Firewalls / Tallafocs. Reguladors del transit:

Xavier Tartera

Tendències de seguretat

Totes les línies actuals d'investigació en seguretat de xarxes comparteixen una idea:

- "La concentració de la seguretat en un punt, obligant a tot el tràfic entrant i sortint passi per un mateix punt, que normalment es coneix com tallafocs o firewall, permetent concentrar tots els esforços en el control de trànsit al seu pas per aquest punt"

Metodologia de seguretat

La primera tasca a realitzar en una xarxa és redactar la **política de seguretat**. Després d'això, conèixer **l'estructura (topologia, accessos) de la xarxa** i finalment, auditar la xarxa per veure el seu estat en recerca de detecció de vulnerabilitats.
Aquest procés de detecció de vulnerabilitats consisteix en:

- Exàmen de hosts i elements de la xarxa, per vulnerabilitats conegudes.
- Ports oberts (observar serveis coneguts segons / etc / services).
- Revisió de l'estructura de fitxers i integritat del sistema en el cas de servidors (per exemple amb eines com Tripwire)

Tallafocs

Consisteix en un dispositiu format per un o diversos equips que se situen entre la xarxa de l'empresa i la xarxa exterior (normalment Internet), que analitza tots els paquets que transiten entre ambdues xarxes i filtra els que no han de ser reenviats, d'acord amb un criteri establert per endavant, de manera simple.

Perquè no es converteixi en un coll d'ampolla a la xarxa, han de processar els paquets a una velocitat igual o superior al router.

Tallafocs

Crea un perímetre de seguretat i defensa de l'organització que protegeix.

El seu disseny ha de ser d'acord amb els serveis que es necessiten tant privats com públics (WWW, FTP, Telnet, ...) així com connexions per remotes.

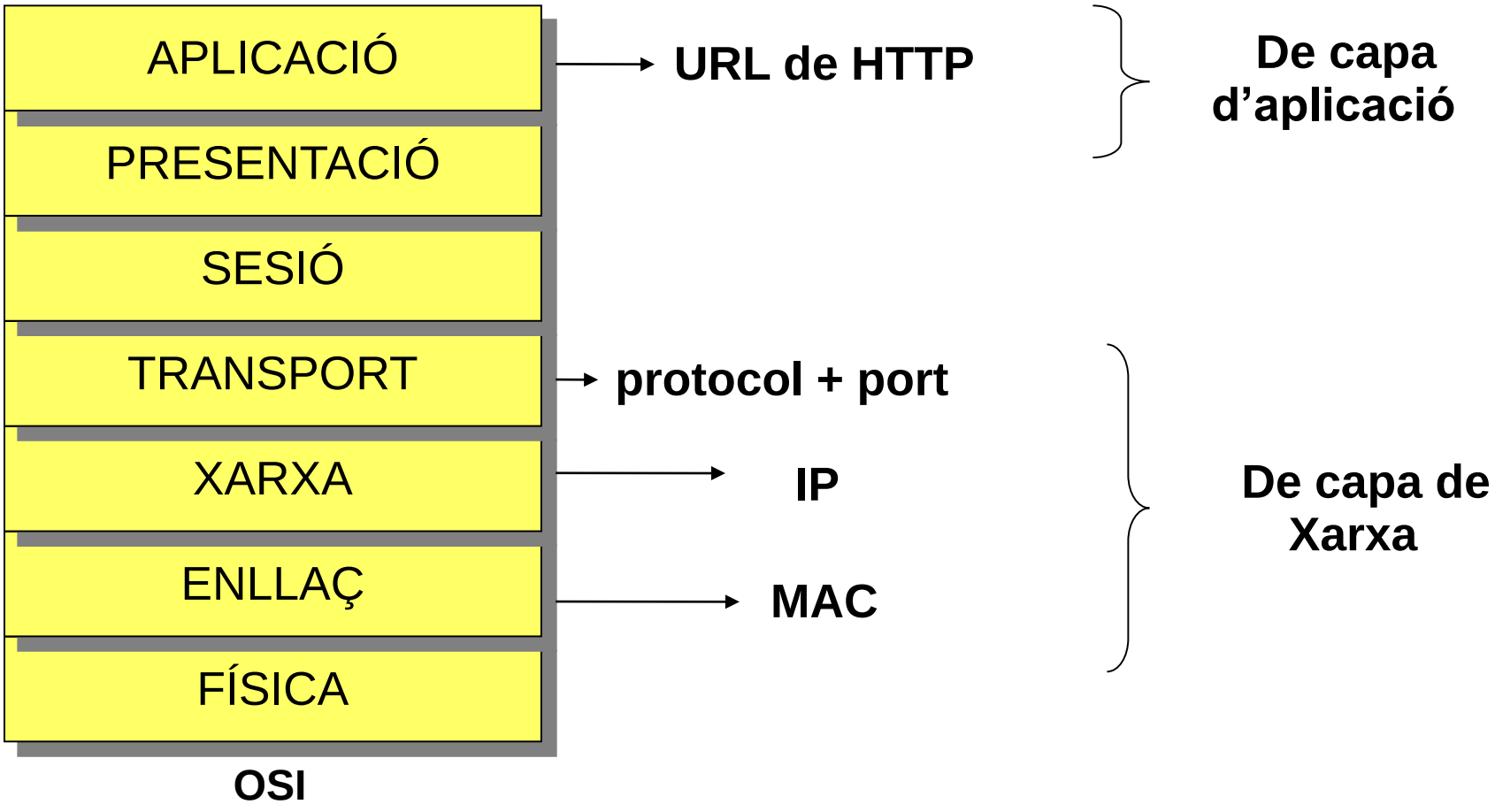
En definir un perímetre, el tallafocs opera també com NAT (Network Address traslation) i Proxy (servidor multipasarela).

Tipus de Tallafocs

- de capa de xarxa o de filtrat de paquets:
  - Funciona a nivell de xarxa (nivell 3) de la pila de protocols (TCP / IP) com filtre de paquets IP. A aquest nivell es poden realitzar filtres segons els diferents camps dels paquets IP: adreça IP origen, adreça IP destí. Sovint es permeten filtrats segons camps de nivell de transport (nivell 4) com el port origen i destí, o a nivell d'enllaç de dades (nivell 2) com l'adreça MAC
- de capa d'aplicació:
  - Treballa en el nivell d'aplicació (nivell 7), per exemple, si es tracta de tràfic HTTP es poden realitzar filtrats segons la URL a la qual s'està intentant accedir. En aquest cas és denominat Proxy.
  - personal
    S'instal·la com programari en un computador, filtrant les comunicacions entre aquest ordinador i la resta de la xarxa i viceversa.

Firewalls / Tallafocs. Reguladors del transit:

Tipus de Tallafocs



Tipus de fitratge en els tallafocs

- Tallafocs de **filtratge de paquets sense estat (*stateless*):** *les dades que* fan servir són, estrictament, les que conté el paquet. Normalment, les dades que s'utilitzen són l'origen, la destinació, el protocol i, si el protocol de transport ho suporta, el port d'origen i el de destinació.

Tipus de fitratge en els tallafocs

- Tallafocs de **filtratge de paquets amb estat (*stateful*):** *no només es basa* en les dades que proporciona el paquet, sinó que també manté una taula interna d'estat. D'aquesta manera, permet identificar si un determinat paquet inicia una connexió nova, si és d'una connexió existent o si és un paquet invàlid. Això permet evitar atacs que injecten paquets amb un origen invàlid (passarien per un tallafoc sense estat) i provoquen denegacions de servei, però sense que estiguin relacionats amb cap connexió.

Tipus de fitratge en els tallafocs

- Tallafocs a **escala d'aplicació (*proxy):*** *aquesta classe de tallafocs no es* limita a inspeccionar els paquets que passen per la xarxa, sinó que entén el protocol d'aplicació. Això permet que aquests tallafocs detectin si s'intenta fer servir el protocol d'alguna manera que pugui provocar algun tipus de comportament no desitjat o, fins i tot, filtrar segons el contingut. Evidentment, inspeccionar amb més profunditat el trànsitque circula implica un cost més gran.

Possibles fitratges en els tallafocs

- a nivell de xarxa, amb adreces IP i la interfície per la qual arriba el paquet, generalment a través de **llistes d'accés** (en els routers)
- a nivell de **transport**, amb els ports i tipus de connexió, a través de llistes d'accés (en els routers)
- a nivell **d'aplicació**, amb les dades, a través de **passarel·les** per les aplicacions permeses analitzant el continguts dels paquets i els protocols d'aplicació (exemple servidor proxy o passarel·la multiaplicació)

Polítiques per defecte dels tallafocs

És possible configurar tots els tallafocs per tal que tinguin dues intencions,
denegar només un part del trànsit o bé permetre'n només una part:

- Política **restrictiva**: denega tot el trànsit, tret del que se li indica (equival a una llista blanca).
- Política **permissiva:** permet tot el trànsit, tret del que se li indica (equival a una llista negra).

Llistes d'accés

Són una tècnica de **filtrat de paquets**, que consisteix en unes ordres executades seqüencialment a l'arribada / sortida de cada paquet en les interfícies del router, amb les opcions de *permit* o *deny* en complir la condició especificada en la seqüència segons la informació de la capçalera del paquet IP i de transport. En realitzar en el propi router, solen ser ràpides davant una altra tècnica de filtrat.

exemple:

permit tcp 192.168.0.0 0.0.255.255 host 172.16.1.2 eq 443
deny any any

Llistes d'accés

Inconvenient: al ser processat els paquets de forma independent, **no es guarda informació de context (no s'emmagatzemen històrics de cada paquet),** ni es pot analitzar a nivell de capa d'aplicació, ja que està implementat en els routers. A més, són difícils de seguir en execució.

recomanacions:

- situar els filtres al més a prop possible de l'element a protegir.
- no filtrar el mateix trànsit més d'una vegada

Firewalls / Tallafocs. Reguladors del transit:

Exemple: Tallafocs de **filtratge de paquets amb estat (*stateful)***

Si un client inicia una sessió TCP a un servei extern, escollirà un port no reservat (> 1023), amb la qual cosa quan contesti el servidor al client utilitzant el seu port, el tallafocs pugui impedir (si només permet l'entrada a ports coneguts) la entrada al port "desconegut" (el que va escollir el client).

La inspecció d'estat es basa en la inspecció de paquets basat en context: tipus de protocol i ports associats.
Internament es defineix una taula de sessions permeses (tant TCP com UDP), on el paquet de connexió inicial (per exemple en TCP el primer segment marxa amb bit ACK = 0 i SYN = 1) es comprova contra les regles, i si està permès s'apunta a la taula de sessions i després d'això, els paquets següents de la mateixa sessió es deixen passar.

Exemple: obertura de FTP en mode Actiu Mode

Firewalls / Tallafocs. Reguladors del transit:

Exemple: Obertura del FTP en mode passiu.

Suposem un escenari d'un perímetre que prohibeix l'establiment de connexions des de l'exterior.

FTP opera als ports 21 de control i 20 per transferència de dades.

Quan el client es connecta al port 21 i realitza la connexió, el servidor a continuació pel port 20 realitza la connexió amb el client (Mode Actiu).

Si estan prohibides l'obertura de connexions des de l'exterior (cosa bastant habitual), l'FTP mai funcionarà a menys que es configuri el client en mode passiu, és a dir, de manera que el propi client també realitzi l'obertura del port de dades o bé s'hagi configurat el perímetre amb inspecció d'estats i habiliti la sessió establerta.

Configuracions de Tallafocs

1. **Un router separant la xarxa Intranet d'Internet**, també conegut com **Screened Host Firewall**, que pot enviar el trànsit d'entrada només al host bastió.

2. **Un host bastió o passarel · la per les aplicacions permeses separant la xarxa Intranet d'Internet**, també conegut com **Dual homed Gateway**. Permet filtrat fins a la capa d'aplicació.

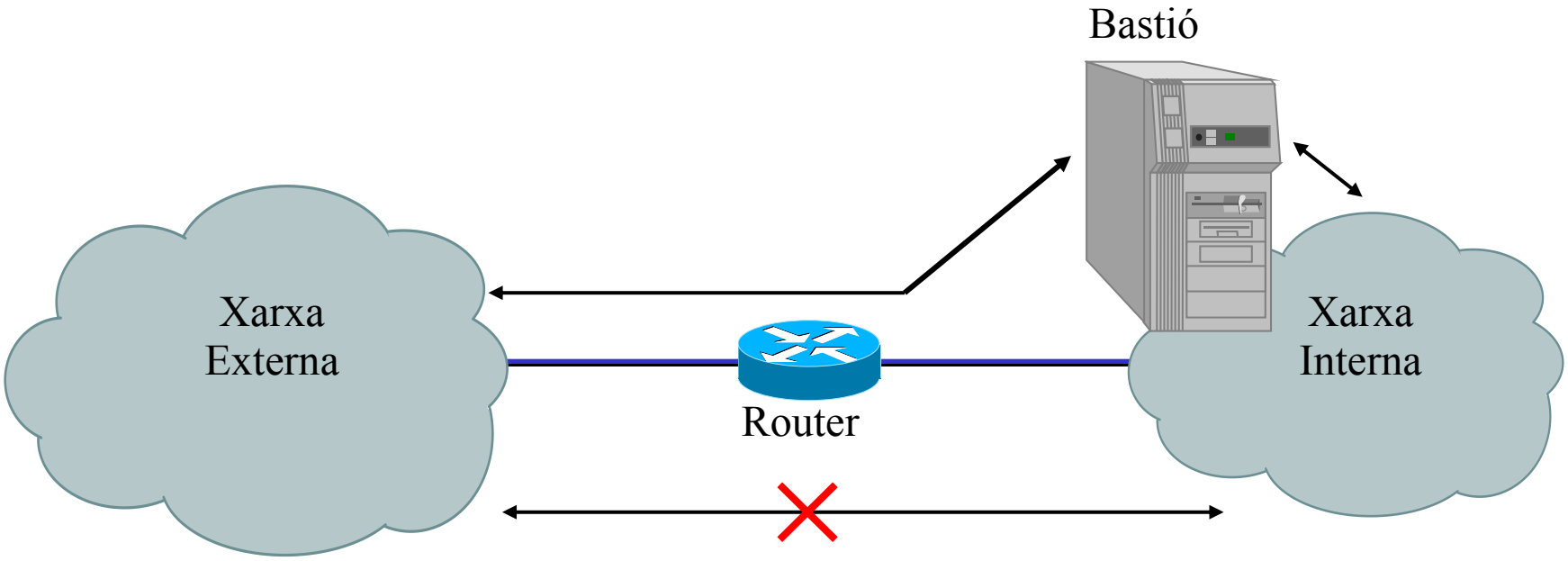
3. **Amb dos routers separant la xarxa Intranet i Internet i amb el host bastió dins de la xarxa formada per dos routers**, també coneguda com **Screened Subnet**, aquesta xarxa interna és coneguda com a zona neutra de seguretat o zona desmilitaritzada (**DMZ Demilitarized Zone).**

Screened Host

- Es tracta d'un router que bloqueja tot el tràfic cap a la xarxa interna, excepte al bastió
- Suporta serveis mitjançant proxy (bastió)
- Suporta filtrat de paquets (router)
- No és complicada d'implementar
- Si l'atacant entra al bastió, no hi ha cap seguretat

Firewalls / Tallafocs. Reguladors del transit:

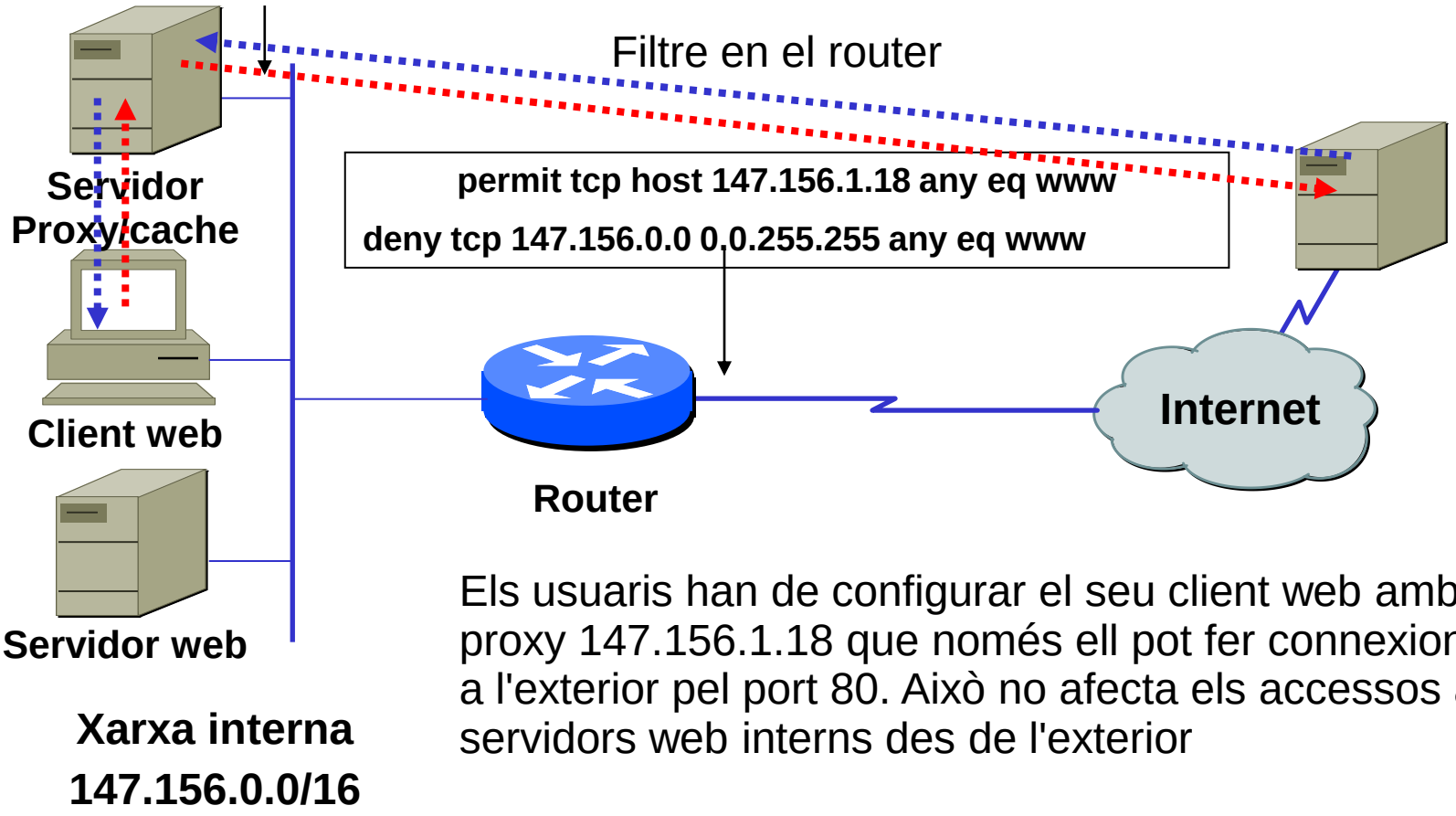
Screened Host



Aquesta arquitectura permet mantenir la connectivitat transparent quan estigui justificat, i obligant a passar pel 'bastion host' la resta de paquets.

Firewalls / Tallafocs. Reguladors del transit:

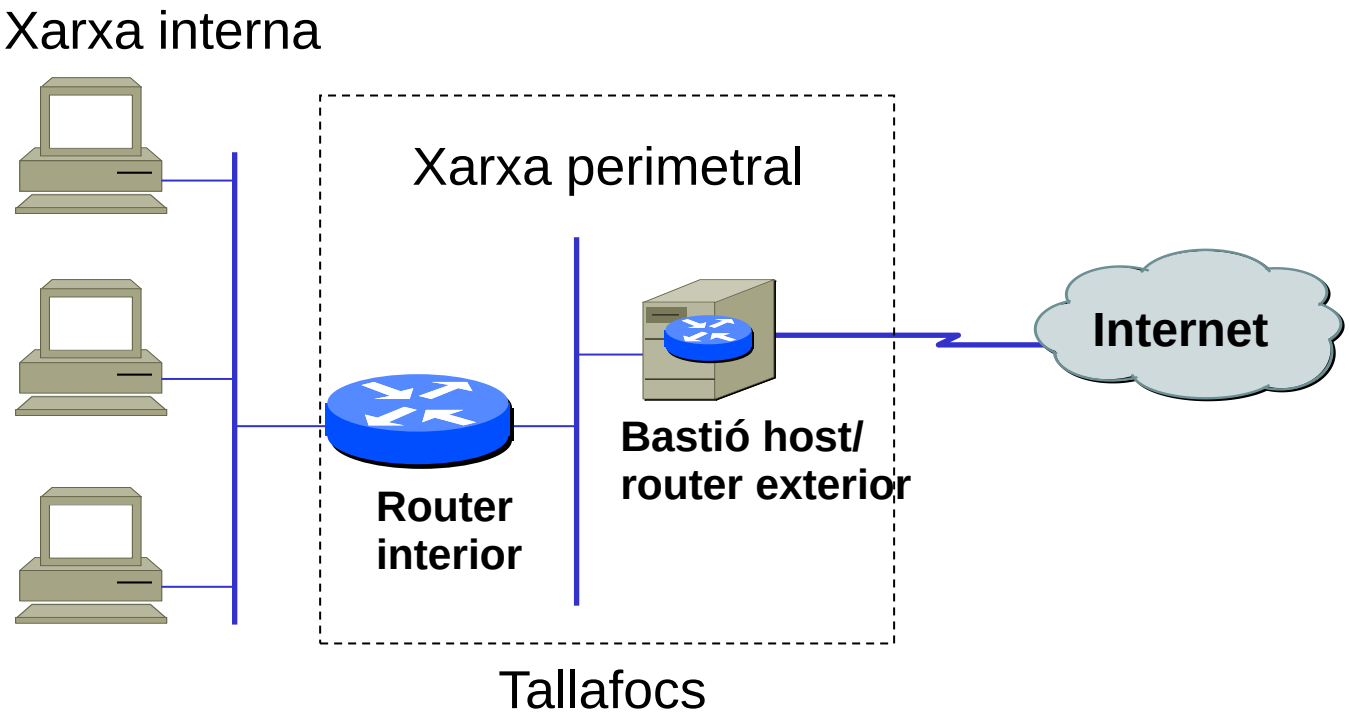
Exemple:Xarxa amb un servidor proxy d'ús obligatori.



Els usuaris han de configurar el seu client web amb el proxy 147.156.1.18 que només ell pot fer connexions a l'exterior pel port 80. Això no afecta els accessos a servidors web interns des de l'exterior

Firewalls / Tallafocs. Reguladors del transit:

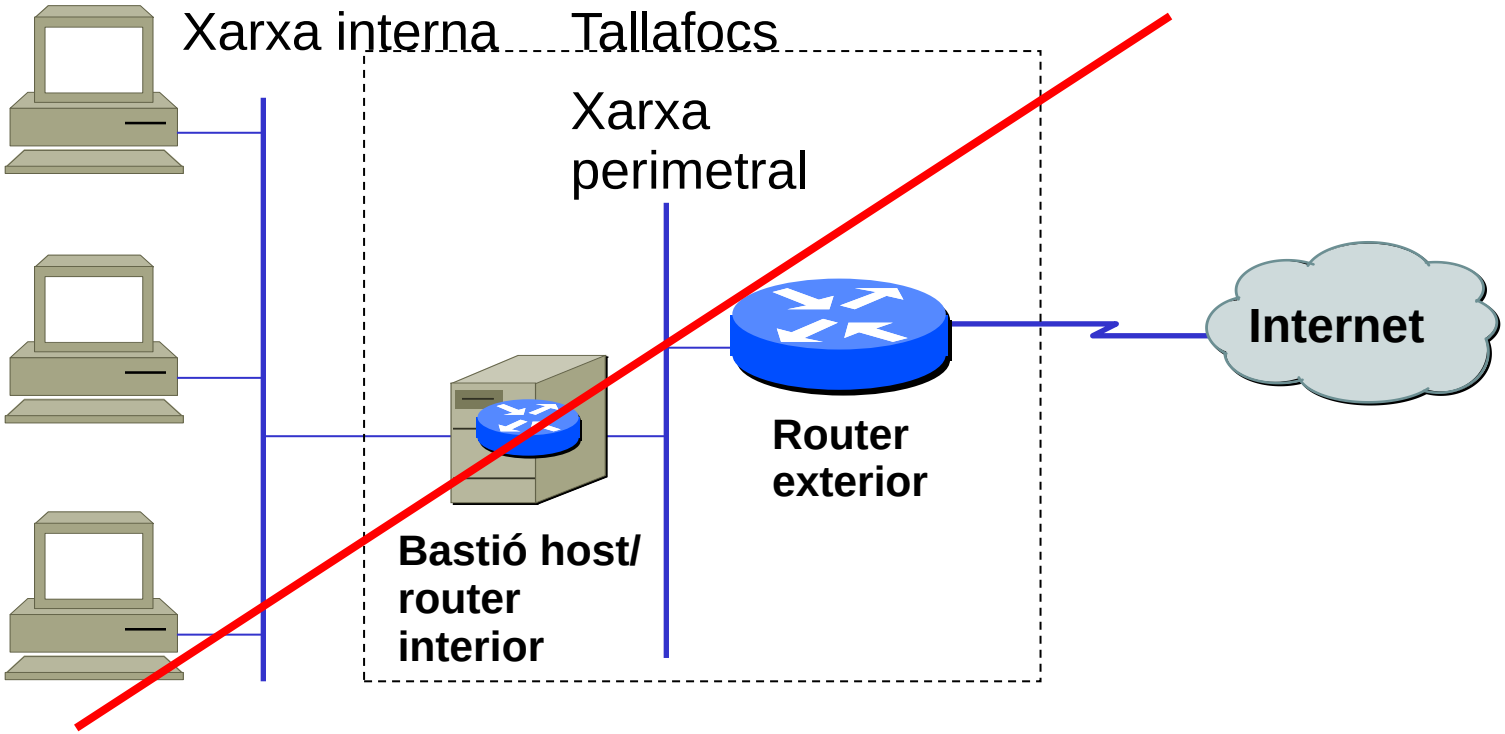
Col·locació del node bastió. Opció 1



Mantenir el bastion fora del router, implica més seguretat per a la xarxa interna, però el bastió estarà sotmès a més atacs que el router

Firewalls / Tallafocs. Reguladors del transit:

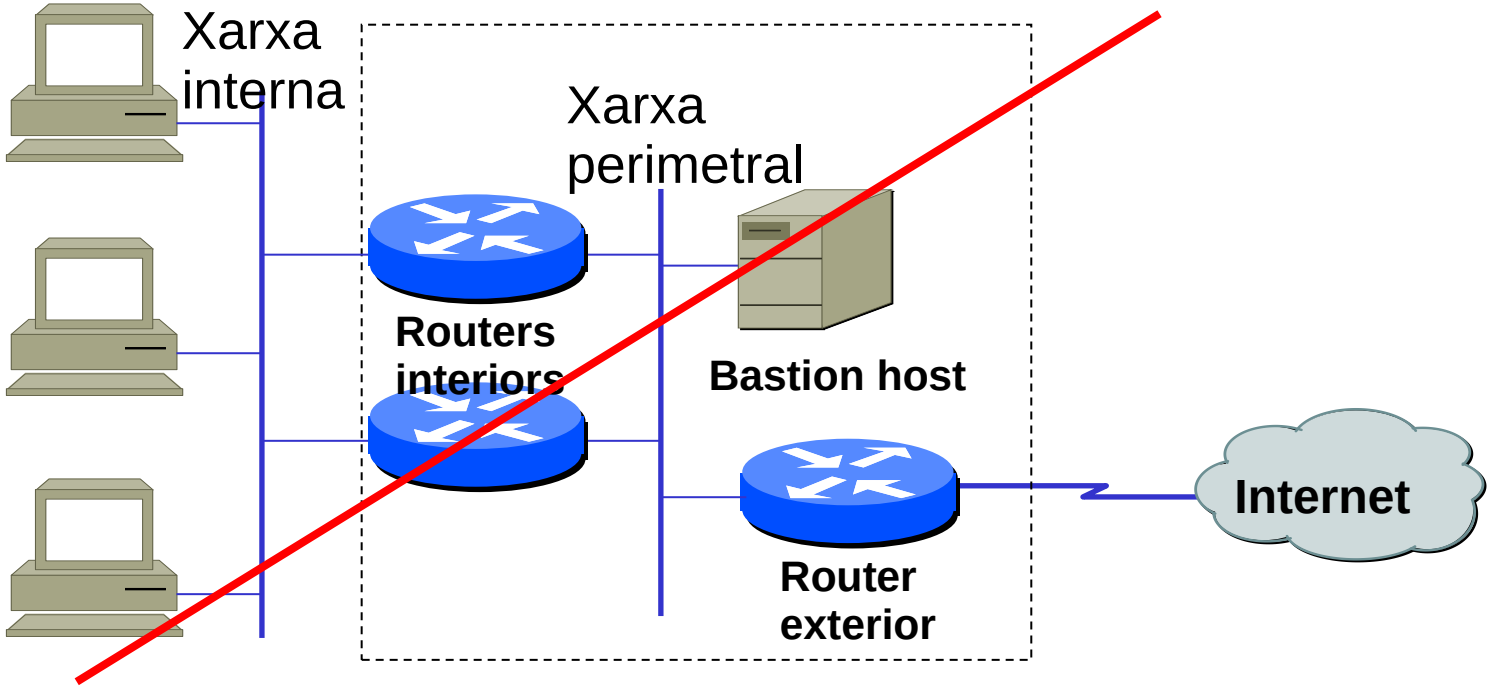
Col·locació del node bastió. Opció 2



Configuració no recomanada (un atac de *Bastion host* comprometria la seguretat de la xarxa interna)

Firewalls / Tallafocs. Reguladors del transit:

Col·locació del node bastió. Opció 3



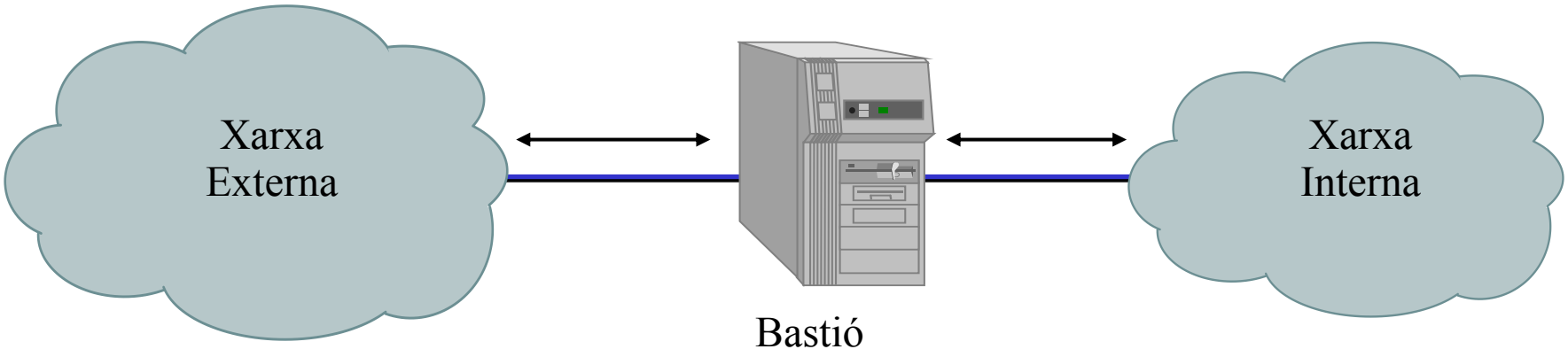
Configuració no recomanada (amb *routing dinàmic* el trànsit de la xarxa interna podria utilitzar la xarxa perimetral com a via de trànsit)

Dual-Homed gateway

- Es tracta d'un host (bastió) amb dues targetes de xarxa, connectades a xarxes diferents
  - En aquesta configuració, el bastió pot filtrar fins capa d'aplicació.
- Són sistemes molt barats i fàcils d'implementar
- Només suporten serveis mitjançant proxy
- El filtrat de paquets, es pot fer en Linux a través de "iptables" (http://www.linux-firewall-tools.com) que són sentències del tipus:

accept|deny amb declaració de ports, direccions IP, ...

Dual-Homed gateway



Screened subnet

- Se situa una xarxa DMZ (DeMilitarized Zone) entre la interna i l'externa, usant dos routers i que conté el bastió
- Trànsit sospitós s'envia cap al bastió, si no podeu saltar.
- Suporta serveis mitjançant proxy (bastió)
- Suporta filtrat de paquets (routers)
- És complicada i cara d'implementar
- Si l'atacant entra al bastió, encara té un router per davant (no pot fer sniffing)

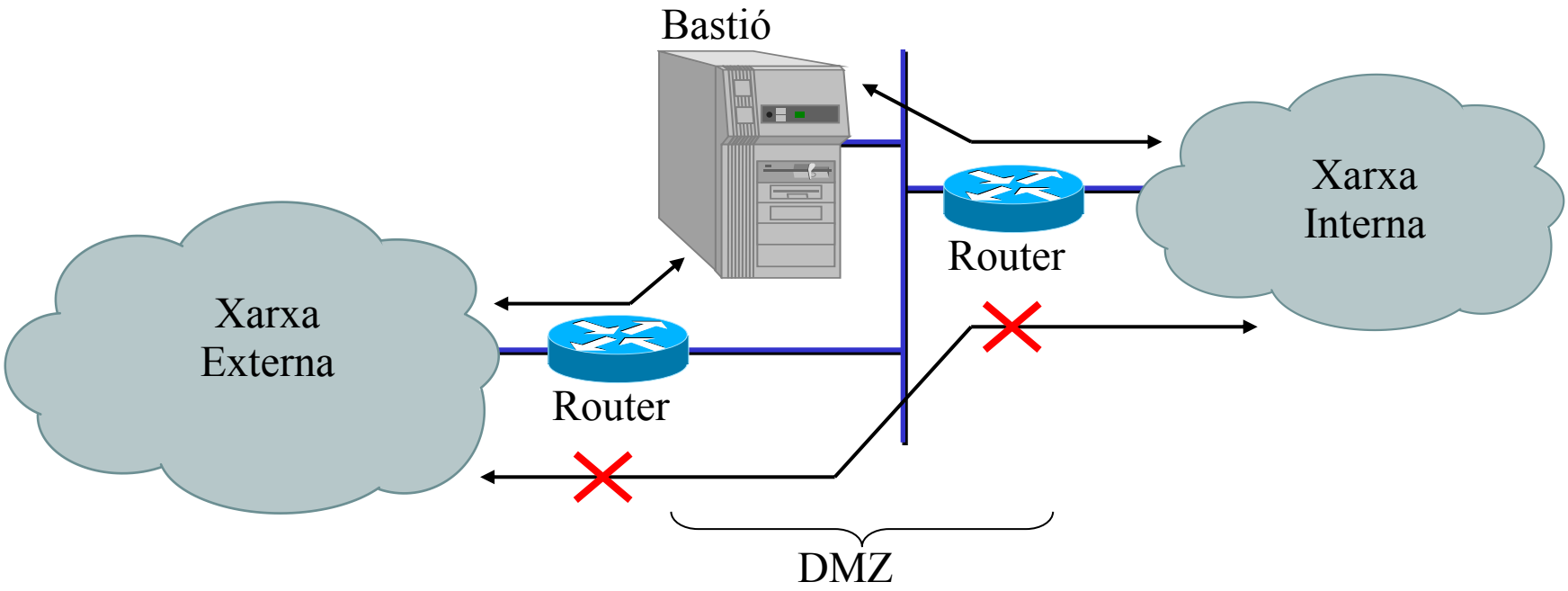
Screened subnet

Configuració: consisteix en implementar un perímetre amb 2 routers i un host bastió, és l'arquitectura més segura i té els avantatges que:

- en cap moment l'exterior pot saturar la xarxa interna, ja que estan separades.
- en cap moment es pot monitoritzar (detectar) la xarxa interna en el cas que el host bastió fora sabotejat. (sniffer).

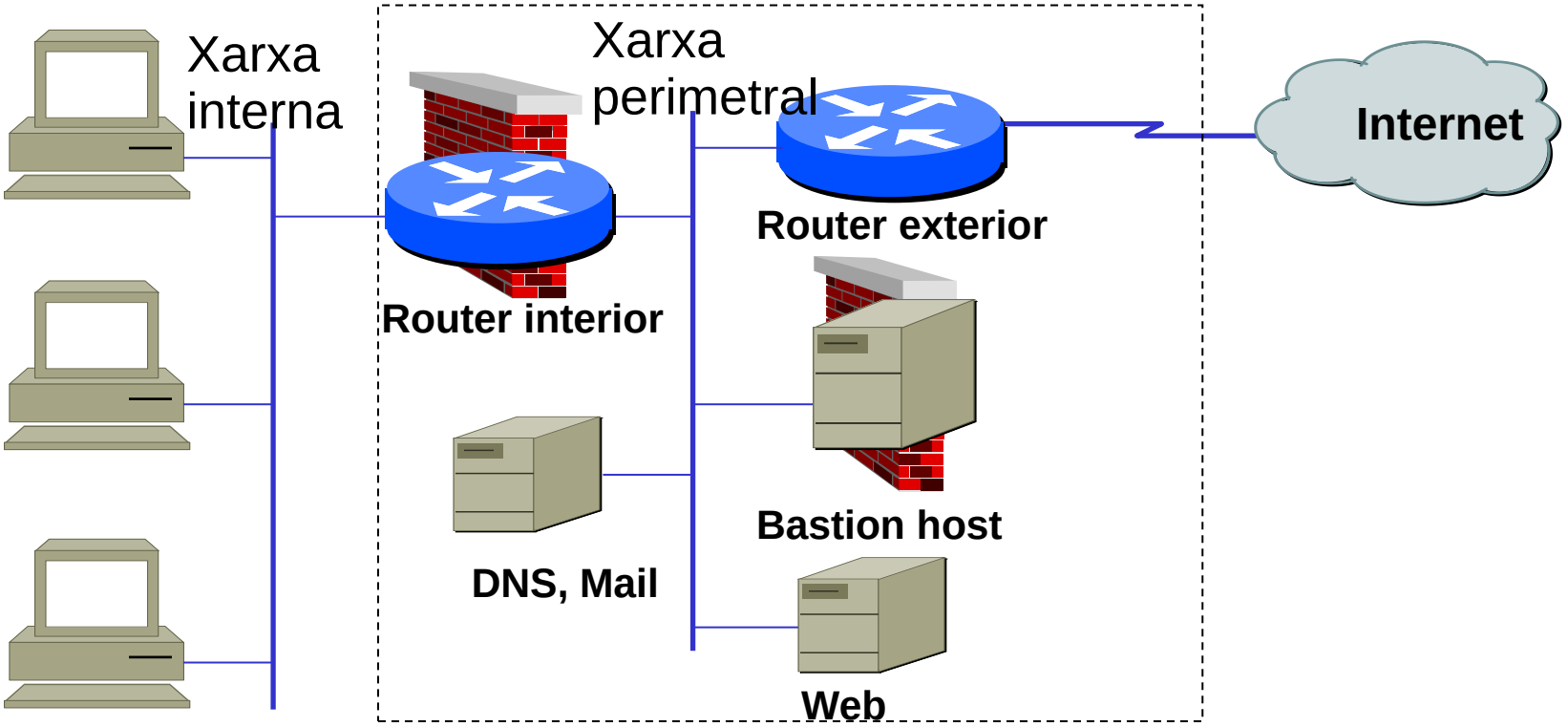
Firewalls / Tallafocs. Reguladors del transit:

Screened subnet



Firewalls / Tallafocs. Reguladors del transit:

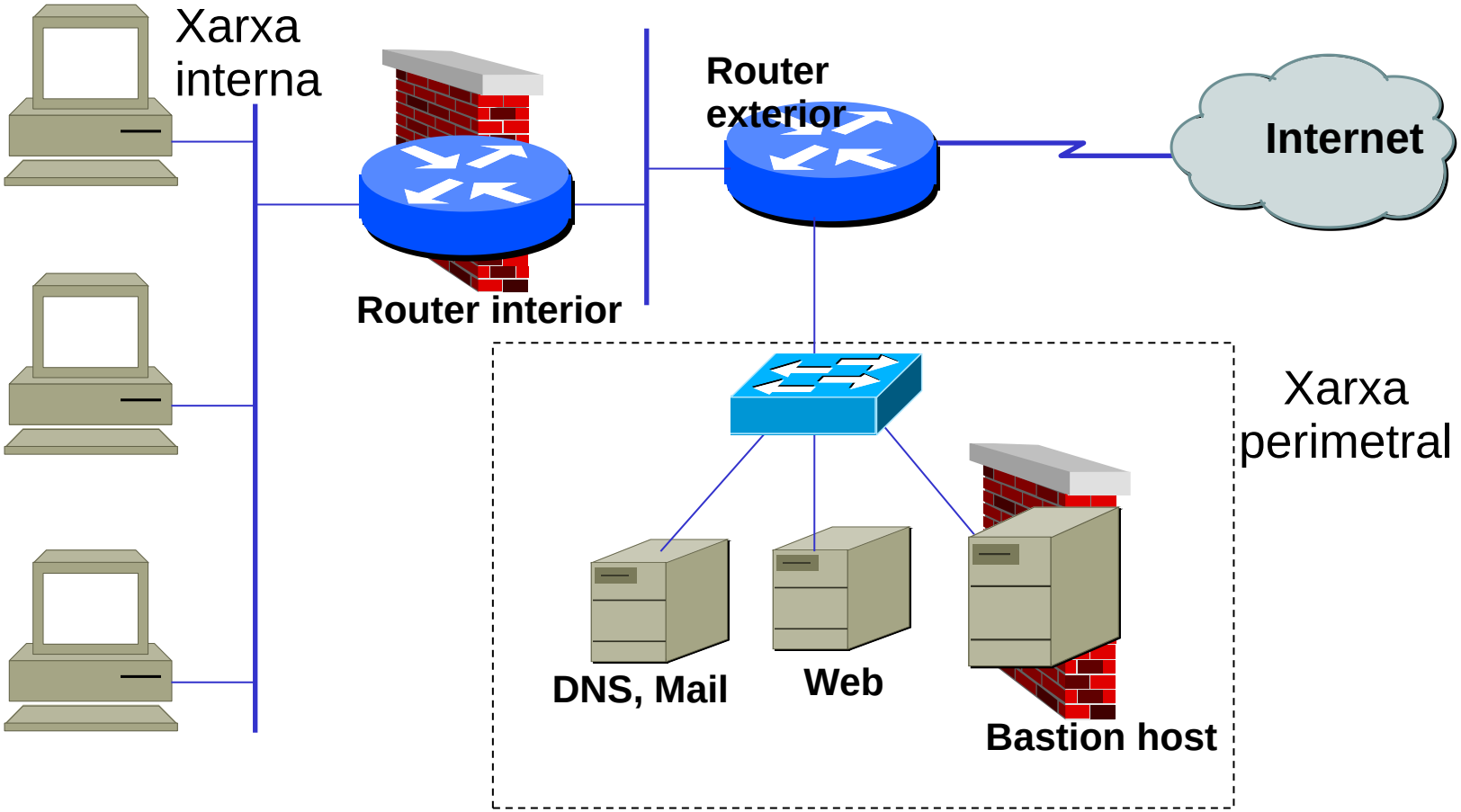
Exemple Tallafocs amb Zona Desmilitaritzada



Zona desmilitaritzada (DMZ)
o Free Trade Zone (FTZ)

Firewalls / Tallafocs. Reguladors del transit:

Tallafocs amb DMZ conmutada



Zona desmilitaritzada (DMZ)
o Free Trade Zone (FTZ)

Preparació del Router

- Definir la **access list** per redirigir el trànsit extern al bastió
- Rebutjar els missatges externs amb direcció interna (**anti-spoofing**)
- Deshabilitar la resposta als missatges "ICMP redirect“
- Treure el suport d'accés per telnet (almenys externament)
- Separar trànsit de gestió i de servei, mitjançant assignació de diferents direccions, o diferent localització

Preparació del node Bastió en UNIX

- Instal·lació segura del UNIX: Eliminar executables amb bit SUID i GUID i connexions a través de SSH
- Deshabilitar els serveis no requerits
  - NFS, XPAs, ftpd, bootd, CMU, rshd, rlogind, rexecd
- Instal·lar les passarel·les per als serveis requerits (proxies)
- Treure els executables i llibreries no essencials
- Instal·lar un sistema d'anàlisi de logs (swatch) en temps real
- Muntar els file systems possibles de només lectura
- Instal·lar un Tester d'integritat (Tripwire)
- Realitzar un backup complet del sistema net

Productes Comercials

- Comercials
  - Firewall-1 (Check Point)
  - IBM Firewall (International Bussines Machines)
  - Gauntlet (Trusted Information Systems)
  - Private Internet Exchange (PIX) de Cisco i / o CBACs Context Based
  - Access Control
- Lliure Distribució
  - FWTK (Trusted Information Systems)

Comentaris de tallafocs i seguretat

- Però aquestes configuracions no són suficients, en moltes ocasions poden aparèixer forats per zones no controlades, com accessos remots per mòdem, etc
- A més, les llistes d'accés són difícils de definir i de testejar, atès que es poden produir molts casos diferents que cal contemplar.
- Els tallafocs, que inclouen capa d'aplicació i interfície d'usuari, són més fàcils de configurar que les llistes d'accés. A més permet aplicacions addicionals com antivirus, filtra codi actiu, ... però disminueixen les prestacions.
- Tornem a insistir que addicionalment ha d'haver una bona política de seguretat, especificant tipus d'aplicacions a instal · lar, coses permeses i no permeses, polítiques de contrasenyes, etc

Limitacions dels tallafocs

- No protegeix d'atacs fora de la seva àrea.
- No protegeix d'espies o usuaris inconscients.
- No protegeix d'atacs de "enginyeria social“.
- No protegeix contra atacs possibles a la transferència de dades, quan dades són enviades o copiats a un servidor intern i són executats despatxant un atac.

Detecció d'intrusos: **IDS**

- Les vulnerabilitats dels diferents sistemes dins d'una xarxa són els camins per realitzar els atacs.
- En moltes ocasions, l'atacant emmascara l'atac en trànsit permès pel tallafocs i per tant per delatar es necessita un IDS. Són complementaris.
- L'augment d'aquest tipus d'atacs ha justificat la creació d'equips de respostes d'emergència informàtica (CERT: Computer Emergency Response Team), que òbviament també poden veure els intrusos.
- Característiques desitjables per a un IDS són:
  - contínuament en execució i s'ha de poder analitzar ell mateix i
  - detectar si ha estat modificat per un atacant
  - utilitzar els mínims recursos possibles
  - ha d'adaptar-se fàcilment als canvis de sistemes i usuaris, pel que en ocasions tenen "intel·ligència" per adaptar-se (aprendre per la seva experiència) i configurar.

Tipus de IDS segons localització

- NIDS (Network Intrusion Detection System): detecta els paquets armats maliciosament i dissenyats per no ser detectats pels tallafocs. Consta d'un sensor situat en un segment de la xarxa i una consola. Avantatge: no es requereix instal · lar programari addicional en cap servidor. Inconvenient: és local al segment, si la informació xifrada no pot processar

- HIDS (Host Intrusion Detection System): analitza el trànsit sobre un servidor. Avantatges: registra comandaments utilitzats, és més fiable, més probabilitat d'encert que NIDS.

Tipus de IDS segons models de detecció

- Detecció de mal ús: verifica sobre tipus il · legals de trànsit, seqüències que prèviament sap s'utilitzen per realitzar atacs (conegudes com exploits)

- Detecció d'ús anòmal: verifica diferències estadístiques del comportament normal d'una xarxa, segons franges horàries, segons la utilització de ports (evitaria el rastreig de

Tipus de IDS segons acció

- Passius: registren violació i genera una alerta
- Reactius: responen davant la situació, anul · lant sessió, rebutjant connexió pel tallafocs, etc

SNORT, un bon IDS

Snort és una eina molt utilitzada en la Seguretat Informàtica a nivell mundial. Snort és un Sniffer de paquets i un Sistema de Detecció d'intrusos (IDS), el qual disposa un llenguatge interpretatiu de regles, com patrons per a la monitorització dels sistemes informàtics d'una xarxa.

Defineix també una sèrie de regles i filtres ja predefinits, que es poden ajustar a les necessitats de l'usuari, que a més compta amb la capacitat d'emmagatzemar tot tipus de logs, en una bases de dades creada en MySQL.

SNORT, un bon IDS

Els IDS's utilitzen diferents tècniques d'anàlisi per alertar l'administrador en cas de veure accions sospitoses. Aquest en particular és un NIDS (N de Network) que s'encarrega d'analitzar el tràfic de xarxa, inspeccionant el contingut dels paquets per disparar alertes, o fins i tot, fer algun tipus d'acció quan detecta trànsit sospitós.

La idea és simple (implementar no ho és tant), Snort sniffa la xarxa i a través d'un conjunt de regles decideix si el trànsit és sospitós. Les regles contenen la informació que hauria de contenir un paquet per considerar-se sospitós, com ser la IP origen, el port origen, la IP destí, el port destí i el contingut del paquet. En les regles es poden utilitzar expressions regulars i s'ha d'incloure un missatge que descrigui què és el que detecta.

SNORT, un bon IDS

A més del motor de detecció, Snort proveeix preprocessadors. Els preprocessadors permeten als usuaris i programadors estendre la funcionalitat de Snort. El codi dels preprocessadors s'executa abans del motor de detecció, però després que el paquet que ha de ser descodificat.

És molt flexible i permet a l'usuari crear les seves pròpies regles i preprocessadors. Les regles s'emmagatzemen en path/snort/rules/ i tenen una sintaxi simple, els preprocessadors requereixen programació.

Honey Pot

- De vegades és interessant aprendre dels propis atacants.
- Per això, en les xarxes s'ubiquen servidors llocs expressament perquè els intrusos els sabotegen i són monitoritzats per sistemes que actuen com a ponts als servidors, registrant de forma transparent els paquets que accedeixen a aquests servidors.
- Detectat un atac (per modificació de l'estructura d'arxius), es recompon la traça de l'atacant (seqüència de paquets registrats al monitor pont) i es passa a una anàlisi forense.
- Aquesta anàlisi forense conclou, en cas de detectar un nou atac, en una nova regla de detecció.

Exemple: projecte Hades en http://www.rediris.es