

FIREWALL

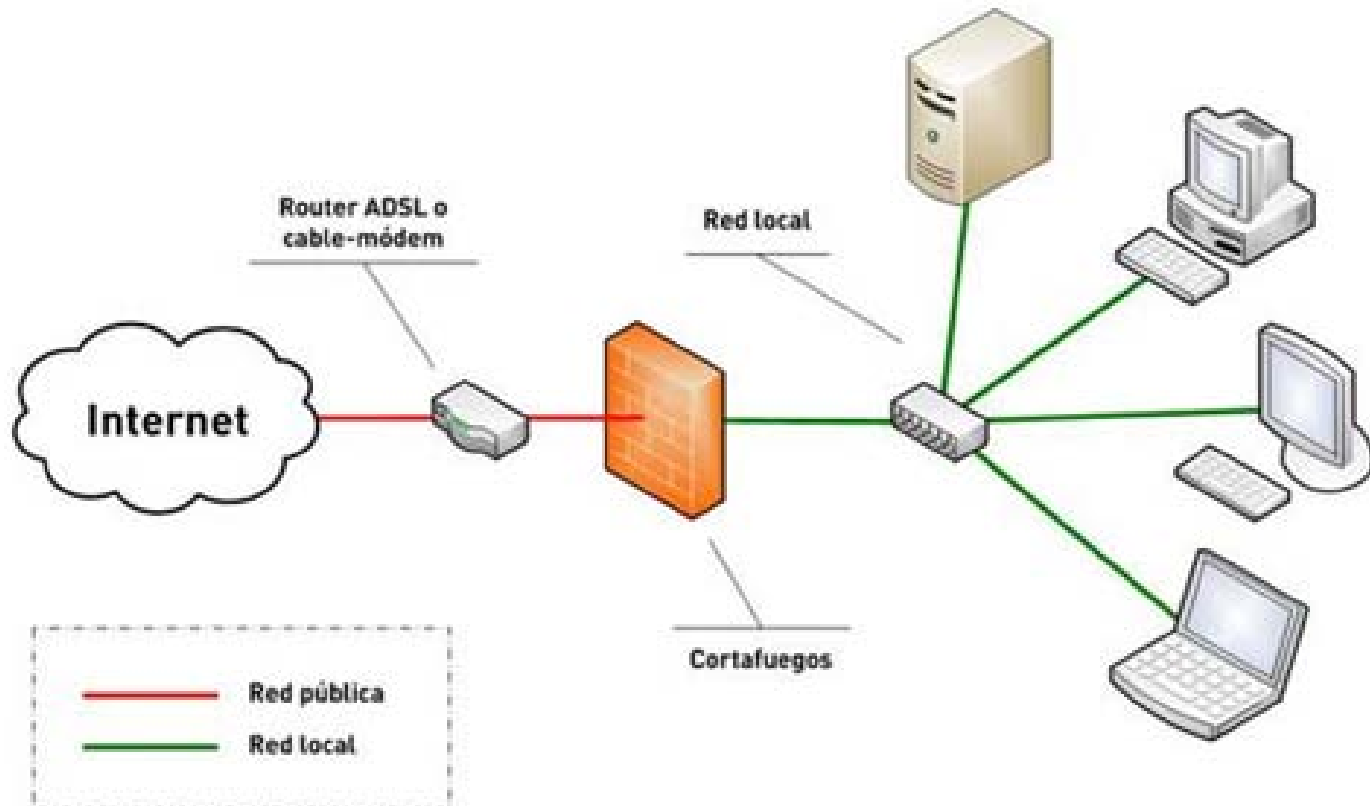
UF3.NF1: INSTAL·LACIÓ I CONFIGURACIÓ
DE TALLAFOCS

FIREWALL

- Sistema que controla el tràfic d'entrada i sortida d'una xarxa o un equip
- Els més habituals són a nivell de TCP/IP
 - > Filtren la informació en funció del port i l'adreça que contenen els segments TCP
- Hi ha dues polítiques per defecte:
 - > Acceptar tot el trànsit d'entrada i sortida i especificar al tallafocs què ha d'impedir.
 - > Denegar tot el trànsit d'entrada i sortida i especificar què pot deixar passar

FIREWALL

Estructura bàsica d'una xarxa amb tallafocs (on el tallafocs és el router)



FIREWALL

- Sistema que audita i evita els intents de connexió no desitjats (controla el tràfic d'entrada i sortida d'una xarxa o equip)
- Filtren els paquets a partir d'unes regles (tenint en compte, les adreces IP origen i destí i el servei de xarxa amb el que tenen relació)
- Funció primària dels tallafocs és delimitar zones amb diferents nivells de seguretat.

> Exemple, *screened router*

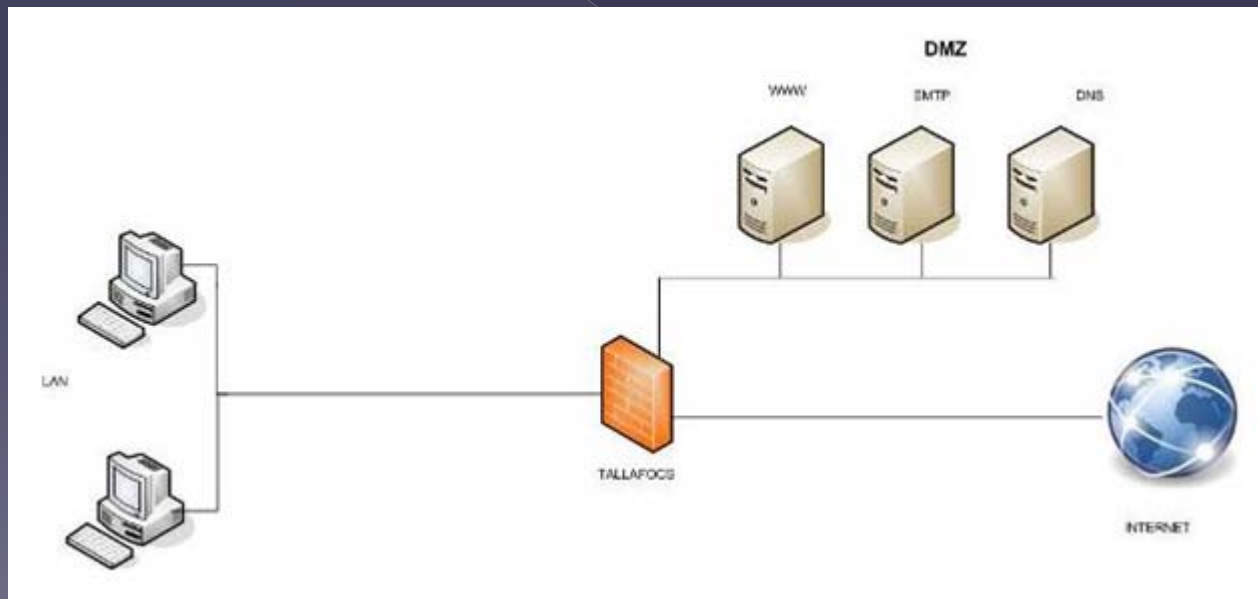
- *Dos zones: Segura i no Segura (Internet)*
- *Router : Delimitador entre zones.*

Nota: mòdem-routers dels ISP, inclouen els elements necessaris per bloquejar connexions entrants a través de determinats ports.



FIREWALL

- Podem establir nivells més detallats de filtratge de connexions entrants i sortints.
- Zona desmilitaritzada (DMZ)**, es gestiona amb unes regles diferents a les que s'apliquen pels equips de la LAN.



ALTRES FUNCIONS FIREWALL

- A més a més del filtre de paquets, l'ús de tallafocs ens ofereix una sèrie de serveis addicionals:

Servei	Definició
Bloqueig de trànsit no autoritzat	Restringeix serveis d'Internet, bloquejant pàgines Web o el trànsit provenient d'un rang d'adreces IP
Ocultació d'equips de la LAN	Ocultava equips per a que no siguin detectats per possibles atacs
Registre del trànsit	Com que el tallafocs s'instal·la a la frontera entre la xarxa interna i l'externa, detecta tot el trànsit que entra i surt de la xarxa, pel que pot emmagatzemar la seva activitat
Readreçament del trànsit entrant	Redirigeix el trànsit entrant a l'organització a la zona DMZ, evitant que arribi als equips locals
Limitació d'ample de banda	Limita l'ample de banda utilitzat per un protocol o un tipus de trànsit
Seguiment de trànsit i monitoratge d'atacs	Genera estadístiques amb dades sobre l'ample de banda consumit, permetent detectar, per exemple, si des d'un determinat equip s'està descarregant un alt volum de dades procedents d'Internet. Monitoritza els atacs des de l'exterior per prendre mesures com el bloqueig de l'anàlisi de ports per evitar els atacs més habituals.

TIPUS DE TALLAFOCS

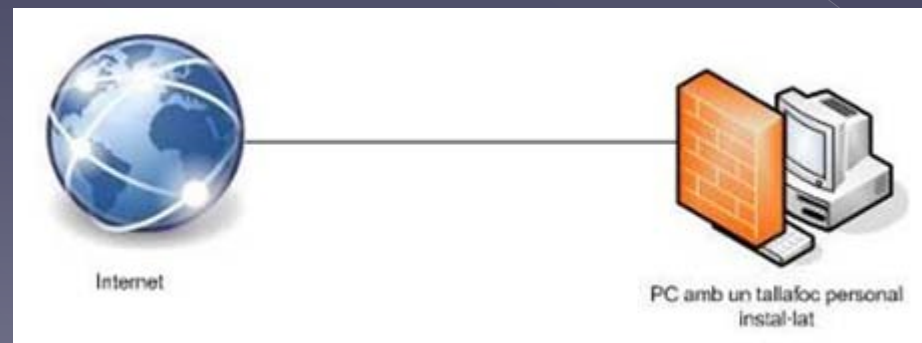
- Existeixen dos criteris de classificació:
 - > Segons la seva **UBICACIÓ**:
 - Tallafocs de sistema o personals.
 - Tallafocs de subxarxes
 - > Segons la seva **TECNOLOGIA** :
 - Tallafocs que actuen a nivell de paquets de dades.
 - Tallafocs que actuen a nivell de circuits
 - Tallafocs que actuen com a passarel·les d'aplicació
 - Tallafocs transparents



TIPUS DE TALLAFOCS

SEGONS LA SEVA UBICACIÓ

- **TALLAFOCS DE SISTEMA O PERSONALS:**
 - Restringeixen la comunicació no autoritzada amb un equip, actuant com un sistema de defensa perimetral.
 - Protegeixen els equips que pertanyen a xarxes privades particulars.
 - Per exemple, en un equip domèstic el tallafocs pre-instal·lat en sistemes Windows.



TIPUS DE TALLAFOCS

SEGONS LA SEVA UBICACIÓ

○ TALLAFOCS DE SISTEMA O PERSONALS:



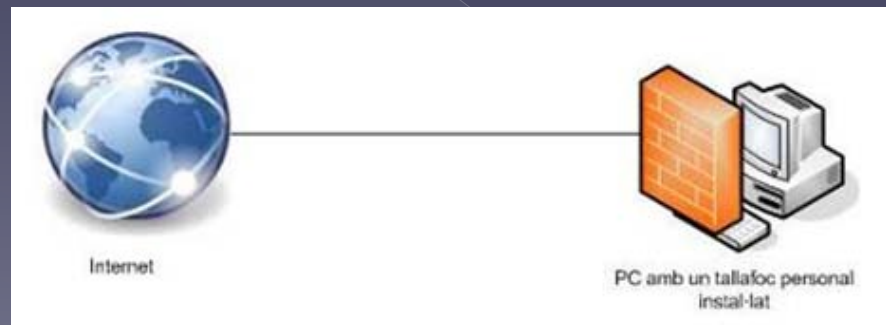
> Proporciona 5 funcions principals:

- Permet supervisar totes les connexions amb l'exterior, incloent els accessos a serveis d'Internet.
- Permet monitorar els programes locals que intenten accedir a Internet per a que l'usuari pugui decidir si permet que ho facin o no.
- Proporciona mecanismes per bloquejar els possibles intents d'intrusió a l'equip o altres atacs (com l'atac de denegació de servei) realitzats des d'internet.
- Realitza un registre de totes les connexions realitzades des de l'equip.
- Alguns incorporen filtres anti-spam, detecció de virus o altres codis que poden ser perjudicials per l'equip.

TIPUS DE TALLAFOCS

SEGONS LA SEVA UBICACIÓ

- **TALLAFOCS DE SISTEMA O PERSONALS:**
 - > En l'actualitat, es troben:
 - Integrats dins del paquet de seguretat, **ANTIVIRUS**, com Panda o McAfee.
 - Integrats en els propis **SISTEMES OPERATIUS**, com el tallafocs que incorpora Windows XP/Vista/7.
 - > Cal mantenir el sistema operatiu i tallafocs actualitzats.



TIPUS DE TALLAFOCS

SEGONS LA SEVA UBICACIÓ

○ TALLAFOCS DE SUBXARXES:

> Principals funcions:

- Autorització de serveis (entrants i sortints)
- Control d'accés als serveis basant-se en la identitat de l'usuari o equip
- Registre i monitoratge d'accés a la xarxa.

