Presentació Projecte Final de Carrera

VULNERABILITATS EN XARXES WLAN

PROTOCOLS I MECANISMES DE PROTECCIÓ

J. Luis Blasco de Gracia

Gener 2016

Continguts

Introducció

Les xarxes sense fils WLAN s'han implantat fortament a nivell social i empresarial donada la seva versatilitat, baix cost i mobilitat que aporta als usuaris.

Aquest fet ha afavorit el desenvolupament de la tecnologia WiFi en xarxes domèstiques i WLAN empresarials, que recolzada en la família d'estàndards IEEE 802.11, regula i facilita la interconnexió i l'intercanvi d'informació entre dispositius sense fils.

Tanmateix, la transmissió d'informació a través de l'aire és un escenari potencialment vulnerable i atractiu per als atacants. Per tant, és necessari protegir les dades i evitar que la nostra informació quedi compromesa.

Afortunadament els estàndards IEEE 802.11i IEEE 802.11x implementen mecanismes de seguretat per protegir la informació. Aquests mecanismes es basen en el xifratge i l'autenticació.

Tot i així, hem de ser proactius a l'hora d'utilitzar xarxes WiFi i ser conscients de les vulnerabilitats a les que ens enfrontem. Això ens permetrà aplicar els mecanismes adients per minimitzar qualsevol atac amb èxit.

Objectius

Oferir una visió global de les **xarxes WLAN** i presentar els estàndards de seguretat dissenyats per a tecnologies WiFi.

Conèixer els principals **riscos i amenaces** presents en xarxes WiFi.

Recomanar **mesures preventives i mecanismes de protecció** alhora de configurar els nostres dispositius.

Demostrar la importància de la **conscienciació i prevenció** alhora d'aconseguir una xarxa segura i la navegació a través d'ella.

Presentar els **sistemes de detecció i prevenció d'intrusions** com eines que vigilen els moviments de la xarxa i que ajuden a mantenir un alt nivell de seguretat.

Xarxes sense fils WLAN

WLAN (*Wireless Local Area Network*)

Significa Xarxa d'àrea local sense fils. Sistema de comunicació que permet la transmissió de dades entre dispositius mòbils utilitzant ones de radiofreqüència.

Regulació IEEE: 802.11

Família d'estàndards IEEE 802.11 desenvolupats per donar suport al constant desenvolupament de les comunicacions WLAN.

Tecnologia: WiFi

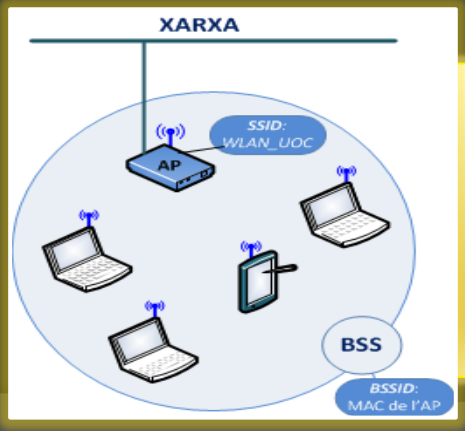
L'empresa *Wi-Fi Alliance* desenvolupa la tecnologia coneguda popularment per la marca ***WiFi.***

Compatibilitza les comunicacions Ethernet sense fils i una homogeneïtzació dels productes.

Xarxes sense fils WLAN (elements)

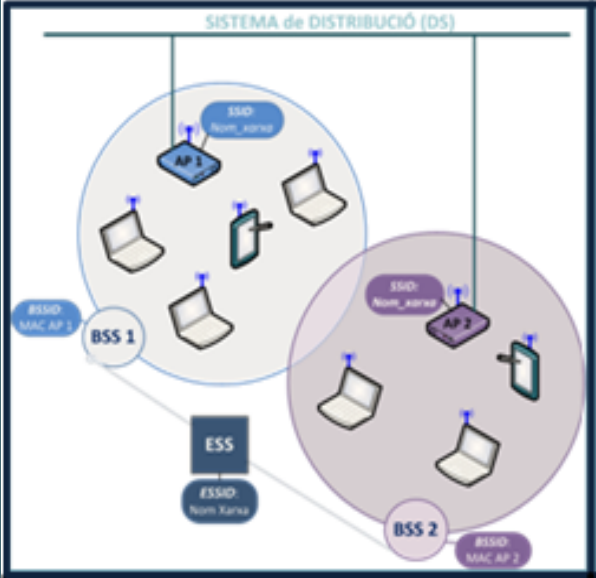
-Hosts sense fils: dispositius connectats a una xarxa no cablejada i proveeixen o utilitzen serveis d'ella; ordinador portàtil, tauleta, *smartphone* etc.

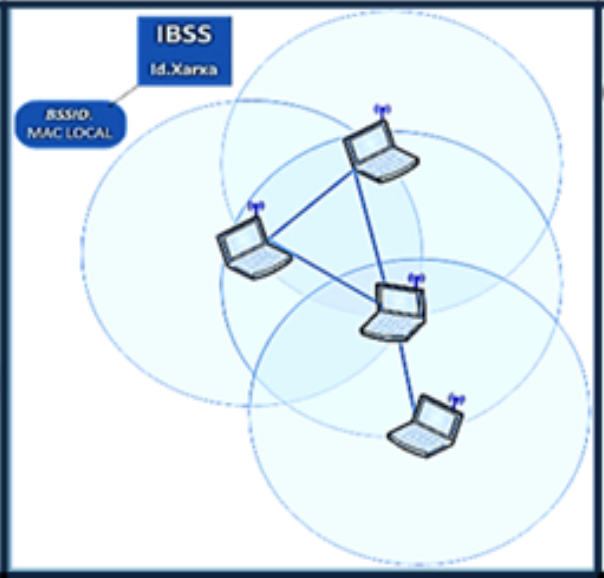
-Estacions base o AP (*Acces Point*): dispositiu que envia i rep dades d'un host que utilitza tecnologia sense fils. Tenen un abast d'uns 150 metres.

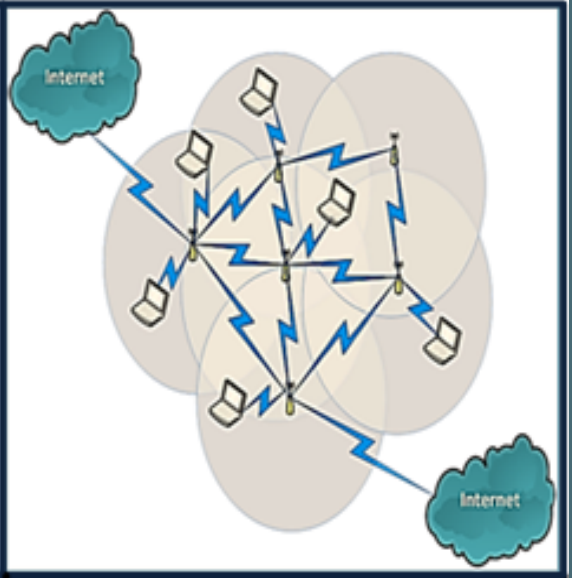


-BSS (*Basic Service Set*) : Bloc o cel·la de comunicació bàsica formada pels AP's i hosts associats. Una xarxa WiFi pot estar formada per diferents BSS, els quals, formen un conjunt de serveis estesos (ESS).

Xarxes sense fils WLAN (topologies)







Infraestructura:

Cada host es connecta a un punt d'accés a través d'un enllaç sense fils. Cada BSS s'identifica amb el seu BSSID (Basic Service Set Identifier) que correspon a la MAC del AP associat.

Ad-Hoc

Els hosts no es connecten a cap xarxa a través d'un AP, sinó que es connecten entre sí formant una xarxa punt a punt on cada equip actua com a client i punt d'accés a la vegada.

Mesh

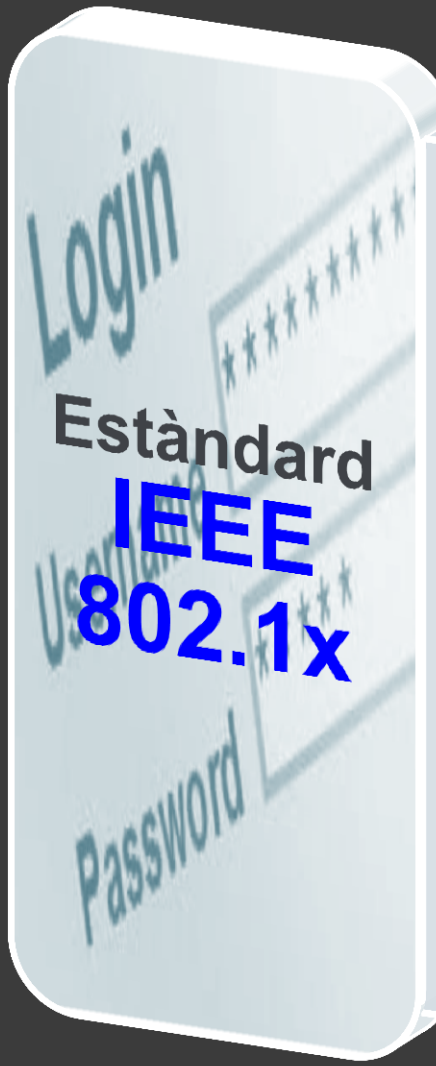
Confluència de les topologies Infraestructura i Ad-hoc.

Existeix almenys dos camins en cada node.Són molt tolerants a fallades

Estàndards de seguretat WLAN (802.11i)

- Soluciona els problemes de seguretat que implementava la norma original 802.11. Preveu diversos mecanismes que ajuden a incrementar la seguretat durant el procés de connexió i intercanvi de dades a través de la xarxa.
- Xifrat simètric de 128 bits i vector d'inicialització de 48 bits de longitud.
- Inclou un esquema de xifrat basat en AES (*Advanced Encryption Estandard*), el qual, és un dels algoritmes més segurs i més utilitzats avui en dia, amb una longitud de la clau que pot anar des de 128 bits fins a 256 bits.
- Proporciona autenticació. Aquest procés es porta a terme gràcies al component d'autenticació 802.1x que ja s'havia provat en xarxes cablejades.

Estàndards de seguretat WLAN (802.1x)

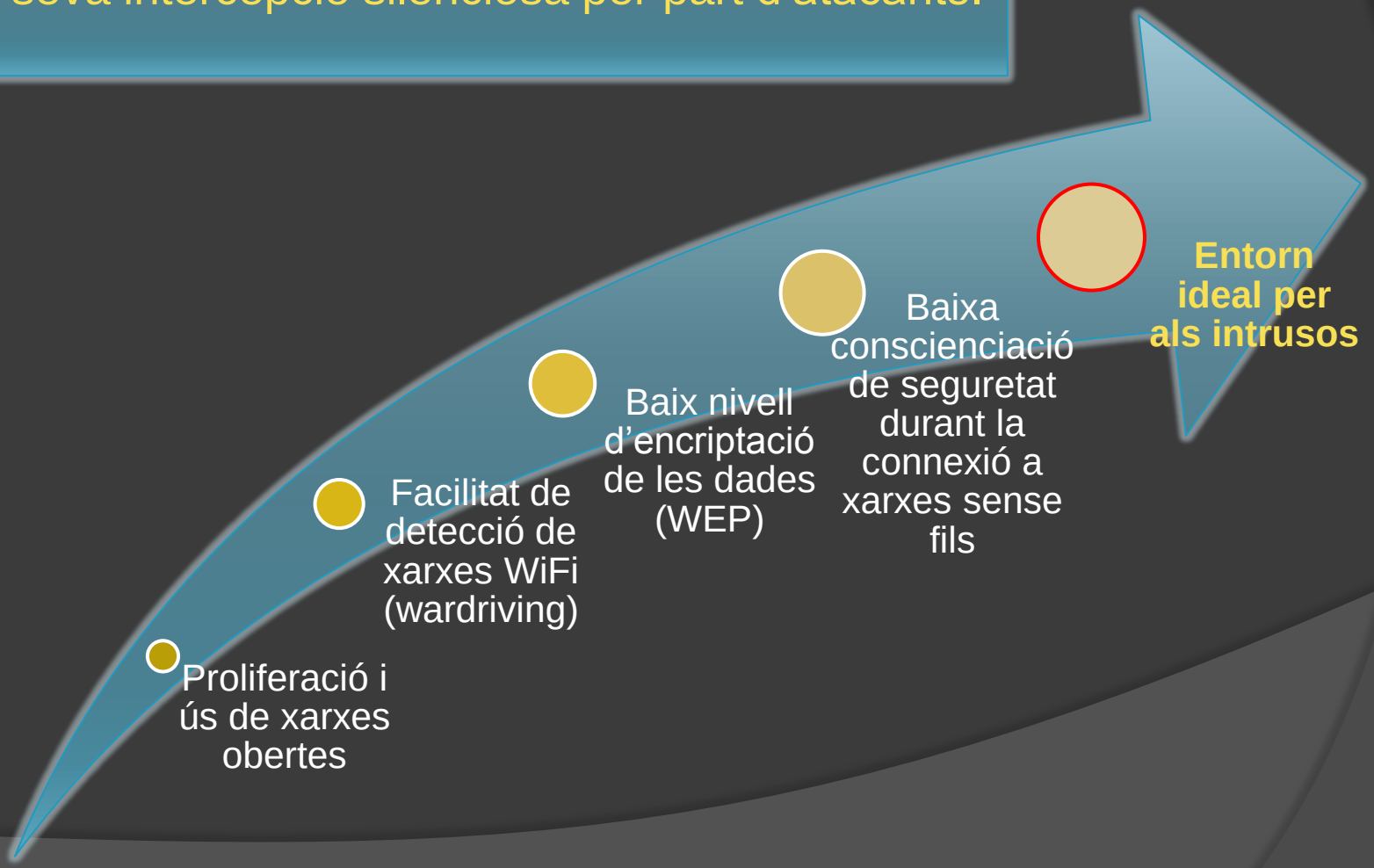


Estàndard IEEE 802.1x

- Eix vertebrador de la seguretat WiFi que complementat amb l'estàndard 802.11i s'aconsegueix un nivell de seguretat robust.
- El punt d'accés ja no autoritza la connexió a la xarxa. L'autenticació d'usuaris es realitza mitjançant servidors d'autenticació RADIUS o DIAMETER.
- Els missatges s'envien encapsulats mitjançant diferents versions del protocol EAP.
- El port de comunicació no s'obrirà per a permetre la connexió mentre que l'usuari no estigui autoritzat.

Amenaces en xarxes WiFi (I)

La transmissió de dades a través de l'aire facilita la seva intercepció silenciosa per part d'atacants.



Amenaces en xarxes WiFi (II)

Detecció i accés a la xarxa il·lícitament degut a:

- Fàcil detecció de xarxes inclús amb ESSID ocult.
- Trencament de llistes ACL on l'intrús s'assigna una MAC vàlida a través d'un *sniffer*.
- Descobriment de contrasenyes poc segures, curtes o predicibles.

Manipulació o escolta il·lícita d'informació degut a:

- Utilització de xarxes obertes o amb seguretat basada en el dèbil mecanisme WEP.
- Modificació de taules ARP d'un client legítim interceptant les seves comunicacions entre altres hosts.
- Comunicacions interceptades a través de connexions VPN en xarxes obertes o a través de portals captius, els quals associen client-AP sense xifrar.

Mecanismes de seguretat (I)

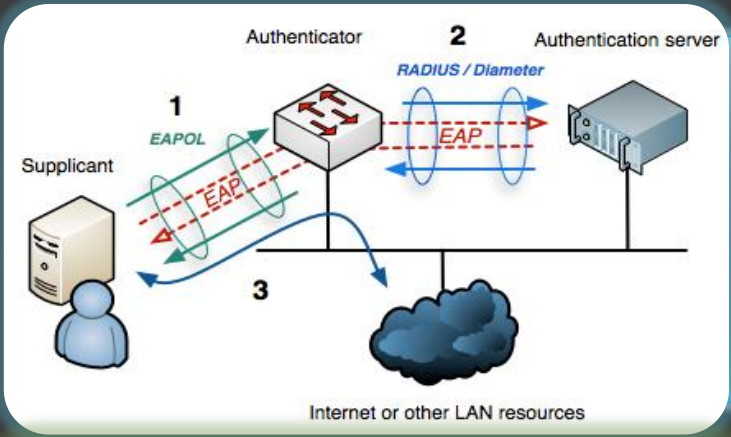
WEP

- *Utilitza l'algoritme RC4 de 128 bits per al xifrat de la clau secreta compartida per tots els integrants, la qual es fa servir per xifrar les dades enviades.*
- *És poc segur i fàcilment vulnerable.*

WPA / WPA2 / WPA-PSK

- **WPA:** evolució directa del mecanisme WEP amb mètode de xifrat més robust.
- **WPA2:** basat en l'estàndard 802.11i que utilitza l'algoritme AES molt resistent a possibles atacs.
- **WPA-PSK:** genera una clau pre-compartida de entre 8 i 63 caràcters des de l'inici de la comunicació i amb la que utilitzarà per generar aleatòriament noves claus. És una de les opcions de xifrat més robusta.

Mecanismes de seguretat (II)



Autenticació 802.1x

- Permet l'accés a la xarxa controlant els ports i encapsulant els protocols d'autenticació extensible EAP.
- Els protocols EAP es basen en el mètode de infraestructura pública (PKI), que permeten l'intercanvi d'autenticació entre host client i servidor d'autenticació mitjançant certificats digitals.

Xarxes Privades Virtuals (VPN)

- Tecnologia de xarxa utilitzada per connectar un o més dispositius a una xarxa privada utilitzant Internet i dades xifrades mitjançant protocols com *Ipsec*.

Portals Captius

- Sistema que valida als usuaris i els obliga a passar per una pàgina web si vol navegar per Internet i durant un temps limitat.
- Utilitza un programa o dispositiu informàtic integrat en una xarxa per vigilar el tràfic *http*.

Comunicacions WiFi més segures

Configuració de punts d'accés / encaminadors

- Modificar credencials per defecte d'accés al portal de l'encaminador.
- Activar l'accés al portal de configuració amb credencials.
- Configurar el tipus de xifrat WPA2 amb encriptació AES.
- Configurar els ports disponibles per a l'accés extern a la xarxa.
- Habilitar l'accés a l'encaminador a través de connexions *https*.
- Modificar l'SSID de la xarxa per un d'alfanumèric sense cap relació amb l'usuari o entitat.
- Ocultar l'SSID de la xarxa.
- Desactivar l'opció WPS per dificultar possibles atacs.
- En encaminadors empresarials habilitar ,si és possible, el filtrat MAC de clients i autenticació RADIUS.

Navegació

- Accedir solament a xarxes sense fils protegides amb contrasenya.
- Evitar connexions basades en WEP. Preferiblement WPA o WPA2.
- Configurar el tipus de connexió en el nostre dispositiu com "Xarxa Pública".
- Navegar de forma segura a través de pàgines *https*.
- Evitar accedir a llocs web mitjançant enllaços de procedència desconeguda

Prevenció i detecció d'Intrusions (I)

La prevenció és, en sí mateixa, una actitud segura i per tant, un pilar important a l'hora de lluitar contra atacs maliciosos.

Els atacs, es produiran silenciosament i aprofitant fissures o deficiències de seguretat, les quals s'han de localitzar i solucionar.

Amb els escàner de vulnerabilitats, podrem realitzar una auditoria sobre tots els dispositius integrats en la xarxa, detectar possibles vulnerabilitats i eliminar-les.

Prevenció i detecció d'Intrusions (II)

Escàners de vulnerabilitats

QUÈ ES UN ESCÀNER DE VULNERABILITAT?

És una aplicació que analitza la nostra configuració de xarxa i executa un conjunt de tècniques d'atac, per detectar possibles deficiències de seguretat potencialment utilitzables per atacants.

QUÈ ENS PROPORCIONA UN ESCÀNER DE VULNERABILITAT?

- Actúa com un consultor de seguretat virtual, realitzant un anàlisi exhaustiu de tots els equips de la xarxa i generant un informe de riscos. Ofereix suport immediat per solucionar les vulnerabilitats detectades.
- Administra usuaris i dispositius per grups d'equips o dominis, ja sigui de manera remota o mitjançant agents virtuals, als quals es els especifica un conjunt d'equips amb un perfil d'anàlisi.

QUINES CATEGORIES D'ESCÀNERS HI HAN I QUINES SON LES SEVES DIFERÈNCIES?

Bàsicament dos: Escàners basats en **màquina** i Escàners basats en **xarxa**

Basat en Màquina:
El seu objectiu és detectar vulnerabilitats en comptes d'usuari obertes, permisos de manipulació d'arxius, entrades d'usuari inusuals o sospitoses etc.

Basat en Xarxa:
Realitza proves d'atac reals a les connexions de la xarxa objectiu i registra les vulnerabilitats detectades, com ports oberts o indicis de de possibles atacs.

Prevenció i detecció d'Intrusions (III)

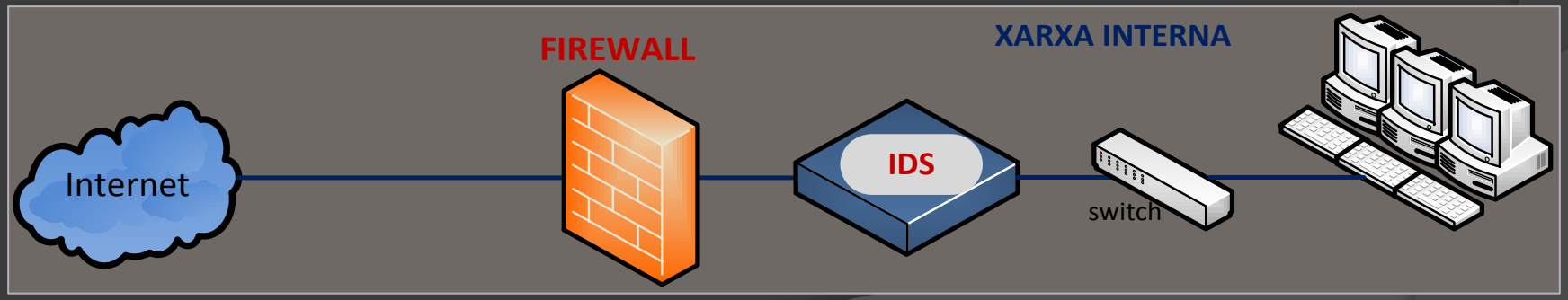
Sistemes de Prevenció i detecció d'Intrusions

IPS (Sistema de Prevenció d'Intrusions)

Programari dissenyat per analitzar, monitoritzar i bloquejar qualsevol intent d'atac abans de que pugui causar danys a la xarxa. Conegut pel nom de tallafoc (*Firewall*).

IDS (Sistema de Detecció d'Intrusions)

Eina que mitjançant sensors distribuïts estratègicament, identifica i dona resposta a activitats malicioses o moviments sospitosos en equips de la nostra xarxa.

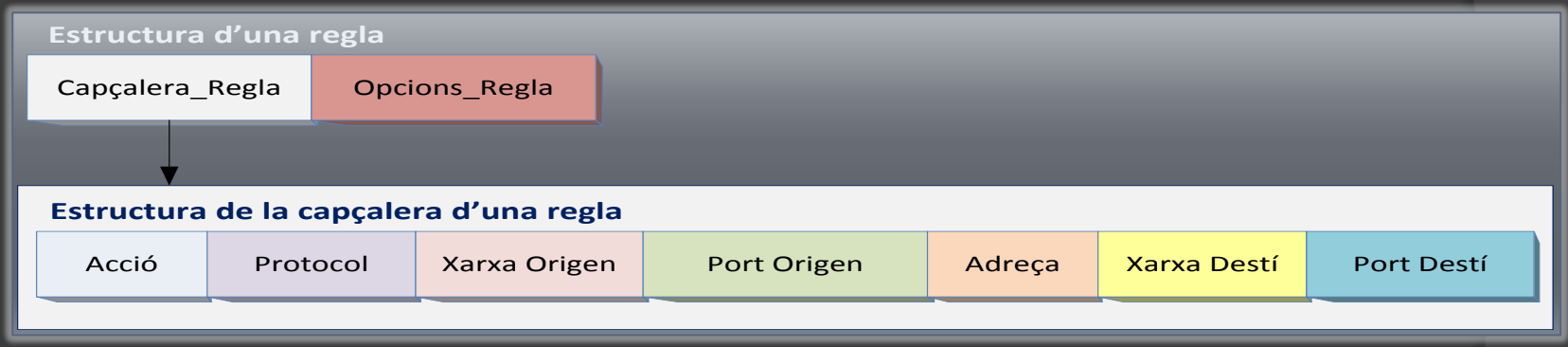


Esquema simplificat d'ubicació d'un IPS (Firewall) i un IDS

Prevenció i detecció d'Intrusions (IV)

L'IDS SNORT

Snort és un dels principals IDS de lliure distribució que utilitza tècniques de detecció de firmes i anomalies. Pot funcionar com un *sniffer* de paquets o com un NIDS (sistema de detecció d'intrusos de la xarxa). Inclou fitxers amb extensió *.rules* on s'inclouen les regles amb les que *Snort* utilitza per detectar moviments sospitosos en la xarxa. A continuació veurem un exemple.



Regla configurada per detectar "*pings*" sospitosos a la xarxa:

```
alert icmp any any -> any any (itype:8;sid:1;msg:"DETECCIÓ PING D'EXPLORACIÓ A LA XARXA";)
```

Alerta generada pel *IDS Snort* després de la detecció:

```
Not Using PCAP_FRAMES
12/01-23:40:08.182335  [**] [1:1:0] DETECCIO PING D'EXPLORACIO A LA XARXA [**] [
Priority: 0] {ICMP} 192.168.1.39 -> 192.168.1.44
12/01-23:40:09.264720  [**] [1:1:0] DETECCIO PING D'EXPLORACIO A LA XARXA [**] [
Priority: 0] {ICMP} 192.168.1.39 -> 192.168.1.44
```

Conclusions

Desenvolupament de *smartphones*, tauletes i computadores portàtils:

GRAN ACCEPTACIÓ I DIFUSIÓ DE XARXES WI-FI

Dispositius orientats a la comunicació + configuracions per defecte poc segures + hàbits de l'usuari insegurs:

DADES VULNERABLES

Necessitat de protegir les dades amb robusts algoritmes mitjançant els estàndards **802.11i** i **802.1x** . Aconseguim:

AUTENTICACIÓ, CONFIDENCIALITAT I INTEGRITAT

Auditoria i correcció de vulnerabilitats + IDS / IPS actualitzats

INCREMENT DE SEGURETAT PERMANENT

Conscienciació de l'usuari + Prevenció + Detecció

REDUCCIÓ D' ATACS AMB ÈXIT

Moltes Gràcies