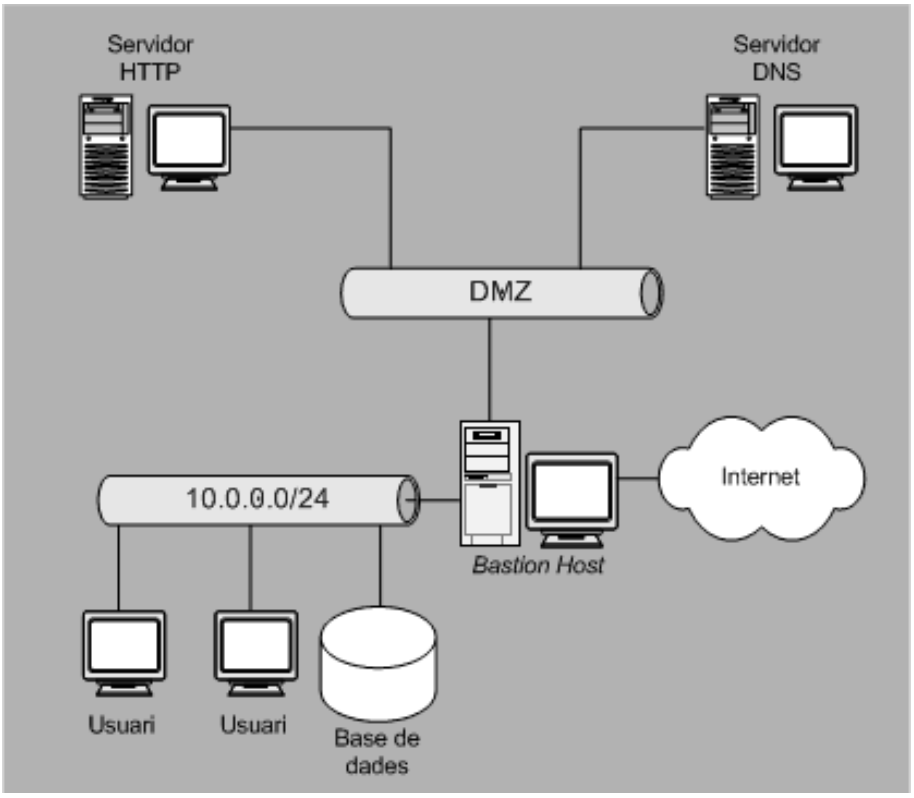
Una altra manera de solucionar els mateixos problemes plantejats consisteix en la utilització d'un sistema que implementi una inspecció d'estats en el filtre de paquets.

La **inspecció d'estats***, dissenyada per l'empresa de productes de seguretat *Chekpoint* i implementada inicialment en el producte *Firewall-1*, pretén combinar (igual que les pasarel·les a nivell de circuit) el rendiment dels filtres de paquets amb la seguretat addicional que presenta la utilització de servidors intermediaris.

*** En anglès, *Stateful Multi Layer Inspection.***

D'aquesta forma es pot simplificar l'esquema plantejat anteriorment i mantenir alhora un nivell de rendiment sense renunciar a les capacitats de monitoratge que ofereix la utilització d'un punt de protecció únic.

En la figura següent s'il·lustra la implantació d'un equip bastió amb arquitectura de tallafoc dual-homed i amb implantació d'inspecció d'estats.


Servidor
HTTP
Servidor
DNS
DMZ
10.0.0.0/24
Internet
Bastion Host
Usuari
Usuari
Base de
dades

4. Característiques addicionals dels sistemes tallafoc

Com ja hem vist, la utilització d'un sistema tallafoc suposa una barrera de control que manté la xarxa protegida de tots aquells accessos no autoritzats, actuant com un punt central de control i fent les tasques d'administració més simples.

No obstant això, aquest control i protecció de la xarxa és únicament una de les possibilitats que els sistemes tallafoc més moderns poden arribar a oferir-nos.

Pel fet de situar-se en un punt de xoc, els sistemes tallafoc poden oferir altres funcions interessants. Algunes d'aquestes característiques addicionals inclouen:

- **Filtratge de continguts -** Moltes organitzacions volen evitar que els seus usuaris utilitzin els recursos corporatius per navegar per determinats llocs web no desitjats. El filtratge de continguts ofert per alguns sistemes tallafoc pot bloquejar l'accés a aquests llocs web, alhora que protegir la xarxa contra codi maliciós inserit en les seves pàgines, com per exemple *ActiveX* i codi *Java* hostil.

- **Xarxa privada virtual* -** Aquest tipus de funcionalitat oferta per la majoria dels sistemes tallafoc actuals permet la construcció d'un túnel segur entre dos punts de la xarxa, usualment per a protegir les comunicacions d'una xarxa corporativa en travessar una xarxa hostil (com és el cas d'Internet).

- **Traducció d'adreces de xarxa** -** Encara que no es tracta estrictament d'una funcionalitat relacionada amb la seguretat, la majoria dels sistemes tallafoc ofereixen la possibilitat de realitzar NAT i poder així associar adreces IP reservades (indicades en l'RFC 1918) a adreces vàlides. Un exemple podria ser la traducció d'adreces IP del rang 10.0.0.0/24 d'una xarxa privada perquè surtin cap a Internet com l'adreça IP 212.46.31.224.

- **Balanceig de la càrrega -** El balanceig de la càrrega oferta per molts sistemes tallafoc és la tasca de segmentar el trànsit d'una xarxa de manera distribuïda. Alguns sistemes tallafoc ofereixen actualment funcionalitats que poden ajudar, per exemple, a distribuir trànsit FTP i HTTP de manera totalment distribuïda.

- **Tolerància a fallades -** Alguns sistemes tallafoc ofereixen actualment suport per a determinats tipus de fallades. Per a això, en la majoria de les situacions se solen utilitzar funcionalitats d'alta disponibilitat***. En aquestes situacions, la major part de les estratègies inclouen la utilització de diferents sistemes tallafoc sincronitzats, de manera que un dels sistemes estarà a l'espera que es produeixi una fallada en l'equip original per a poder posar-se en funcionament.

*** En anglès, *Virtual Private Networking, (VPN).***
**** En anglès, *Network Address Translation, (NAT).***
***** En anglès, *High-Availability, (HA).***

- **Detecció d'atacs i intrusions -** Molts dels fabricants de sistemes tallafoc incorporen en els seus productes la capacitat per detectar sondejos i atacs coneguts. Encara que aquest tipus de funcionalitat no comporta un problema en si mateix, hauríem de tenir present que la realització d'aquestes deteccions en el propi sistema tallafoc pot arribar a implicar una alta càrrega de treball.

- **Autenticació d'usuaris -** Atès que el sistema tallafoc és un punt d'entrada a la xarxa, pot dur a terme una autenticació addicional a la que efectuen els serveis de xarxa. Així, l'autenticació d'usuaris en un sistema tallafoc té la finalitat de permetre o denegar la connexió a l'usuari que sol·licita connexió a un servei intern (normalment mitjançant un mecanisme més fort que l'implantat pel servei al qual es connecta).

Finalment, cal comentar que la introducció de serveis addicionals en un sistema tallafoc incrementa el nombre de vulnerabilitats sobre aquest, i per tant, el risc. La pràctica d'implantar diferents serveis sobre un tallafoc no és recomanable. Des del punt de vista de la seguretat és millor buscar una arquitectura distribuïda.

Resum

Quan un sistema es connecta a una xarxa de computadors, s'exposa a un conjunt d'amenaces que sempre hi són presents. Com ja hem vist en el mòdul anterior, és molt probable que aquests sistemes presentin vulnerabilitats, augmentant la probabilitat que aquestes amenaces ocorrin.

Els sistemes tallafoc focalitzen les decisions de seguretat en un únic punt que es localitza allà on hi ha les majors vulnerabilitats, denegant qualsevol connexió que no estigui expressament permesa.

Mitjançant un escenari de configuració de filtre de paquets en sistemes tallafoc simples, es podran aplicar tecnològicament les decisions d'una política de seguretat definida per l'organització.

També és possible la construcció de sistemes tallafoc mitjançant tecnologies de servidors intermediaris o pasarel·les, de manera que tot el trànsit rebut pugui ser interpretat a nivells superiors del de xarxa.

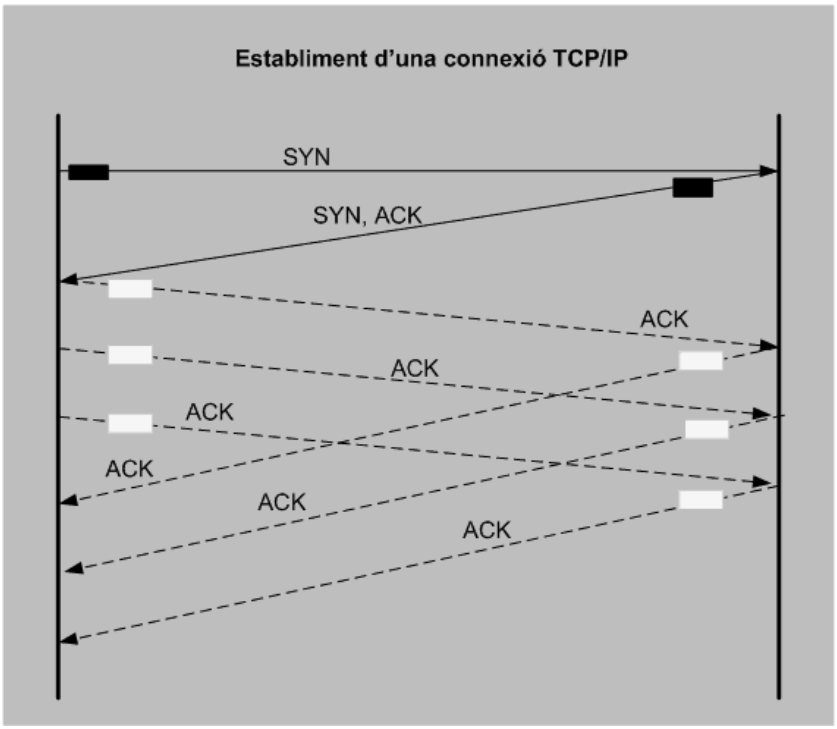
Així doncs, la utilització d'un sistema tallafoc suposa una barrera de control que mantindrà la xarxa protegida de tots aquells accessos no autoritzats, actuant com un punt central de control i fent les tasques d'administració més simples.

Per altra banda, pel fet de situar-se en un punt de xoc, els sistemes tallafoc ofereixen altres funcions de seguretat interessants com podrien ser el monitoratge de les connexions de xarxa, l'anàlisi de contingut (per cercar, per exemple, virus), realitzar controls d'autenticació addicionals, construcció de xarxes privades virtuals, etc. També poden realitzar funcions no relacionades directament amb la seguretat de la xarxa, com traducció d'adreces de xarxa (NAT), gestió de serveis de xarxa, control de l'amplada de banda, ...

Finalment, hem de tenir present que els sistemes tallafoc són únicament mecanismes de prevenció i que no són una solució única per solucionar tots els problemes de seguretat d'una xarxa connectada a Internet. Aquests sistemes no podran protegir mai la xarxa d'aquells atacs que es produeixin al seu interior i és possible que un atacant extern pugui ser ajudat per un usuari intern (legítim) per col·laborar en els atacs. Tampoc podran evitar atacs contra serveis amb accés global (on tothom pot accedir des de qualsevol lloc), ni podrà protegir la xarxa contra la transferència d'aplicatius maliciosos (virus, cucs, ...). Seria impracticable la utilització d'un dispositiu que es dediqui a analitzar tot el trànsit que circula a través seu. És per això que calen mecanismes de protecció addicionals, com els que es presentaran en mòduls posteriors.

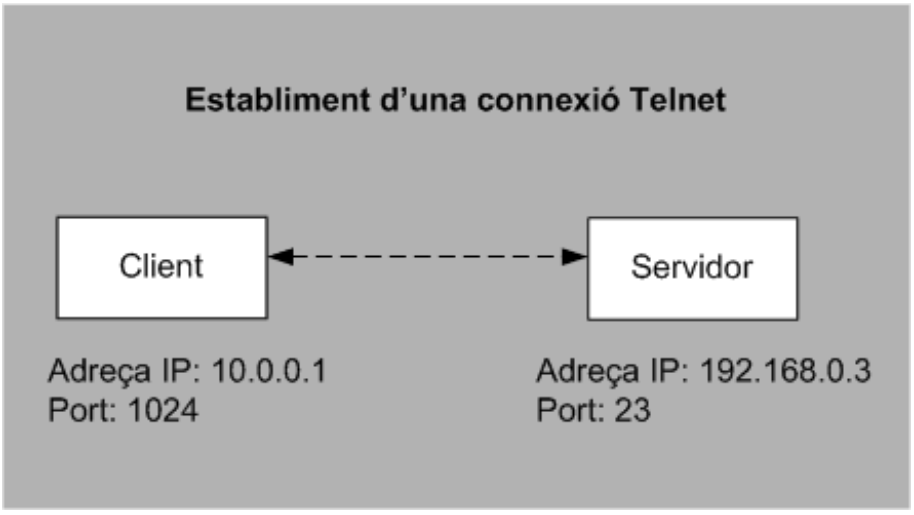
Exercicis d'autoavaluació

1) Segons el següent esquema, on s'il·lustra com ocorre una connexió TCP:



Quin tipus de paquets podria inspeccionar un encaminador amb filtratge per tal de verificar els intents de connexió? I per identificar les respostes?

2) A partir de la següent figura, on s'observa una connexió Telnet feta des d'un client a un servidor:

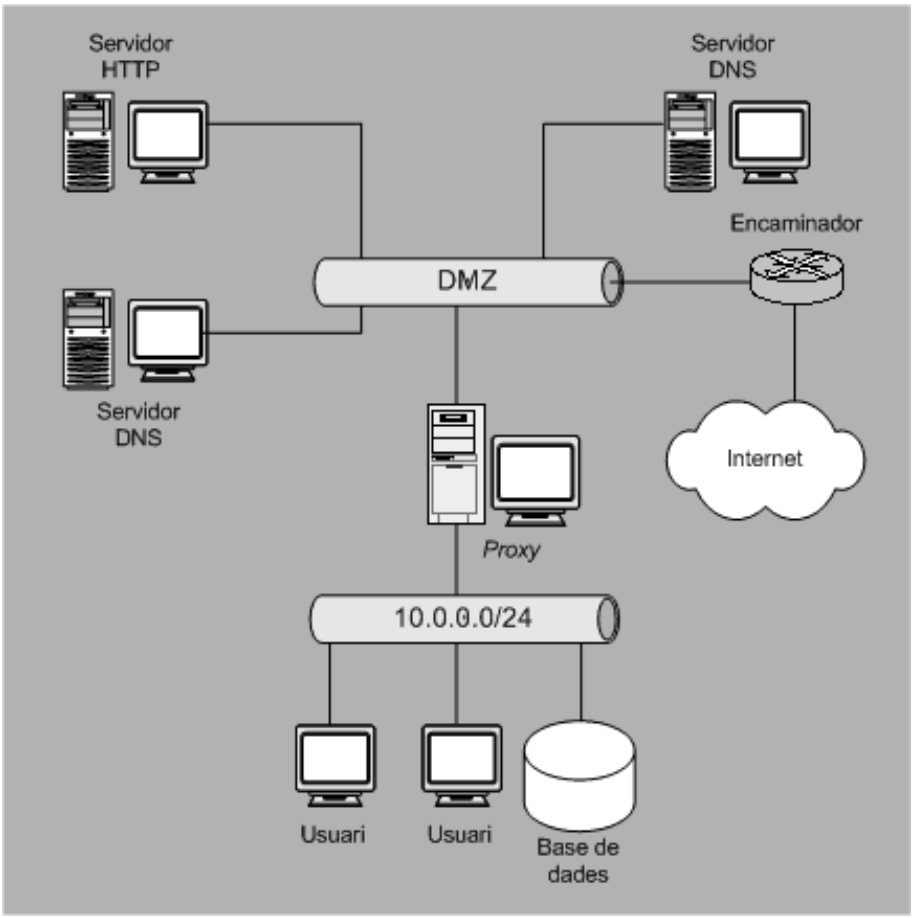


Si suposem que el servidor 192.168.0.3 és el servidor Telnet de la xarxa interna, com es poden bloquejar les connexions destinades a aquest, exceptuant les procedents del sistema 10.0.0.1?

3) Segons la següent política de seguretat, com impediríeu que es fessin connexions a servidors HTTP externs que funcionen sobre un port diferent del 80?

Regla	Acció	Origen	Port d'origen	Destinació	Port de destinació	Indicador	Descripció
1	Rebutja	10.0.0.0	*	*	80	TCP	Rebutja qualsevol connexió a servidors HTTP
2	Permet	10.0.0.0	*	*	*	TCP	Permet connexions TCP sortints
3	Permet	*	*	10.0.0.1	80	TCP	Permet connexions HTTP entrants
4	Permet	*	*	10.0.0.2	25	TCP	Permet connexions SMTP entrants
5	Permet	*	*	10.0.0.3	53	UDP	Permet connexions DNS entrants
6	Rebutja	*	*	10.0.0.0	*	*	Rebutja qualsevol altra connexió a la xarxa interna

4) Per què no trobem la base de dades de la següent figura dins de la zona desmilitaritzada?



Solucionari

1) El filtre de paquets inspeccionarà només el paquet de sincronisme o petició d'inici de connexió (indicador SYN); si s'autoritza el pas a aquest paquet, es permet l'establiment de la connexió.

Per identificar respostes es recorre a la inspecció del paquet que tenen els indicadors ACK i SYN activats. La resta de paquets no són rellevants.

2) Per bloquejar les connexions destinades al servidor 192.168.0.3, exceptuant les procedents del sistema 10.0.0.1, ho podem fer de la manera següent:

Regla	Acció	Origen	Port d'origen	Destinació	Port de destinació	Indicador	Descripció
1	Permet	10.0.0.1	> 1023	192.168.0.3	23	TCP	Permet connexions del sistema de teletreball
2	Rebutja	*	*	*	*	*	Rebutja qualsevol altra connexió

3) A nivell de xarxa no es pot distingir si els paquets adreçats a un port arbitrari corresponen al protocol HTTP o no. Per tant, amb un filtre de paquets l'única solució seria rebutjar tots el paquets amb origen en la xarxa interna, excepte els que puguin ser respostes a peticions dels serveis permesos (ports TCP d'origen 25 i 80).

Regla	Acció	Origen	Port d'origen	Destinació	Port de destinació	Indicador	Descripció
1	Permet	10.0.0.0	80	*	*	TCP	Permet respostes a peticions HTTP
2	Permet	10.0.0.0	25	*	*	TCP	Permet respostes a peticions SMTP
3	Rebutja	10.0.0.0	*	*	*	TCP	Rebutja qualsevol altre paquet sortint
4	Permet	*	*	10.0.0.1	80	TCP	Permet connexions HTTP entrants
5	Permet	*	*	10.0.0.2	25	TCP	Permet connexions SMTP entrants
6	Permet	*	*	10.0.0.3	53	UDP	Permet connexions DNS entrants
7	Rebutja	*	*	10.0.0.0	*	*	Rebutja qualsevol altra connexió a la xarxa interna

4) En la configuració de l'exemple se suposa que l'accés a la base de dades només es pot fer des de la xarxa interna. Per tant, és millor aïllar-la de la xarxa externa amb dos sistemes tallafoc (l'encaminador i el servidor intermediari) que no pas deixar-la en la zona desmilitaritzada, on només la separaria de la xarxa externa l'encaminador.

Un altre criteri és el de posar el servei al més a prop possible dels sistemes; evidentment la base de dades és un servei per a la intranet que té clients a la zona desmilitaritzada. Mai s'hi accedeix directament a través d'Internet (en el supòsit que això fos un requeriment ineludible, es recorreria a treballar sobre una base de dades rèplica en un sistema de només lectura si és possible).

Glossari

arquitectura dual-homed: Equip que té, almenys, dues interfícies de xarxa.

equip bastió: Equip que ha estat fortament protegit per suportar els suposats atacs des d'un lloc hostil i que actua com a punt de contacte entre l'interior i l'exterior d'una xarxa.

encaminador amb filtratge de paquets: Dispositiu de xarxa que encamina trànsit TCP/IP sobre la base d'una sèrie de regles de filtratge que decideixen quins paquets s'encaminen a través seu i quins són descartats.

passarel·la a nivell d'aplicació: Dispositiu de xarxa que actua com a retransmissor a nivell d'aplicació.

passarel·la a nivell de circuit: Similar a una passarel·la a nivell d'aplicació quant a la connexió, però operant de manera similar a un filtre de paquets a nivell de xarxa una vegada que la connexió ha estat inicialitzada.

política de seguretat: Resultat de documentar les expectatives de seguretat d'una xarxa, tractant de plasmar en el món real els conceptes abstractes de seguretat.

seguretat perimetral: Seguretat basada tan sols en la integració a la xarxa de sistemes tallafoc i altres mecanismes de prevenció.

servidor intermediari: Servidor programari que s'encarregarà de realitzar les connexions sol·licitades amb l'exterior i retransmetre-la cap a l'equip que havia iniciat la connexió. En anglès, *proxy*.

tallafoc: Element de prevenció que realitzarà un control d'accés per tal de separar la nostra xarxa dels equips de l'exterior (potencialment hostils). En anglès, *firewall*.

zona desmilitaritzada: Dins d'una xarxa protegida per un tallafoc, zona separada dels servidors públics per un segon tallafoc.

Bibliografia

[1] Hare, C.; Siyan, K. (1996). *Internet Firewalls and Network Security, 2nd ed.* New Riders.

[2] Buch i Tarrats, J. (2000). *Sistemes de comunicacions - Arquitectures segures de xarxes (Sistemes tallafoc).* FUOC.

[3] Zwicky, E. D.; Cooper, S.; Chapman, D. B. (2000). *Building Internet Firewalls, 2nd ed.* O'Reilly & Associates.

[4] Cheswick, W. R.; Bellovin, S. M.; Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker, 2nd ed.* Addison-Wesley Professional Computing.