



# Seguretat operacional (2)

Organitza:



SOC

Servei d'Ocupació  
de Catalunya

Generalitat  
de Catalunya



Unió Europea  
Fons Social Europeu  
L'FSE inverteix en el teu futur

Imparteix:

UOC  
Universitat  
Oberta de Catalunya

Col·labora:

MOBILE  
WORLD CAPITAL.  
BARCELONA

[PQ]  
[TM] Pla de  
Qualificació en  
Tecnologia  
Mòbil

# Tallafocs

## Mecanismes de prevenció

Joaquín García Alfaro

P07/05070/02623



# Sistemes tallafoc

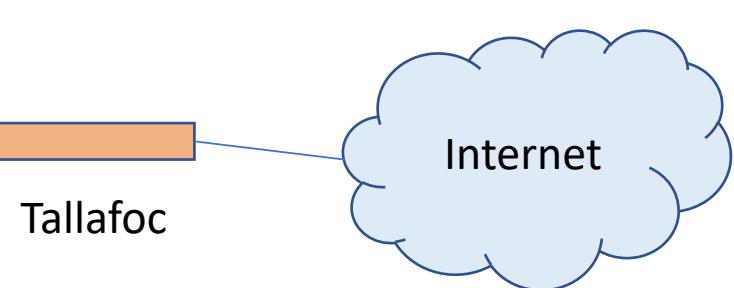
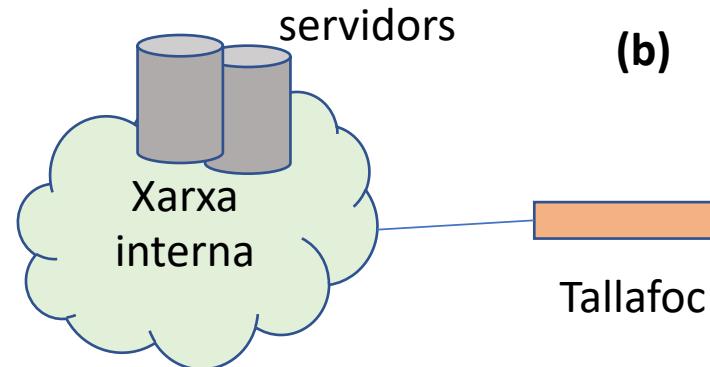
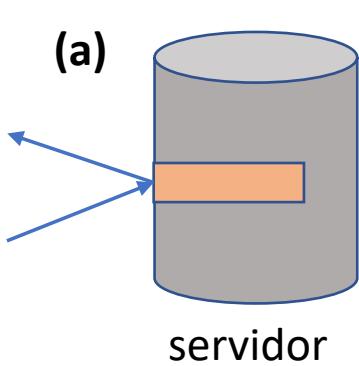
- Construcció de sistemes tallafoc
- Encaminadors amb filtratge de paquets
- Zones desmilitaritzades
- Tallafocs de nova generació

# Construcció de sistemes tallafoc

- Els serveis que requereixen connectivitat a Internet (web, DNS, smtp...) poden ser víctimes d'atacs que poden venir de qualsevol punt.
- Aquests serveis s'allotgen en servidors, que poden ubicar-se en les instal·lacions de l'organització.
  - En aquest sentit noteu que els serveis també podrien ser atacats des de la pròpia xarxa de l'organització!

# Construcció de sistemes tallafoc

- Un sistema tallafoc actua com una barrera per reforçar el control d'accés als serveis que s'executen en una màquina.
- Un parell d'exemples:
  - a) Un servidor pot tenir un tallafoc instal·lat, per controlar l'accés als seus serveis.
  - b) Una organització pot tenir un tallafoc que separa la xarxa Internet de la xarxa interna de l'empresa (**seg. perimetral**)



# Construcció de sistemes tallafoc

- Un tallafoc ha de ser un punt ben protegit del sistema, si falla el tallafoc hi pot haver possibles intrusions.
- Cal utilitzar sistemes operatius degudament actualitzats, firmware actualitzat, etc.
- La gestió del tallafoc ha d'estar degudament controlada:
  - Sessions remotes ssh amb autenticació de client per mitjà de clau privada, sessions web autenticades (HTTPS) amb certificat de client, etc.

# Construcció de sistemes tallafoc

- **Característiques addicionals dels sistemes tallafoc**
  - **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 protegeixen la xarxa contra codi maliciós inserit en les seves pàgines.

# Construcció de sistemes tallafoc

- **Característiques addicionals dels sistemes tallafoc**
  - **Xarxa privada virtual.** Aquest tipus de funcionalitat oferida 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).

# Construcció de sistemes tallafoc

- **Característiques addicionals dels sistemes tallafoc**
  - **Traducció d'adreces d'internet.** Encara que no es tracta estrictament d'una funcionalitat relacionada amb la seguretat, la majoria dels sistemes tallafoc ofereixen la possibilitat de realitzar NAT.

Després veurem aquest concepte amb més deteniment.

# Construcció de sistemes tallafoc

- **Característiques addicionals dels sistemes tallafoc**
  - **Balanceig de càrrega.** Permet distribuir el trànsit HTTP entre diferents servidors.
  - **Tolerància a fallades.** Arquitectura de diversos tallafocs redundants.
  - **Detecció d'atacs i intrusions.** Noteu que el mateix tallafoc pot analitzar el trànsit per cercar atacs i intrusions, després veurem quina importància té això.

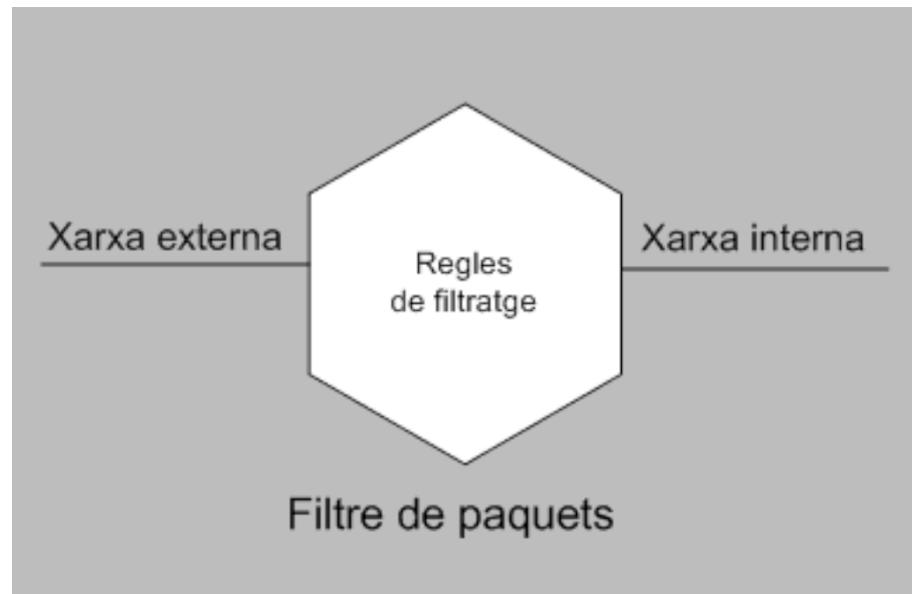
# Construcció de sistemes tallafoc

## ■ Implementació

- Primer coneixerem el concepte d'encaminador amb filtratge de paquets, una de les maneres clàssiques d'implementar un tallafoc.
- En segon lloc, descriurem el concepte de zona desmilitaritzada.
- Finalment, parlarem dels tallafocs de nova generació.

# Encaminadors amb filtratge de paquets

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



# Encaminadors 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, verificant el trànsit de dades legítim entre ambdues parts.
- Els paquets s'accepten o deneguen en funció de les capçaleres IP, UDP, TCP, ICMP:
  - Adreces origen / destí
  - Tipus de protocol
  - Ports d'origen / destí
  - Contingut dels paquets
  - Mida del paquet

# Encaminadors amb filtratge de paquets

- Es poden definir unes **polítiques per defecte**, és a dir:
  - Per defecte denegar tot el trànsit i fer regles per decidir quines s'accepten.
  - Per defecte acceptar tot el trànsit i fer regles per decidir quines es rebutgen.
- *Què creieu que és millor? Teniu alguna experiència al respecte?*

## Exemples de configuració

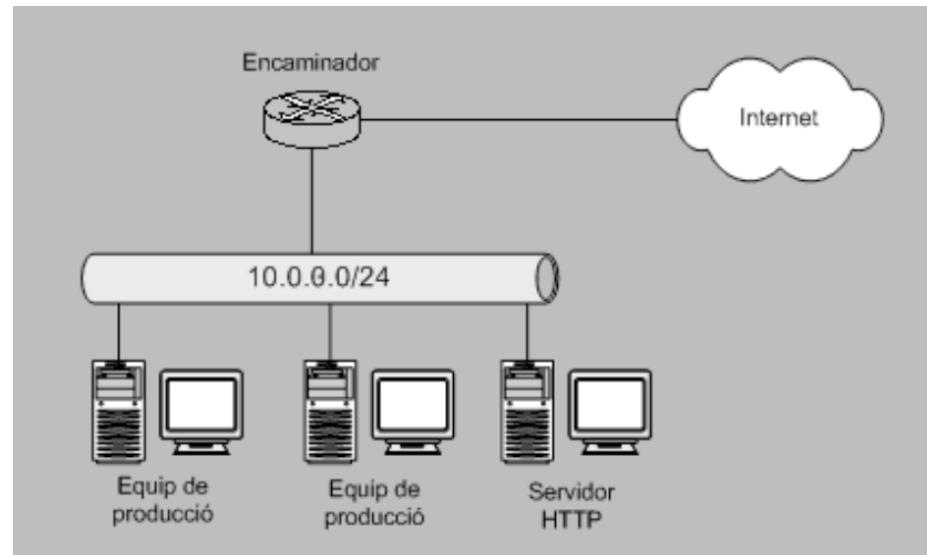
En la figura següent es presenta una possible xarxa a on s'ha implantat la següent política de seguretat mitjançant la configuració d'un conjunt de regles de filtre de paquets aplicades en el mateix encaminador:

- 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).

## 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).



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

# Encaminadors amb filtratge de paquets

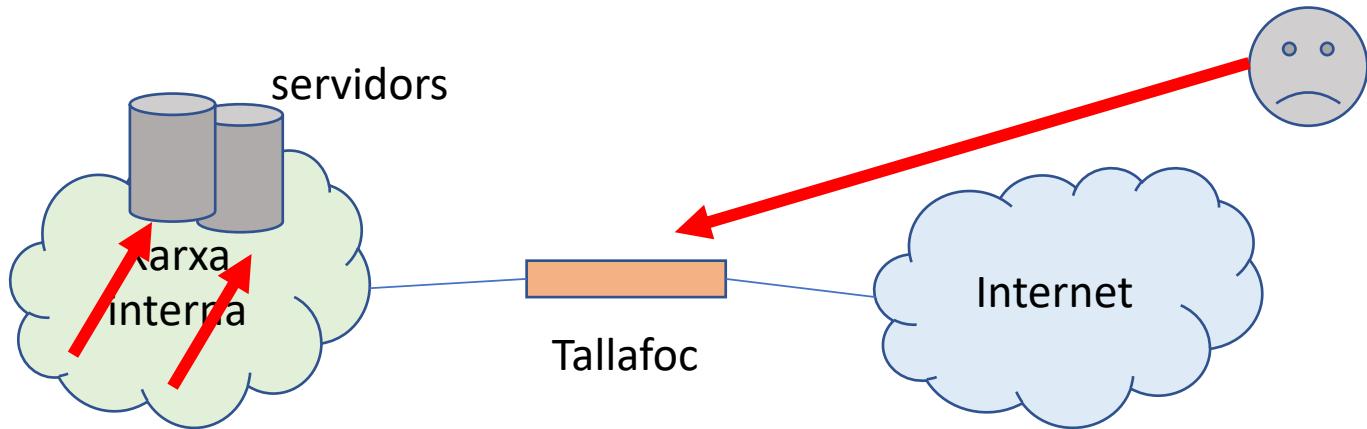
- Com definim...
  - a) Les regles corresponents a permetre el trànsit cap a un servidor web.
  - b) Les regles corresponents a permetre el trànsit cap a un servidor DNS

# Encaminadors amb filtratge de paquets

- Com definim...
  - c) Les regles corresponents a permetre el trànsit en un servidor IMAP.
  - d) Les regles corresponents a permetre el trànsit en un servidor SMTP.

# Zones desmilitaritzades

- Volem protegir uns servidors...

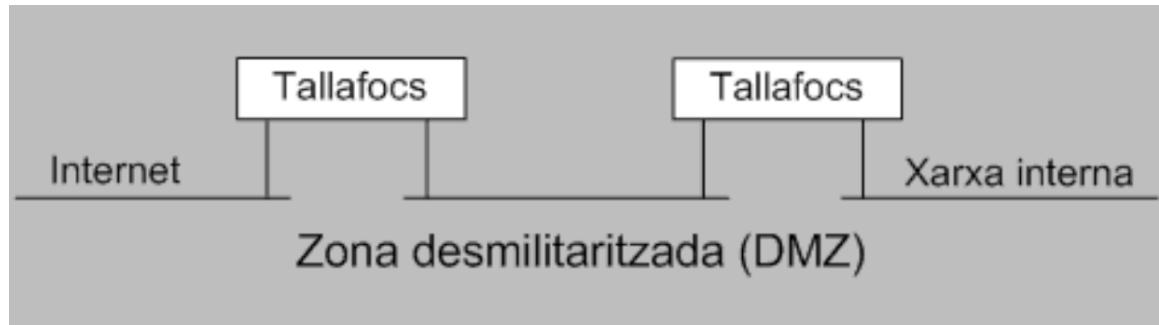


- Atacs des de l'exterior
- Atacs des de l'interior

Òbviament, els servidors s'han de protegir a nivell físic, però suposem que l'organització ja ha pres les mesures necessàries.

# Zones desmilitaritzades

- Una zona desmilitaritzada (DMZ) és una zona l'accés a la qual està controlada, en general, per dos tallafocs.
  - Un tallafocs separa l'exterior de la DMZ, mentre que un altre separa la xarxa interna de la DMZ.
  - Si un atacant accedeix a la DMZ la xarxa interna segueix estant protegida (seguretat per capes).
  - Es dificulta l'accés als servidors des de la xarxa interna.

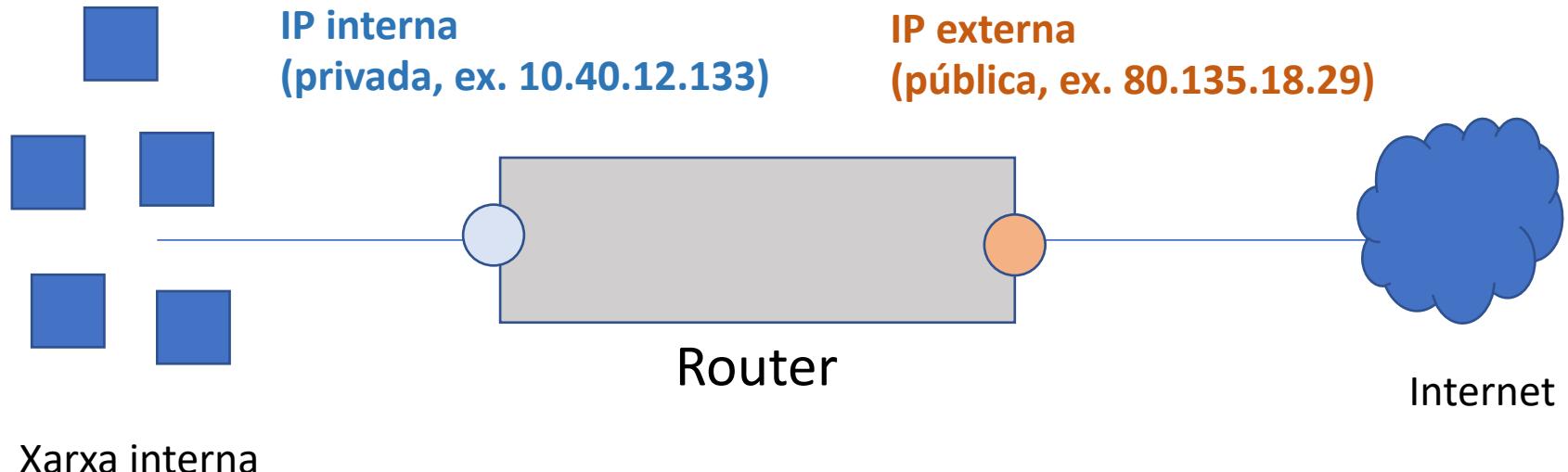


# Zones desmilitaritzades

- La política de denegació per defecte, juntament amb l’obertura dels serveis necessaris, permetran protegir els equips de la DMZ i, de retruc, la xarxa interna.
- Noteu que les màquines de la xarxa interna estan “desprotegides”: es suggereix l’ús de tallafocs a nivell local.

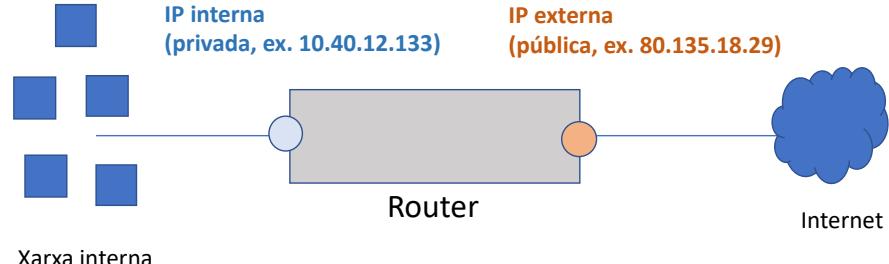
# NAT PAT?

- Routers i adreces



En general, hi ha una única IP externa, però se'n poden llogar vàries. Amb el *port forwarding* podem assignar una IP externa cap a una de les màquines internes, com ara un servidor.

# NAT PAT?

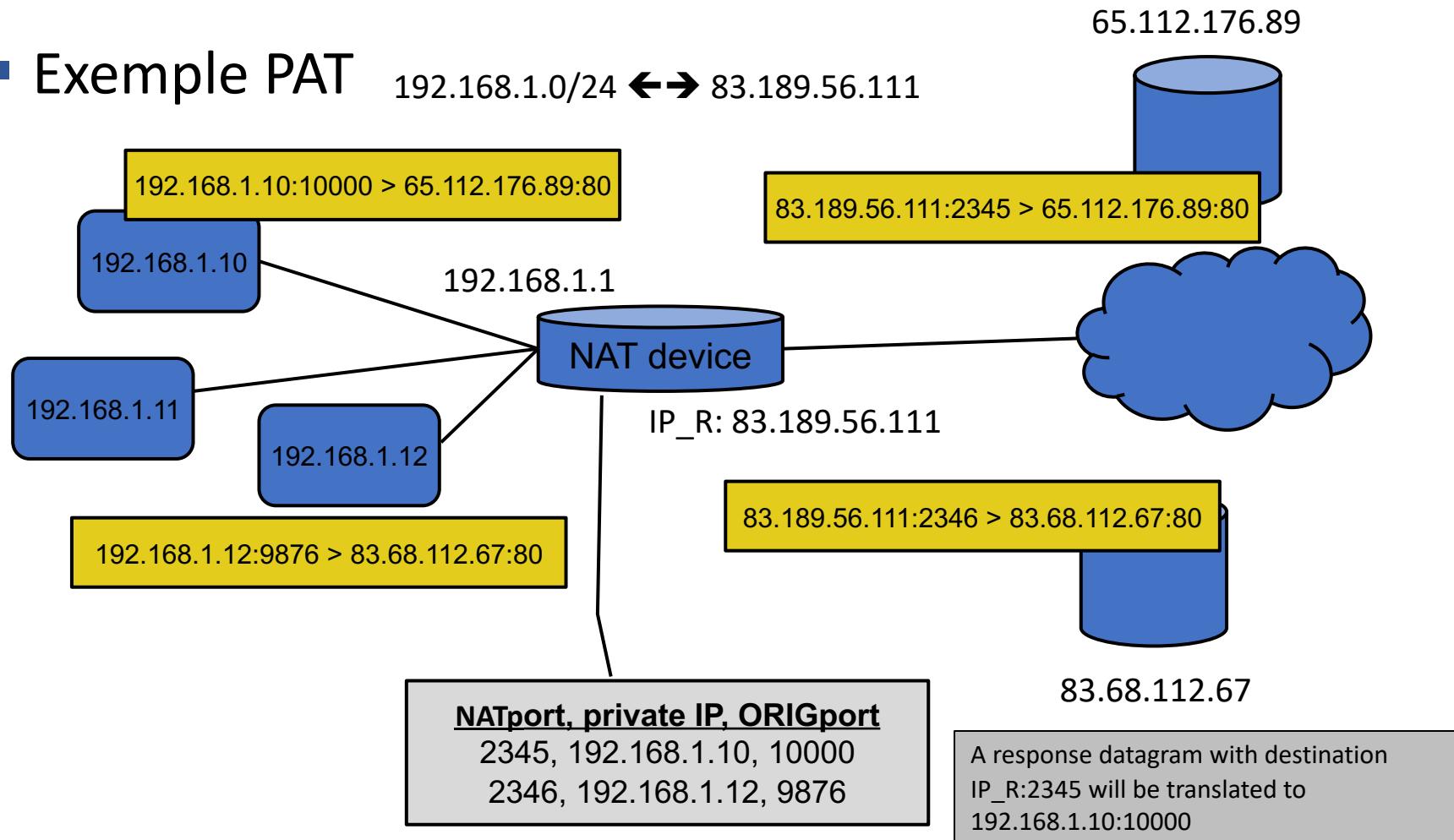


## ■ Routers i adreces

- Ara bé, si tenim només una única IP externa, com la poden compartir les diferents màquines de la xarxa interna?
- Gràcies al PAT (*Port-Address Translation*, una variació del *Network-Address Translation* o NAT), el router (dispositiu NAT) utilitza el número de port per saber a qui corresponen les comunicacions.
- Vegem un exemple!

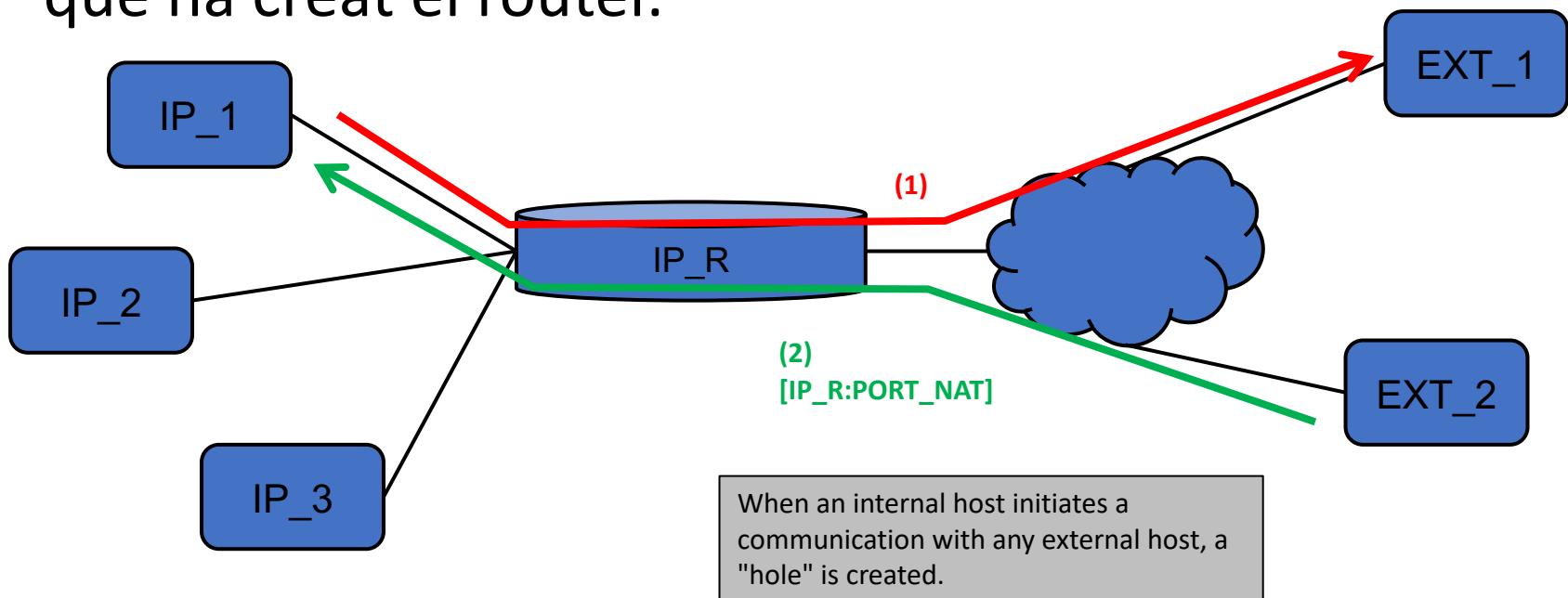
# NAT PAT?

## ■ Exemple PAT



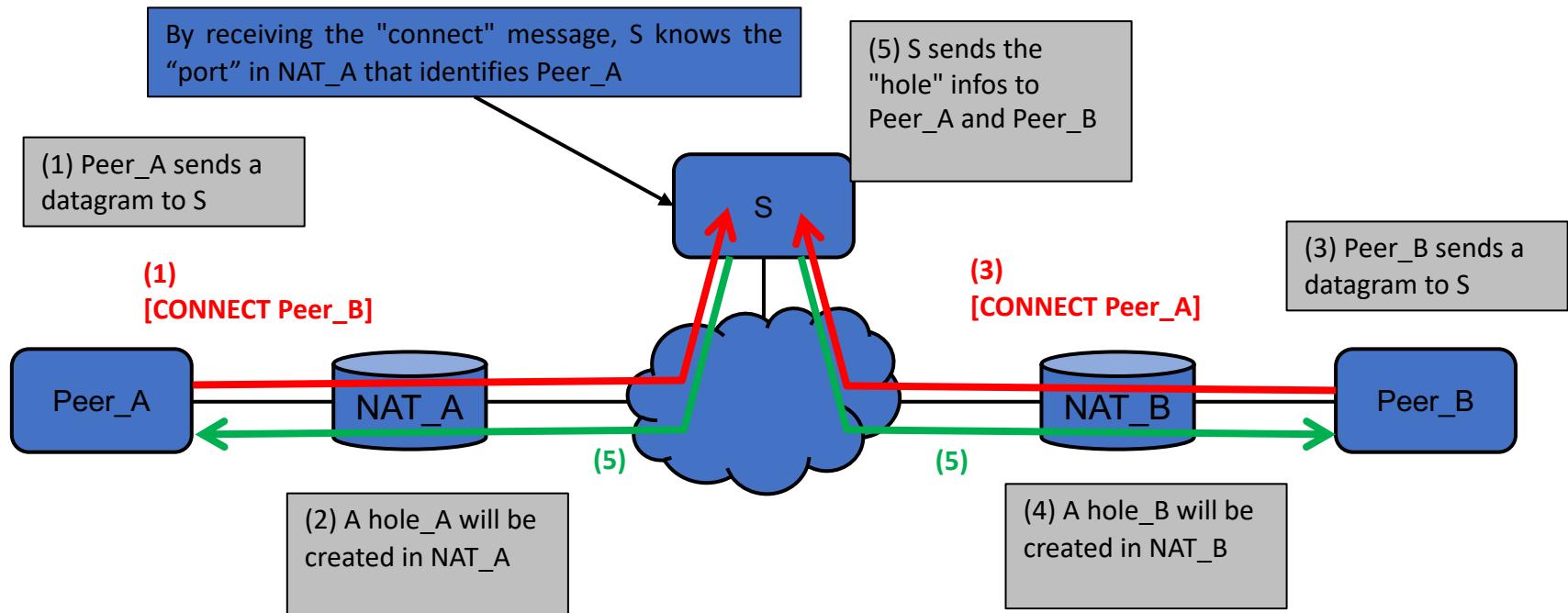
# NAT PAT?

- La màquina EXT\_2 pot accedir a IP\_1 gràcies al “forat” que ha creat el router.



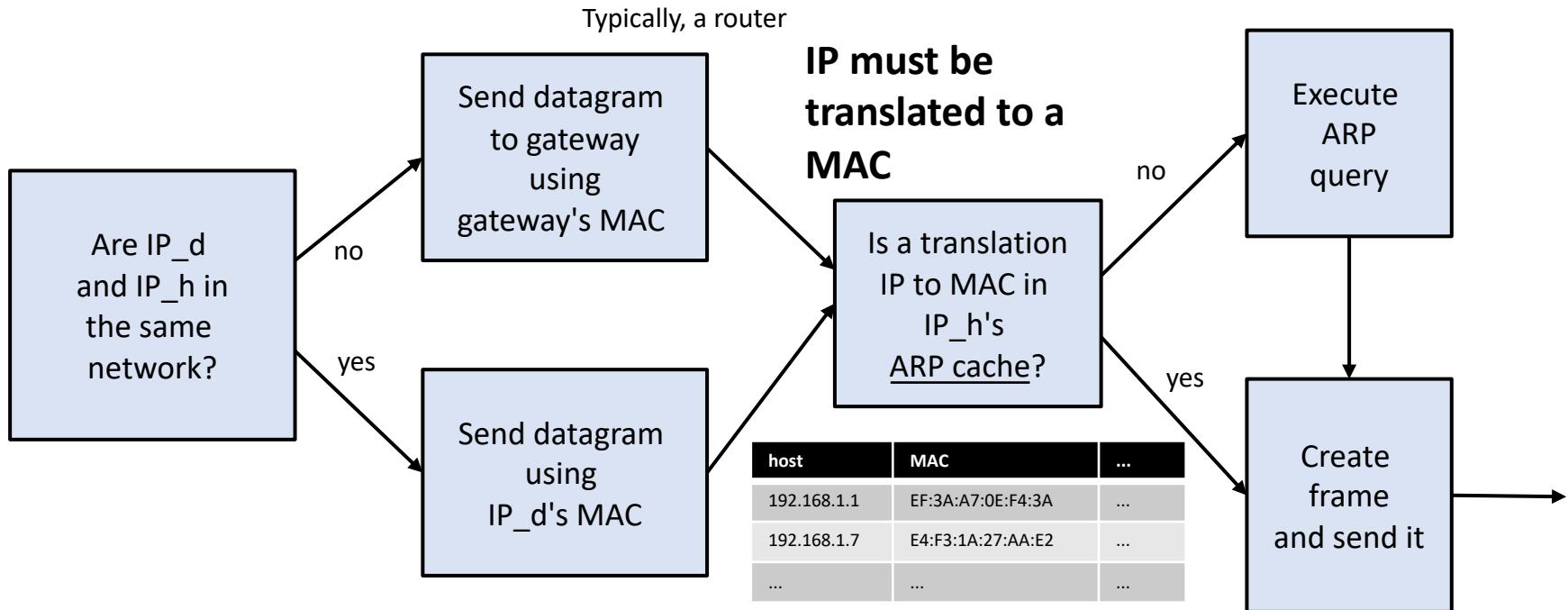
# NAT PAT?

- Comunicació per mitjà de skype i similars



# NAT PAT?

- Com s'envien datagrames entre diferents màquines d'una LAN que usa IP?



# Tallafocs SOHO

- Small Office Home Office



## Firewall settings

Firewall allows you to filter traffic, set up port forwarding or expose certain services to the outside world.

**Enable firewall**



# Tallafocs SOHO

## ■ Small Office Home Office

### Add / Edit Port Forwarding

Enable

Rule Name

Source Zone

Destination Zone

Source IP Address  Source IP Address

Dst. Device

Dst. IP Address

Protocol

Source Port(s)

Destination Port(s)



Noteu que la política és denegació per defecte i hem d'anar afegint regles de “port forwarding”.

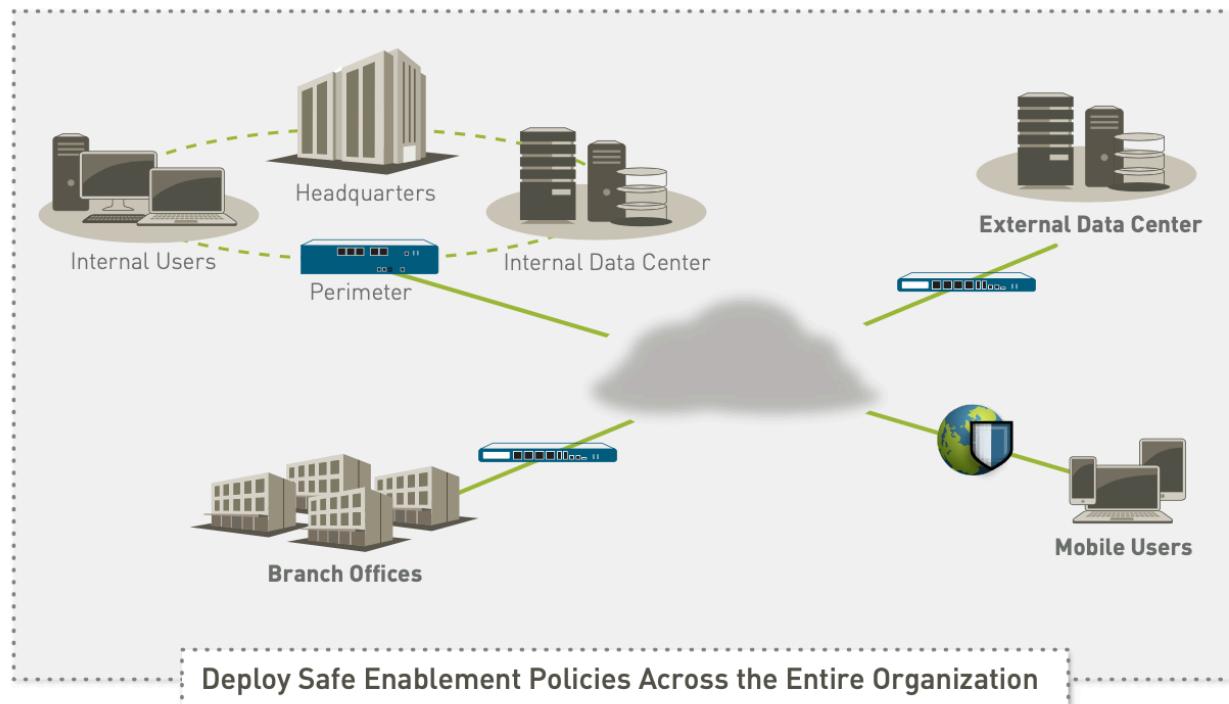
# Tallafochs de nova generació

- **Primers tallafocs:** filtratge de paquets (<1993)
- **1a Generació:** *stateful inspection*
  - Accepten **una connexió** segons unes regles. Quan acaba la connexió (TCP FIN) o després d'un timeout, ja no es permet el tràfic.
  - Monitoritzen els paquets d'una connexió, són més segurs que els primers tallafocs.
- **2a Generació:** maquinari específic (1995-1999)
  - Cisco PIX...
- **3a generació:** integració amb IDS (2000-2005)
- **Next Generation Firewalls (NGFW >2006)**



# Tallafocs de nova generació

- Gestió i anàlisi avançats de la seguretat perimetral d'una xarxa.
- Si hi ha diferents ubicacions geogràfiques, diversos NGFW poden actuar **coordinadament**.

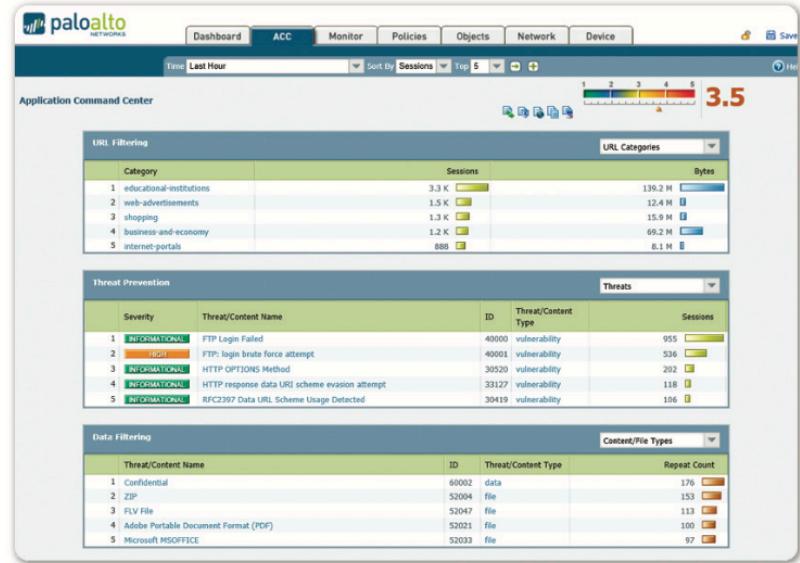


# Tallafocs de nova generació

- Es fonamenten en:
  - **Anàlisi de les aplicacions** que s'utilitzen, no només de ports i paràmetres de les capçaleres.
  - **Potent visualització de dades** i la facilitat de gestió. Integració de serveis de directori per mostrar informació en relació als usuaris de la xarxa, i no només en relació a les IP origen/destí de l'organització.
  - **Protecció contra amenaces conegeudes.** Prevenció d'intrusions i anti-malware. Programari sospitos s'executa en un *sandbox* i es posa a disposició del tècnic de seguretat. Detecció de màquines internes que es comporten com a *zombies*.
  - etc.

# Tallafocs de nova generació

- Focus en l'ús d'Internet:
  - Limitar ús de webmail, whatsapp, etc.
  - Aplicar polítiques de QoS per garantir ample de banda suficient per a tots els usuaris d'acord amb les demandes (temps real vs no temps real).
  - Controlar Facebook, permetent-ne l'ús però impedint que s'hi jugui.
  - Potent filtratge de webs no permeses i webs perilloses, connexió a repositori de llistes negres.
  - Registre de les activitats, alarmes, etc.



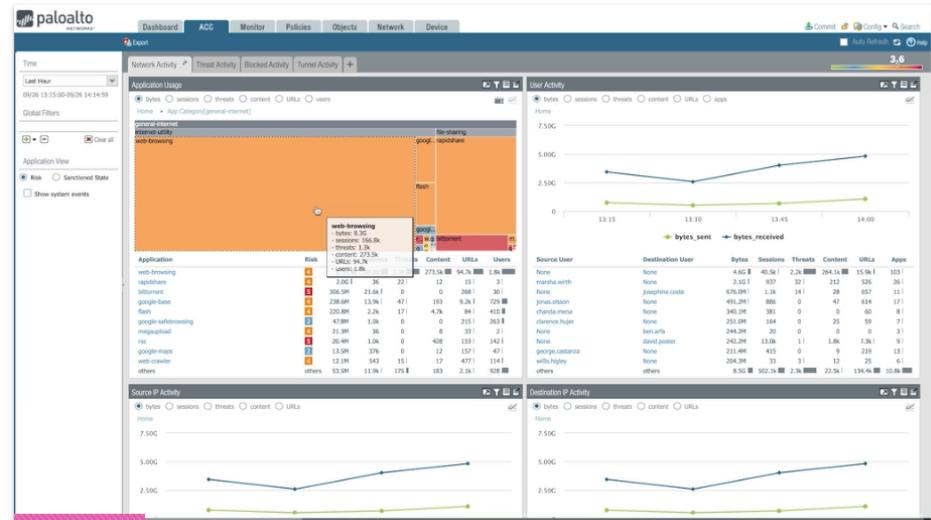
# Tallafocs de nova generació

## ■ Com funcionen?



### PA-3020

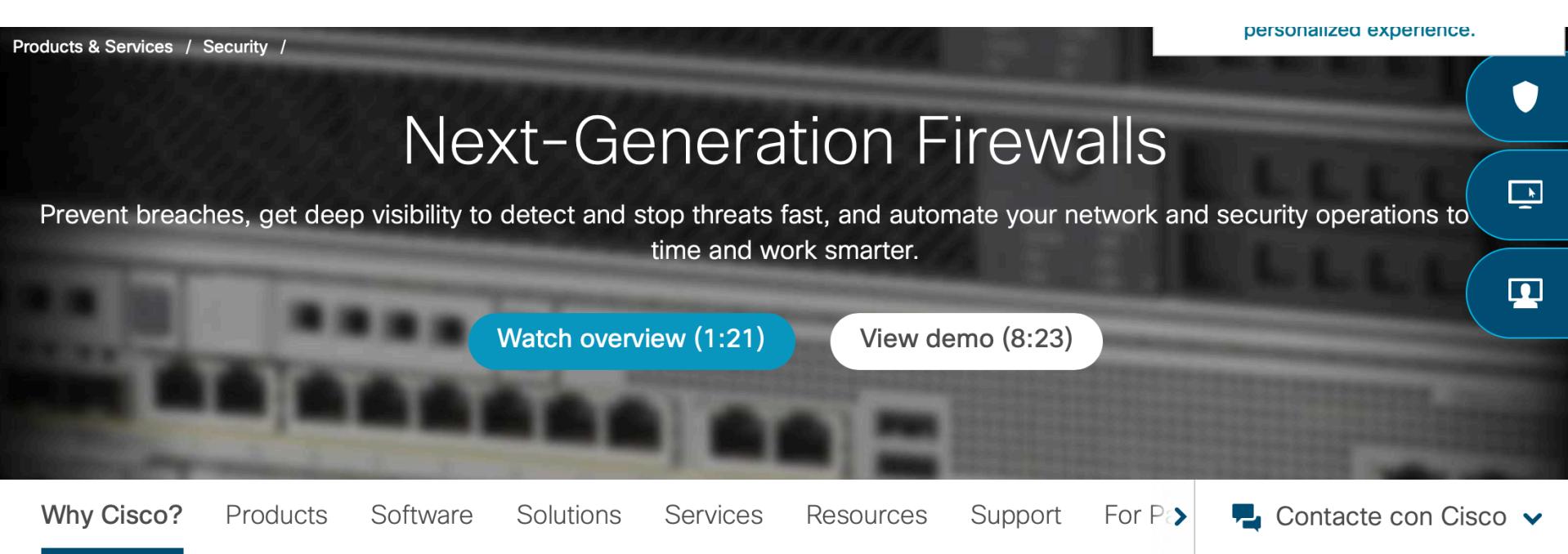
- 2 Gbps firewall throughput (App-ID enabled)
- 1 Gbps Threat Prevention throughput
- 500 Mbps IPsec VPN throughput
- 250,000 max sessions
- 50,000 new sessions per second
- 3,000 IPsec VPN tunnels/tunnel interfaces
- 1,000 SSL VPN users



<https://www.paloaltonetworks.com/resources/demos/ngfw-demo>

# Tallafocs de nova generació

- Com funcionen?



A screenshot of the Cisco website for Next-Generation Firewalls. The page features a large banner with the title "Next-Generation Firewalls" and a subtext: "Prevent breaches, get deep visibility to detect and stop threats fast, and automate your network and security operations to save time and work smarter." Below the banner are two call-to-action buttons: "Watch overview (1:21)" in a blue rounded rectangle and "View demo (8:23)" in a white rounded rectangle. The top navigation bar includes links for "Products & Services / Security /" and "personalized experience." The bottom navigation bar has links for "Why Cisco?", "Products", "Software", "Solutions", "Services", "Resources", "Support", "For Pa>" (partially visible), and "Contacte con Cisco".

<https://www.cisco.com/c/en/us/products/security/firewalls/index.html>

# iptables

- Netfilter/iptables és un framework del nucli Linux que permet interceptar i manipular paquets de xarxa. És un tallafocs amb filtratge de paquets.
- Es pot executar en una màquina (servidor, estació de treball) o en màquines que fan de router (amb vàries interfícies de xarxa). En aquest cas permet fer NAT (*masquerading*)
- Incorpora un mòdul per a *stateful filtering*.
- És gratuït, però s'ha d'executar en un ordinador. Això era molt divertit, però potser pels requeriments de rendiment actuals en una organització potser es queda curt i cal optar per una solució més avançada.

# iptables

- Es defineix una **taula de filters amb tres cadenes**:
  - **INPUT**, tots els paquets destinats al FW travessen aquesta cadena.
  - **OUTPUT**, tots els paquets creats pel FW travessen aquesta cadena.
  - **FORWARD**, tots els paquets que són redirigits pel FW travessen aquesta cadena.
- Addicionalment, hi ha la taula NAT, per traduir adreces de xarxa i la MANGLE, per fer ajustos.

# iptables

- Cal definir regles sobre les cadenes anteriors, basades en els paràmetres de TCP, UDP, IP.
- Quan un paquet es filtra i coincideix amb la regla, té una destinació:
  - ACCEPT, quan un paquet s'accepta
  - DROP, quan un paquet es rebutja
  - REJECT, quan un paquet es rebutja i envia un missatge de rebuig al remitent.
  - LOG, per anotar que el paquet coincideix amb la regla.
- **Podem afegir les regles una a una, o bé tindrem un script.**

# iptables

- **iptables -L -n -v**
  - Per mostrar informació de configuració del tallafocs
  - -L, llista regles
  - -n, mostrar adreces IP com a números i no resoldre DNS
  - -v verbose, informació detallada
- **service iptables stop, start, restart**
  - Aturar, iniciar i reiniciar iptables.

# iptables

- **iptables -F**
- **iptables -X**
  - Ens elimina la configuració de tallafocs
- **iptables -P INPUT DROP**
  - Per als INPUT la política per defecte és DROP
- **iptables -L INPUT -n --line-numbers**
- **iptables -D INPUT 4**
  - Mostra el número de línia de les regles de la cadena INPUT
  - Elimina la regla 4 de la cadena INPUT

# iptables

- **iptables -A INPUT -i lo -j ACCEPT**
- **iptables -A OUTPUT -o lo -j ACCEPT**
  - Permet la gestió local del tallafoc.
- **iptables -A INPUT xxxxxxxxxxxxxxxx**
  - Afegim la regla a la darrera posició de la cadena INPUT.
- **iptables -I INPUT 2 xxxxxxxxxxxxxxxx**
  - Inserirem la regla en la segona posició de la cadena INPUT.

# iptables

- **iptables -A INPUT -p icmp -j DROP**
  - Impedir pings (si política per defecte és ACCEPT)
  - p vol dir ‘protocol’
  - j vol dir ‘jump’
  
- **iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j ACCEPT**
  - Acceptar accés des de la MAC especificada (si la política per defecte és DROP)
  - m vol dir ‘module’

# **iptables**

- **iptables -A INPUT -p tcp --dport 80 -j ACCEPT**
  - Accepta els paquets amb protocol tcp i port destí 80.
- **iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT**
  - Accepta els paquets amb protocol tcp i port origen 80.

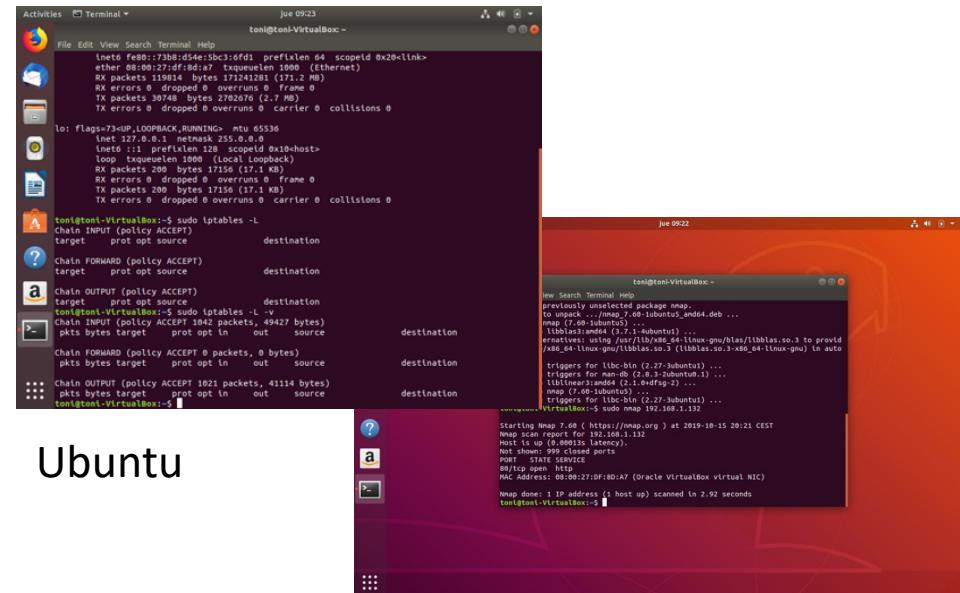
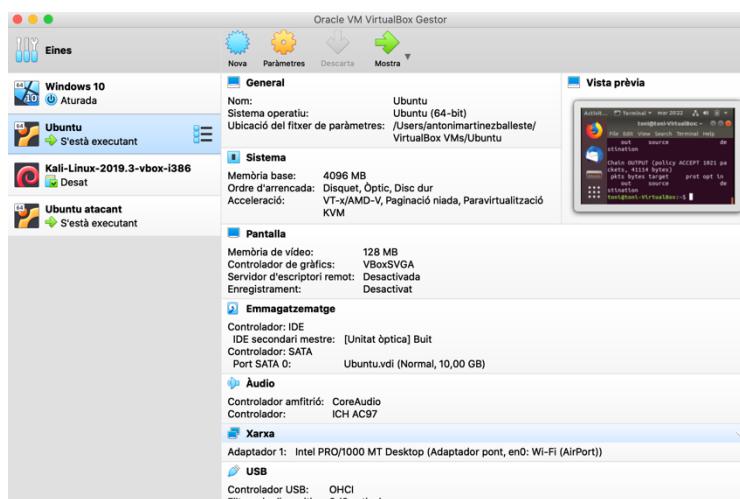
# **iptables stateful**

- **iptables -A OUTPUT -m state --state ESTABLISHED, RELATED -j ACCEPT**
  - Accepta que surtin paquets relacionats amb connexions ja establertes
  - [https://wiki.archlinux.org/index.php/Simple\\_stateful\\_firewall\\_\(Es pañol\)](https://wiki.archlinux.org/index.php/Simple_stateful_firewall_(Es pañol))

# iptables stateful

## Demo!

- **iptables en Ubuntu, executat en un VirtualBox.**
- Mode de xarxa “bridge”, així la Ubuntu està al mateix segment de xarxa que la màquina hoste (podem fer *ping* de la màquina hoste, que executa VirtualBox, cap a la Ubuntu).



Ubuntu

Ubuntu atacant



# Mecanismes per a la detecció d'atacs i intrusions

Joaquín García Alfaro

P07/05070/02626

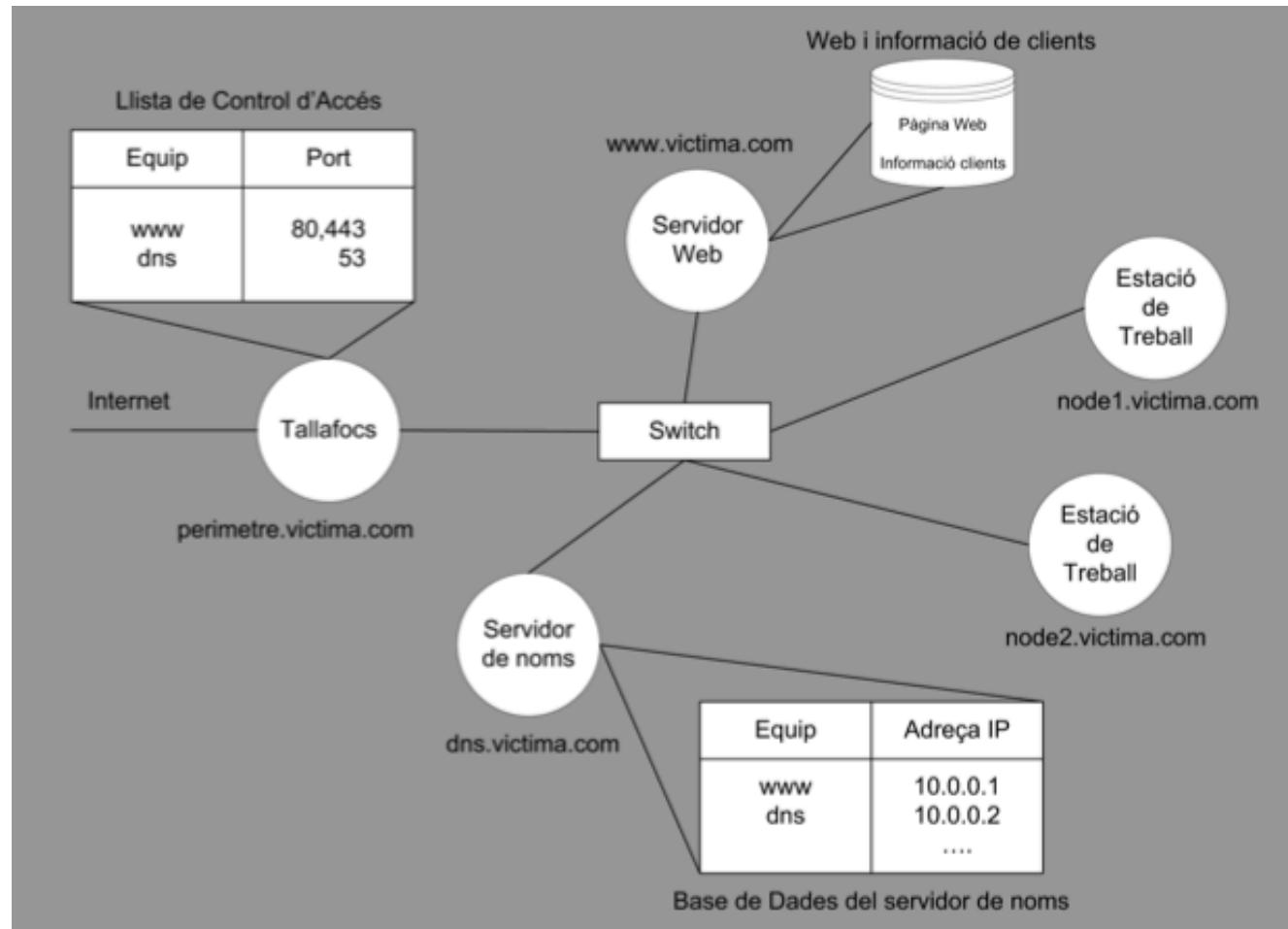


# IDS

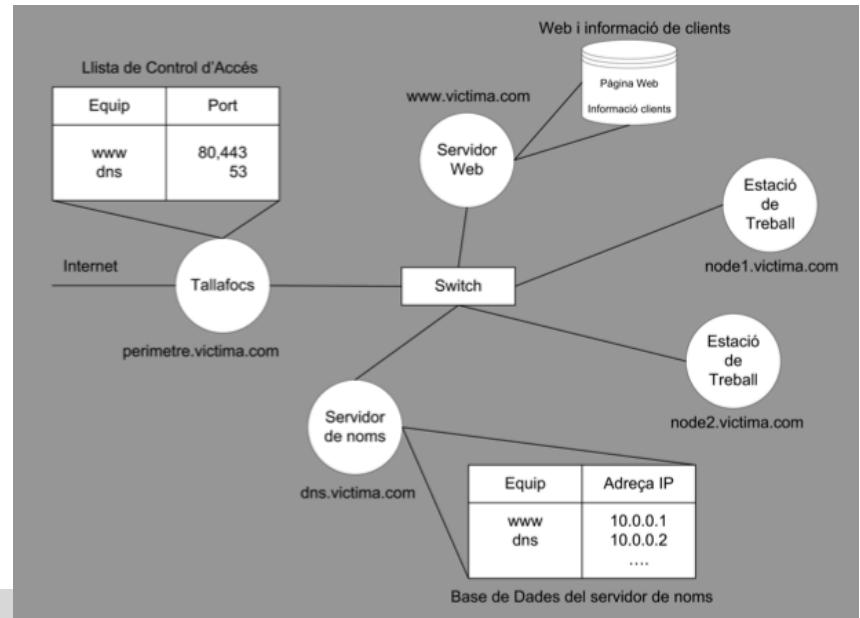
- **Sistemes de detecció d'intrusions (*intrusion detection system*, IDS)**
- Sistemes de prevenció d'intrusions (IPS)
  - Aquí hi juga un paper clau els **escàners de vulnerabilitats**, que analitzen els sistemes cercant potencials problemes que podrien donar lloc a fallades de seguretat, atacs a serveis i servidors, atacs a programari, etc.
  - Aquest concepte, l'estudiarem més endavant.

# IDS

## ■ Escenari



## ■ Escenari



La xarxa està protegida amb un sistema tallafoc, que permet únicament l'entrada de peticions HTTP, HTTPS i consultes de DNS, i també accepta la transmissió de les respques a les peticions HTTP, HTTPS i DNS.

El protocol HTTPS s'utilitza com a mecanisme de protecció de les dades dels clients a l'hora de realitzar transferències segures cap al servidor web, utilitzant tècniques criptogràfiques per protegir la informació sensible que l'usuari transmet cap al servidor web (número de targeta de crèdit, informació personal ...).

## ■ L'atac

La intrusió que l'atacant intentarà portar a terme passarà per les següents quatre fases:

- **Fase de vigilància** - Durant la fase de vigilància, l'atacant intentarà aprendre tot el que pugui sobre la xarxa que vol atacar. En especial, tractarà de descobrir serveis vulnerables i errors de configuració.
- **Fase d'explotació de servei** - Aquest segon pas descriu l'activitat que permetrà a l'atacant fer-se amb privilegis d'administrador (escalada de privilegis) abusant d'alguna de les deficiències trobades durant l'etapa anterior.
- **Fase d'ocultació d'empremtes** - Durant aquesta fase d'ocultació es realitzarà tota aquella activitat executada per l'atacant (una vegada ja produïda la intrusió) per passar desapercebut al sistema.

## ■ L'atac

Dins d'aquesta tercera etapa es preveuen activitats com per exemple l'eliminació d'entrades sospitoses en fitxers de registre, la instal·lació i modificació de comandes d'administració per ocultar l'entrada en els sistemes de la xarxa, o l'actualització dels serveis vulnerables que ha utilitzat per dur a terme la intrusió (a fi d'evitar que terceres parts s'introdueixin de nou en el sistema)...

- **Fase d'extracció d'informació** - En aquesta última fase, l'atacant amb privilegis d'administrador tindrà accés a les dades dels clients a través de la base de dades de clients.

L'intrús començarà el seu atac obtenint el rang d'adreses IP on es troba allotjat el servidor del web [www.victima.com](http://www.victima.com). Per a això, n'hi haurà prou de realitzar una sèrie de consultes cap al servidor de DNS de la companyia.

A continuació, realitzarà una exploració de ports cap a cadascuna de les adreces IP trobades en el pas anterior. L'objectiu d'aquesta exploració de ports és la cerca de serveis en execució en cada una de les màquines del sistema, mitjançant alguna de les tècniques vistes en els mòduls anteriors.

Gràcies als mecanismes de prevenció instal·lats a la xarxa del nostre exemple (el sistema tallafoc i les llistes de control mostrades a la figura), la major part de les connexions seran eliminades. D'aquesta forma, l'atacant tan sols descobrirà dues de les màquines de la xarxa (el servidor de DNS i el servidor web).

L'atacant decideix atacar el servidor web. Per a això, tractarà de descobrir quin tipus de servidor web està funcionant en aquest equip (li interessa el nom i la versió del servidor web en qüestió), ja que sap que és molt probable que existeixin deficiències de programació en aquest tipus d'aplicacions.

Per altra banda, l'atacant també intentarà descobrir el sistema operatiu i l'arquitectura hardware on el servidor web s'està executant. Aquesta informació serà important a l'hora de buscar els exploits que finalment utilitzarà per realitzar la intrusió.

Per obtenir tota aquesta informació, l'atacant en té prou amb les entrades de DNS que la pròpia companyia li està oferint (a través dels camps HINFO de les peticions).

D'aquesta forma, l'atacant descobreix que el servidor web està funcionant sota una arquitectura concreta i que en aquest servidor hi ha un determinat sistema operatiu instal·lat.

Amb la informació del sistema operatiu l'atacant ja pot suposar el servidor web que està en execució dins l'equip i pot fins i tot confirmar la suposició observant les capçaleres de les respostes HTTP que el servidor envia en cada petició d'HTTP o HTTPS.

L'atacant, que col·lecciona un ampli repòrtori d'aplicacions per abusar d'aquest producte, acabarà obtenint un accés amb privilegis d'administrador mitjançant, per exemple, la realització d'un desbordament de buffer existent en l'aplicació en qüestió.

La primera observació que podem indicar de tot el procés que acabem de descriure és que els mecanismes de prevenció de la xarxa permeten la realització d'aquest abús contra el servidor web ja que el desbordament de la pila d'execució s'ha fet mitjançant peticions HTTP legítimes (estan acceptades a les llistes de control del sistema tallafoc).

Així doncs, sense necessitat de violar cap de les polítiques de control d'accés de la xarxa, l'atacant pot acabar fent-se amb el control d'un dels recursos connectats a la xarxa de la companyia.

# IDS

Una vegada compromès el servidor web, l'intrús entrarà en la fase d'ocultació i començarà a eliminar ràpidament totes aquelles marques que puguin delatar la seva entrada al sistema. A més, s'encarregarà d'installar a l'equip atacat un conjunt d'eines conegeudes com a *rootkits*. Aquestes *rootkits* són una recopilació de binaris de sistema fraudulents, que s'encarreguen de deixar portes obertes al sistema atacat, per tal de garantir futures connexions amb la mateixa escalada de privilegis, així com a altres eines per a realitzar altres atacs al sistema o a la xarxa (aplicacions per a realitzar denegacions de servei, escoltes a la xarxa, extracció de contrasenyes de sistema, etc).

Una vegada finalitzada la fase d'ocultació d'empremtes, l'atacant disposa d'un equip dins de la xarxa que li podrà servir de trampolí per realitzar nous atacs o intrusions a la resta d'equips de la companyia. A més, operant des d'una màquina interna de la xarxa, l'atacant ja no està subjecte a les restriccions imposades pels sistemes de prevenció.

Finalment, un cop arribats a aquest punt, l'atacant disposarà sense cap problema de les dades que els clients tenen emmagatzemades a la base de dades.

Aquest exemple ens mostra com l'existència d'un sistema tallafoc (o d'altres mecanismes de prevenció) i la utilització de comunicacions xifrades (com a mecanisme de protecció de dades) no són suficients a l'hora de defensar els nostres sistemes de xarxa.

- Els mecanismes per a la detecció d'atacs i intrusions s'encarreguen de **trobar i reportar** tot tipus d'activitat maliciosa a la xarxa, inclús arribant a **reaccionar** davant de l'atac de la forma apropiada.

En la majoria dels casos és desitjable poder identificar l'atac exacte que s'està produint, de forma que sigui possible detenir l'atac i recuperar-se d'aquest. En altres situacions només serà possible detectar i informar de l'activitat sospitosa que s'ha trobat, davant la impossibilitat de conèixer realment el que ha succeït.

# IDS

Una **intrusió** és una seqüència d'accions realitzades per un adversari maliciós, amb l'objectiu final de provocar un accés no autoritzat sobre un equip o un sistema al complet.

- **Un IDS recollirà indicis d'activitats i detectarà si s'està produint una intrusió.**
  - Per tant, intervenen processos com ara la detecció de patrons, la predicción, l'aprenentatge automàtic, etc. tots relacionats amb la **intel·ligència artificial i/o el *process mining*** (mineria de procés).

# IDS

- **Requeriments d'un IDS** (i de l'aprenentatge automatitzat, també!)
- **Precisió.** No ha de confondre accions legítimes amb accions deshonestes... podríem provocar una denegació de servei contra un usuari o servei legítim!
- **Eficiència.** Cal minimitzar la taxa d'activitat maliciosa no detectada, és a dir, els falsos negatius.
- **Rendiment.** Cal intentar detectar en temps real :-)
- **Tolerància a fallades.** L'IDS ha de seguir funcionant (rèplica).

## ■ Parts d'un IDS

### ■ Sensors

HIDS,  
NIDS

- **Basats en equip**, que recullen informació d'esdeveniments succeïts a nivell de sistema operatiu (com per exemple, intents de connexió i crides al sistema). També poden recollir informació sobre les aplicacions que s'estan executant.
- **Basats en xarxa**, que recullen informació d'esdeveniments a nivell de trames enviades per la LAN.

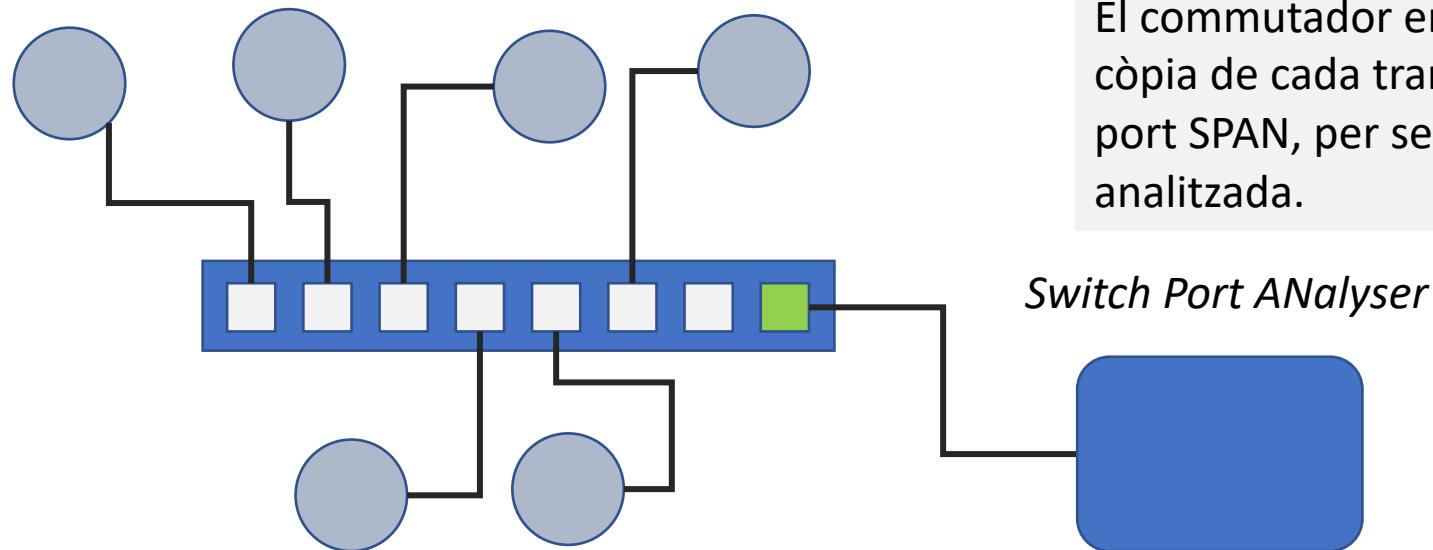
### ■ Processadors d'esdeveniments

- Els processadors d'esdeveniments, també coneguts com a **analitzadors**, conformen el nucli central del sistema de detecció. Tenen la responsabilitat d'operar sobre la informació recollida pels sensors per poder inferir possibles intrusions.

- Parts d'un IDS
  - Unitats de resposta
    - Basades en equip (tancar procés) o en xarxa (bloquejar IP)
  - Sistemes d'emmagatzematge
    - Mooooooltes dades generades!!
    - Podríem desar les dades durant dos o tres dies... però grans volums de dades poden servir per entrenar els analitzadors fent servir tècniques de deep learning.

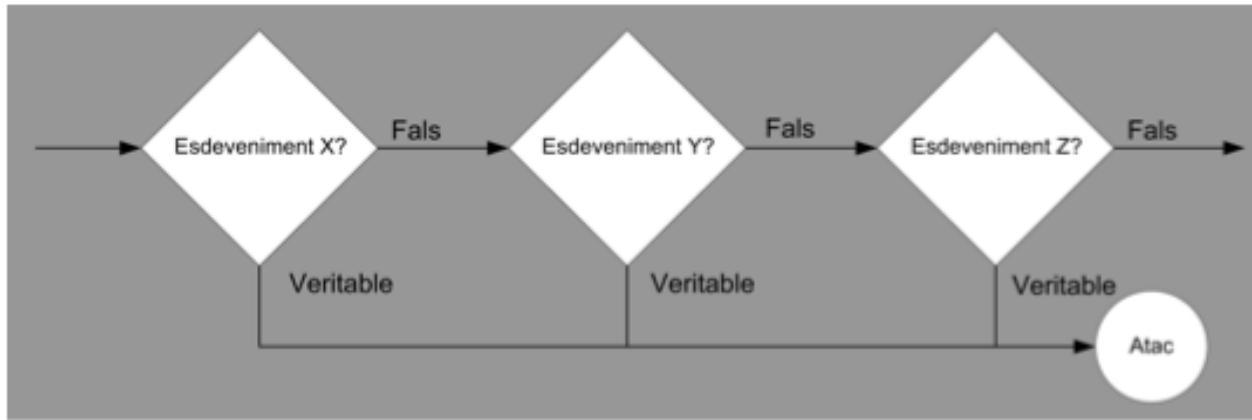
## ■ Ubicació dels sensors

- Juntament amb el tallafoc
- En un TAP/SPAN port a cada commutador



## ■ Processadors o analitzadors

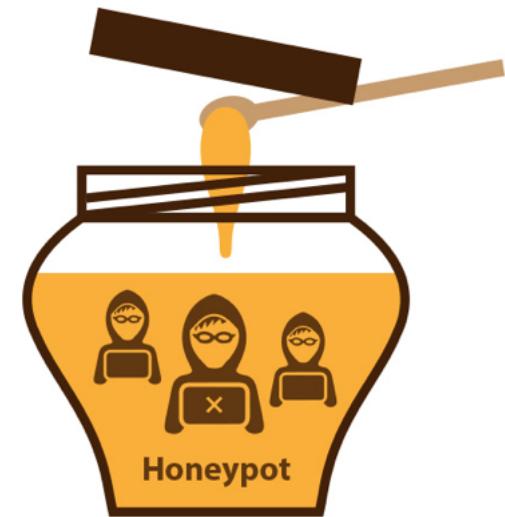
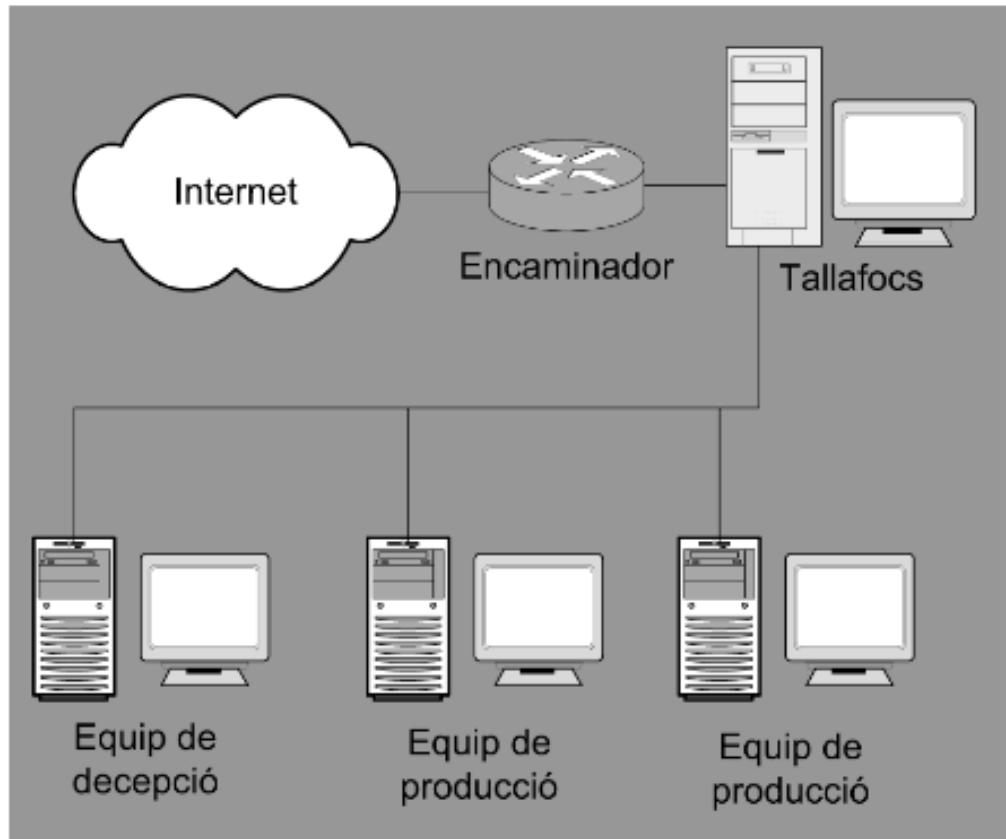
- Analitzadors basats en reconeixement de patrons.



- Podem afegir la relació temporal —> detecció de processos d'atac, transicions d'estats.

# Més enllà dels IDS

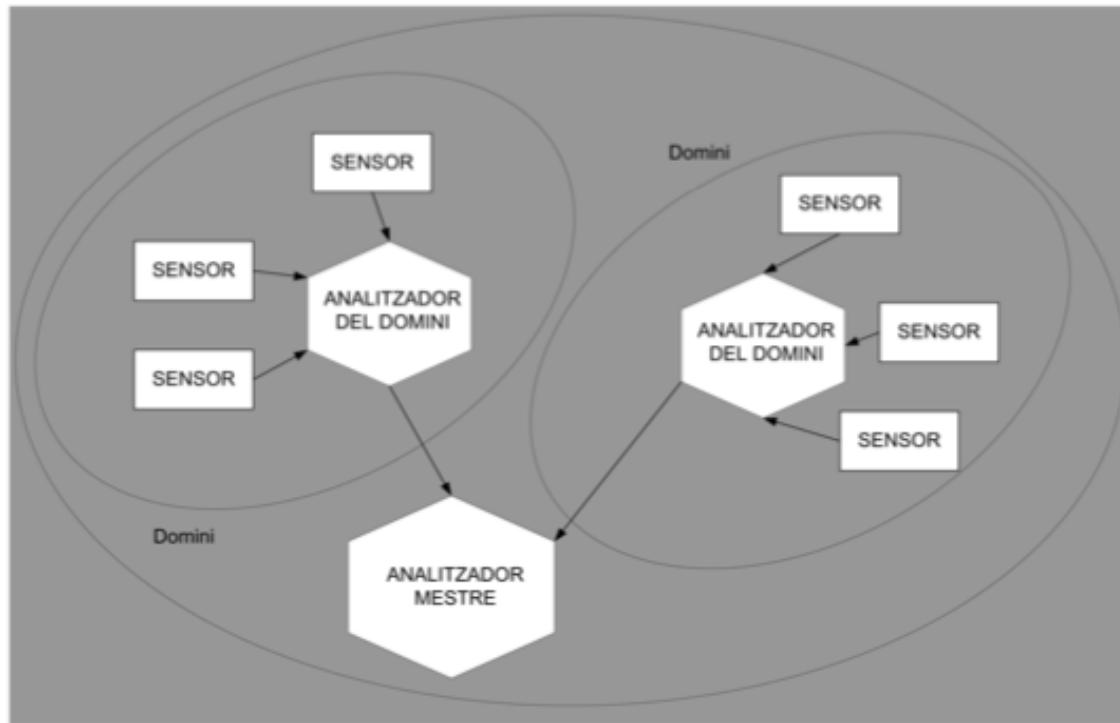
## ■ Equips / xarxes de decepció



<https://www.sofistic.com/productos/honeypot/>

# Més enllà dels IDS

- Detecció d'atacs distribuïts



# Snort

## ■ Què és Snort?

- Snort és un Sistema de detecció d'intrusos (IDS) basat en xarxa (IDSN). Disposa d'un llenguatge de creació de regles en què es poden definir els patrons que s'utilitzaran a hora de monitoritzar el sistema.
- Ofereix una sèrie de regles i filters ja predefinits que es poden ajustar llarg de la instal·lació i configuració.



# Snort

## ■ Regles...

```
alert icmp any any -> any any (itype:8;msg:"Contacte";)
```

```
log tcp any any -> any 80 (msg:"Acces";content:"successlogin.html";)
```

The screenshot shows the Snort rule editor interface with two tabs open:

- Alert Tab:** Displays the first rule:

```
[**] [1:1:0] Contacte []
[Priority: 0]
04/26-17:03:58.850619 192.168.1.39 -> 192.168.1.35
ICMP TTL:128 TOS:0x0 ID:23680 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:30 ECHO
```
- Log Tab:** Displays the second rule:

```
[**] [1:1:0] Contacte []
[Priority: 0]
04/26-17:03:59.853405 192.168.1.39 -> 192.168.1.35
ICMP TTL:128 TOS:0x0 ID:21
Type:8 Code:0 ID:1 Seq:30 ECHO
```

```
[**] "Acces" []
[Priority: 0]
04/26-17:04:47.816476 192.168.1.39:63867 -> 192.168.1.35:80
TCP TTL:128 TOS:0x0 ID:24152 IpLen:20 DgmLen:485 DF
***AP*** Seq: 0x8D710D66 Ack: 0xB4F61362 Win: 0x805 TcpLen: 20
=====
```