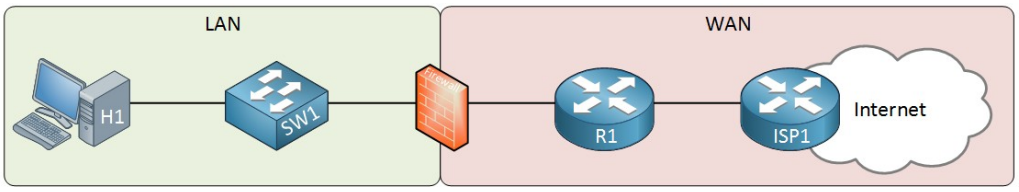
Introducció als tallafocs

Concepte de tallafocs

Un "tallafoc" o "firewall" és un dispositiu (**hardware** o **software**) que fa de barrera entre una/es xarxa/es de confiança i una/es altra/es que no ho és/són, així que sovint s'usa de "frontera" entre una LAN i una WAN (Internet, per exemple). Normalment es col·loca just "darrera" del "router" (o fins i tot, implementat dins del mateix aparell) de manera que tots els paquets passin a través del tallafocs per ser revisats, el qual decidirà en base a certes regles predefinides i les característiques dels paquets detectats, si aquests podran continuar el seu camí o, per contra, hauran de ser eliminats ("filtrats"). El següent esquema mostra un exemple bàsic, on el tallafocs representa el mur de totxo:



NOTA: L'avantatge dels tallafocs basats en maquinari és que són dispositius independents que executen els seus propis sistemes operatius, proporcionant així una línia addicional de defensa a les proteccions que hi puguin haver ja a nivell de sistema amfitrió; a més, solen ser molt més ràpids que els tallafocs de programari. L'avantatge dels tallafocs de programari és la seva capacitat per controlar el comportament específic de la xarxa d'aplicacions individuals d'un sistema però cal tenir en compte que tenir el tallafoc al mateix ordinador que la informació que s'intenta protegir pot dificultar la capacitat del tallafoc per detectar i aturar activitats malicioses (això és especialment cert si l'equip ja està compromès amb programes maliciosos)

Les característiques més habituals d'un paquet que un tallafocs comprova per deixar-lo passar o no (segons la regla que s'hagi definit) són l'adreça IP de l'origen i/o del destí i/o el port. És a dir, els tallafocs típicament treballen fins el **nivell 4** del model OSI (a diferència dels "switchos", que treballen al nivell 2 i els "routers", que treballen al nivell3) . Fent servir aquestes regles senzilles, els tallafocs no triguen gaire temps en filtrar: quan reben un paquet comproven si coincideix amb una entrada de la llista de regles i, si és així, permeten o eliminen el paquet; tant se val si reben un sol paquet o milers: cada paquet es tracta individualment i no es fa cap seguiment dels paquets que s'han inspeccionat abans. Aquest funcionament s'anomena filtratge sense estat (o "stateless").

La majoria de tallafocs, de totes formes, actualment utilitzen filtres amb estat (o "**stateful**"). Aquests tipus de tallafocs realitzen un seguiment de totes les connexions entrants i sortints. Per exemple: suposem que un servidor web (que està funcionant "darrera" d'un tallafoc) accepta una mitjana de 20 connexions TCP noves cada segon des de diferents adreces IP i que el tallafoc fa un seguiment de totes les connexions: si aquest "veu" que una adreça IP d'origen sol·licités un número de connexions TCP noves per segon perillosament proper al límit de 20, i sempre i quan tingui definida la regla pertinent, bloquejarà llavors tot el trànsit provinent de l'adreça IP d'origen, impedint així un possible atac DoS ("denegació del servei").

Alguns tallafocs també implementen algun tipus de **DPI** ("inspecció profunda de paquets". Les regles simples, tal com hem dit, només comproven les adreces i ports origen/destí, que són els nivells 3 i 4 del model OSI. "Inspecció profunda de paquets" significa que el tallafocs podrà inspeccionar fins a la capa 7 del model OSI. Això vol dir que podrà mirar els camps de les capçaleres dels protocols reconeguts d'aquest nivell (DNS, DHCP, HTTP...) i fins i tot el contingut del "payload". Per exemple: en lloc de bloquejar totes les adreces IP que resolguin al domini "lolcats.com", es podria crear un filtre que busqués URIs incloent aquest domini en peticions HTTP i bloquejar-ne aquestes, de manera que no caldria preocupar-se per les adreces IP concretes dels servidors web (les quals, a més, podrien canviar en el futur). Un altre exemple seria la possibilitat de comprovar el "payload" per bloquejar paquets que poguessin contenir malware conegut.

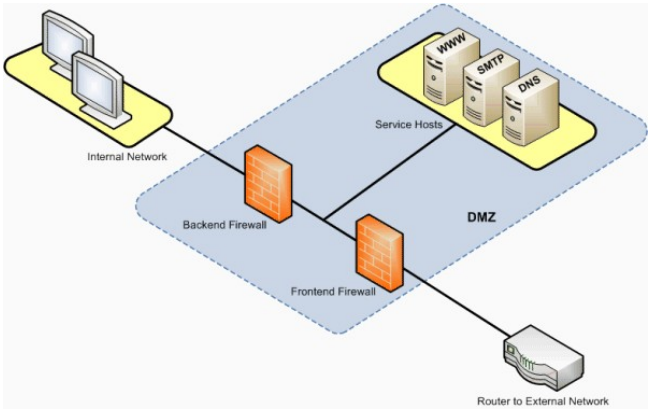
Topologies

*__Tallafocs perimetral:__ Un equip actua com a tallafocs connectant la xarxa interna amb l'externa. Pot venir integrat a nivell de software dins de l'aparell que faci de "router" (opció més simple però també menys versàtil i amb poques opcions de monitorització) o bé pot ser un equip dedicat, ja sigui amb un sistema Linux específicament dissenyat per aquesta tasca (amb les regles adients carregades, l'IP-Forwarding activat, etc) o un dispositiu hardware específic. En qualsevol cas, aquest equip dedicat haurà de tenir com a mínim dues tarjes: una connectada al "router" pròpiament dit i una altra al switch central de la xarxa interna. Aquesta opció és la més comuna si a la xarxa interna no s'implementa cap servei de cara a l'exterior. Cal tenir en compte, no obstant, que si l'equip tallafocs es veu compromès, tota la xarxa també ho estarà. És per això que sovint es completa aquest tallafocs "de la xarxa" amb tallafocs funcionant específicament a cada màquina individual que en forma part.

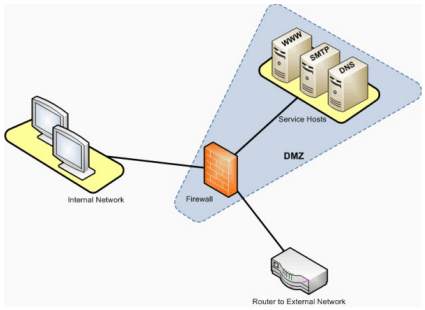
*__"Screened host":__ En el cas de voler oferir serveis des de la xarxa interna cap a l'exterior (web, correu, DNS, etc) , una opció és utilitzar la mateixa topologia descrita a l'apartat anterior però implementar una màquina de la xarxa interna per a què ofereixi aquests serveis, tant "a dins" com "a fora" i configurar llavors el tallafocs per tal de redirigir el tràfic provinent de l'exterior adientment a aquesta màquina (aplicant regles de tipus NAT, normalment). No obstant, aquesta solució no és òptima perquè aquest servidor és un element potencialment vulnerable que, en estar en contacte directe amb la resta de màquines de la xarxa interna, podria expandir-hi un atac reeixit a totes elles de forma molt senzilla. Caldria, per tant, assegurar-se molt bé de tenir en aquesta màquina servidora els mínims serveis funcionant, les darreres actualitzacions de seguretat aplicades, una constant monitorització de logs... En general, doncs no sol ser una bona idea.

*__"Untrusted" host":__ Una opció per aïllar la xarxa interna dels servidors que volguem publicar a l'exterior és deixar a la banda de "fora" del tallafocs aquest/s servidor/s en qüestió. És a dir, ubicar-lo entre el "router" i el tallafocs, de manera que la xarxa interna estigui igualment protegida pel tallafocs i tots els accessos al servidor es quedin a la banda de "fora" d'ell (rera el "router"). No obstant, en aquest cas la configuració i administració d'aquest/s servidor/s públic/s continua sent molt delicada.

*__DMZ:__ La millor opció és fer servir una "zona desmilitaritzada" ("demilitarized zone"). La idea és aïllar el/s servidor/s públic/s de la xarxa interna amb un tallafocs (igual que a la infraestructura del "untrusted" host) però, a més, aïllar aquest/s servidor/s igualment de la xarxa externa amb un altre tallafocs (normalment situat just "darrera" el "router" o en el "router" mateix) de manera que es creï una zona intermitja entre la xarxa externa i la xarxa interna anomenada precisament, "DMZ". D'aquesta manera, es podria configurar cada tallafoc amb regles específiques per tal de deixar passar les peticions vàlides al/s servidor/s públic/s i, a la vegada, evitar l'accés indegut a la xarxa interna. En aquesta configuració, per definició els equips interns no podran confiar en els equips de la DMZ perquè aquests estan exposats al públic i, encara que la DMZ aporta més seguretat que tenir un "untrusted" host, podrien estar igualment compromesos. Com exemple a continuació mostrem un diagrama de xarxa on es veuen varis "routers"/"tallafocs" involucrats en la implementació d'una DMZ (on, per cert, hi podria haver implementat també, algun IDS/IPS, o algun dispositiu TAP, etc ja que és per on passa el tràfic més "interessant")



NOTA: A vegades, es veuen implementacions de DMZ amb un sol tallafocs just darrera del "router". En aquest cas, però, el tallafocs tindrà tres tarjes de xarxa: la directament connectada al "router", una altra connectada a la xarxa interna i una altra a la DMZ (un esquema es pot veure a continuació). Lògicament, haurà de tenir carregades les regles adients per redirigir el tràfic a cada destí aportant tota la seguretat possible.



Proxies

"Proxy" significa intermediari. Per tant, un "servidor proxy" és un programa (encara que també pot ser un hardware dedicat) que fa d'intermediari entre clients (normalment pertanyents a una LAN) i servidors (normalment accesibles a Internet). L'important aquí es tenir en compte que aquesta intermediació es realitza a **nivell 7** del model OSI. Això vol dir que un "servidor proxy" intercepta tots els paquets que el travessen (de sortida i d'entrada) que pertanyen a un (o uns quants) protocol/s determinat/s del nivell d'aplicació, podent inspeccionar (i manipular) el seu corresponent payload i, en general, podent "entendre" les característiques específiques d'aquests protocols, a diferència dels tallafocs estàndar, els quals només arriben fins el nivell 4 i, per tant, no són capaços d'interpretar el tràfic a nivells superiors. Això vol dir que podem tenir tants servidors proxy com diferents protocols d'aplicació volguem interceptar; així, tenim proxies HTTP/S (com per exemple, Squid o fins i tot el propi Apache), proxies SSH, proxies SMTP, etc.

La intermediació realitzada per un servidor "proxy" pot servir, per exemple, per controlar centralitzadament el tràfic d'una xarxa i aplicar les polítiques d'accés convenients (fent tasques, així doncs, similars a la d'un tallafocs, però en aquest cas amb la possibilitat d'inspeccionar tràfic de nivell d'aplicació i, per tant, de poder aplicar regles específiques per aquest nivell). En aquest sentit, un servidor "proxy" pot, per tant, filtrar o restringir trànsit (del protocol adient) entrant i/o sortint a/de la xarxa local a/de Internet. En el cas concret dels proxies HTTP/S (els més habituals), això es tradueix a la pràctica en poder evitar l'accés des d'una xarxa local a determinades pàgines web i/o (atès que el filtratge es pot realitzar en els dos sentits, entrada i sortida) en restrigir l'accés no autoritzat d'usuaris externs a recursos o serveis de la xarxa local, etc.

NOTA: Una funció addicional del servidors intermediaris és la d'emmascarar l'adreça IP dels hosts de la xarxa local, de manera que aquesta no sigui visible des d'Internet, ja que qui fa la petició real als servidors externs és el servidor proxy. En aquest sentit, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other machines.
NOTA: En el cas concret dels proxies HTTP/S, una altra utilitat molt habitual és la de fer-los servir com a servidors-cau de continguts, per tal d'incrementar així l'ample de banda disponible en accedir a Internet des de la xarxa local. És a dir, fer-los servir com a magatzems de la informació que és demanada amb més assiduïtat. Expliquem això: és freqüent que els diferents usuaris d'una mateixa xarxa local consultin les mateixes pàgines web; quan una persona requereix una pàgina web concreta, el proxy connectarà amb el lloc, descarregarà la pàgina i la desarà en memòria (el que se'n diu memòria "cau"); quan una segona persona torni a demanar la mateixa pàgina, el proxy li enviarà la que ha emmagatzemat a la seva memòria cau, i eliminarà així la necessitat de fer la sol·licitud a Internet, la qual cosa estalvia temps i trànsit de paquets a Internet. Algunes etiquetes HTML i/o capçaleres HTTP poden informar el servidor proxy que certes pàgines o certs continguts són dinàmics (és a dir, canvien sovint), informació que fa servir el proxy per incrementar la freqüència en què actualitza la versió d'aquests continguts en la seva memòria cau.
NOTA: Un tamany molt gran de memòria cau ocupa molt d´espai (en RAM i/o en disc), i suposa actualitzar moltes pàgines visitades per evitar inconsistències. Un tamany petit suposa un baix percentatge d´encerts en visitar una pàgina i per tant, poca eficiència. Hi ha diferents algoritmes possibles per actualitzar la memòria cau, com ara sobreescriure els objectes menys recentment usats, o els objectes menys freqüentment usats, o els menys freqüentment usats o grans, etc. La configuració concreta utilitzada dependrà del programa concret utilitzat

En relació a l'estudis dels servidors "proxies" HTTP/S, ens podem trobar amb diferents classificacions, com ara els servidors "directes" (Squid, Apache, etc) vs. els "reverse proxies" -també anomenats "load balancers"- (HAProxy, Apache, etc) , els proxies "transparents", etc. En aquest sentit, segons quin sigui el tipus de proxi implementat a la xarxa local caldrà configurar convenientment els clients (en aquest cas, els navegadors) per fer-ne l'ús adient. Tot això s'estudiarà en un document específic a banda.