Detección de anomalías en los registros de tráfico ofrecidos por IPFIX

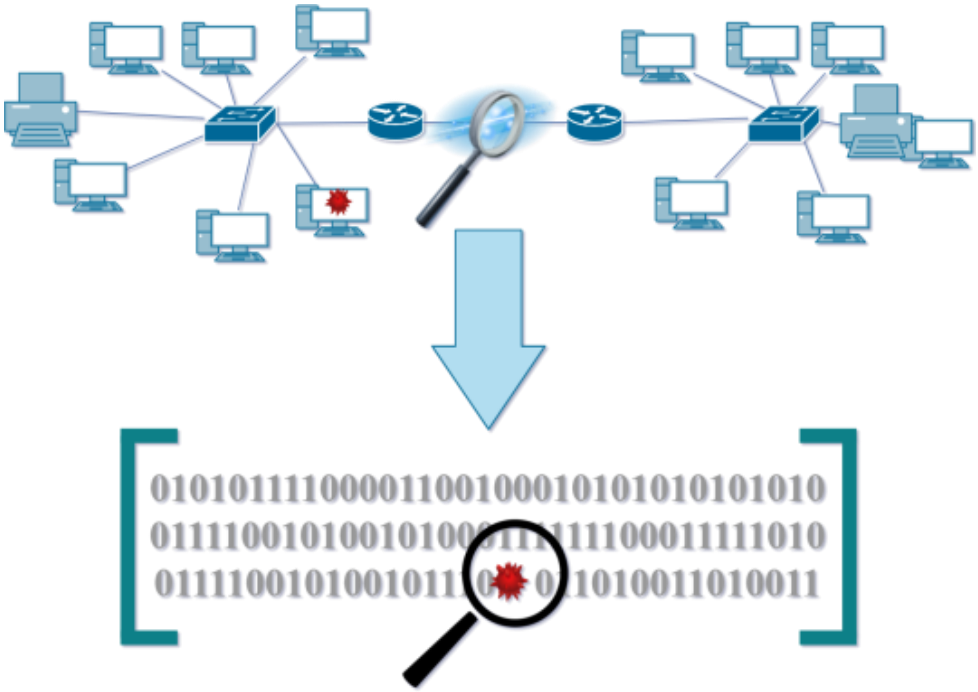
Agustín Walabonso Lara Romero

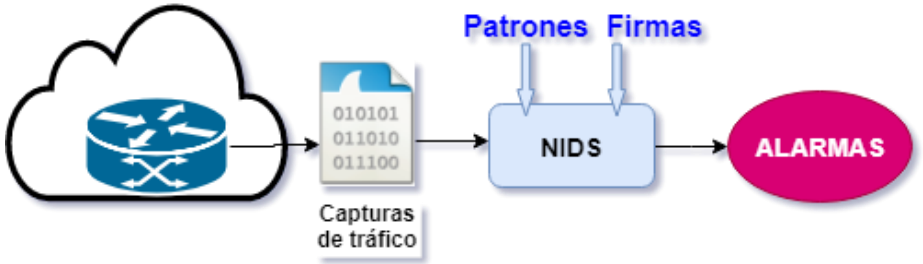
Universidad de Sevilla

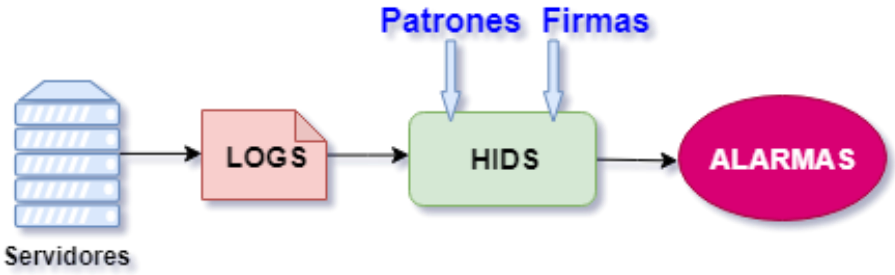
2019

Introducción

- Ataques:
  - Viajan por la red
  - Huellas logs







Detección: IDS

Protección: IPS/FW

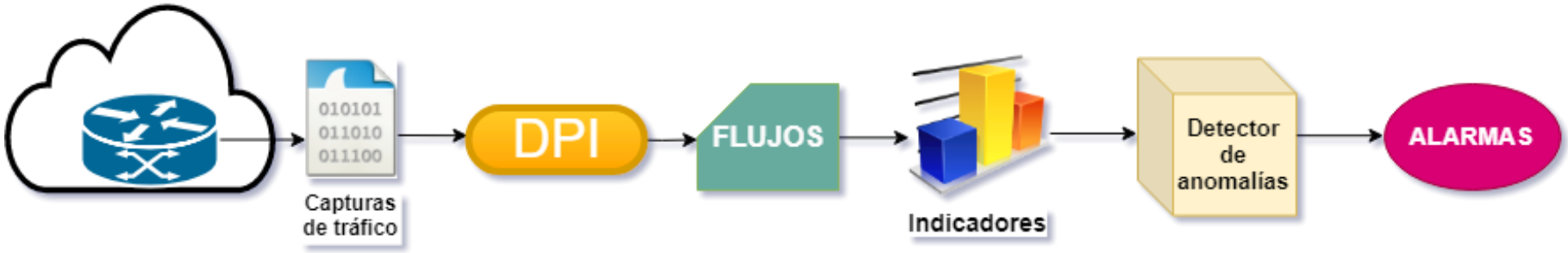
Motivación y Objetivos

- **Limitaciones:**
  - Necesidad del tráfico (PCAP) → **Baja escalabilidad**
    - Inspección de paquetes (FW, DPI): ¿Y si va cifrado?
      - Necesidad de gran capacidad HW de procesamiento
      - Gran cantidad de firmas para comparar
    - Transporte del tráfico en red (¿Port mirroring?)
    - Grado de protección: ¿Ataques sin firmas?

- **Objetivo**: Sistema IDS basado en anomalías
  - Uso de flujos
    - Diseño del sistema, implementación de un piloto y evaluación de indicadores

Arquitectura propuesta

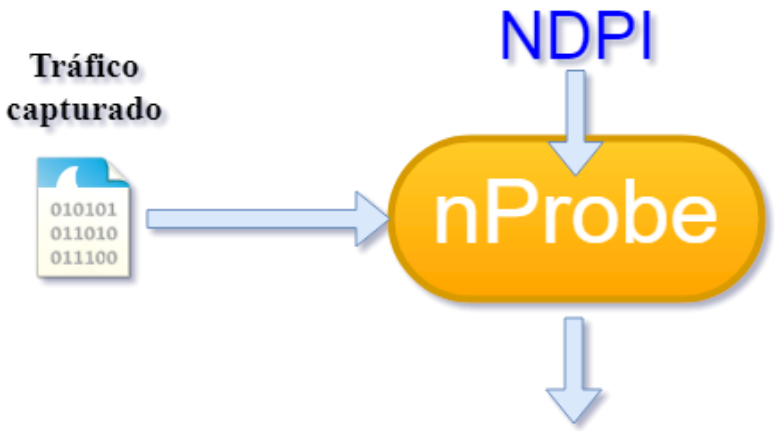
- **Arquitectura híbrida flexible**
  - Adaptable a diversos escenarios (configurable)

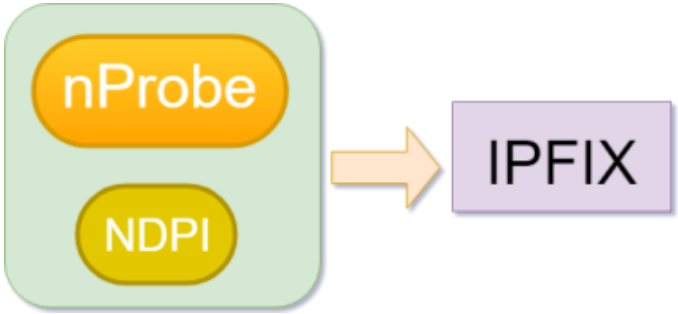


  - Flujos:
    - Generados localmente o por routers/switch intermedios
      - » **Opcional:** enriquecidos con **DPI**

Diseño del sistema

- Generación de **flujos** local: **nProbe**
  - Incluye **nDPI**
    - Indicadores de aplicaciones

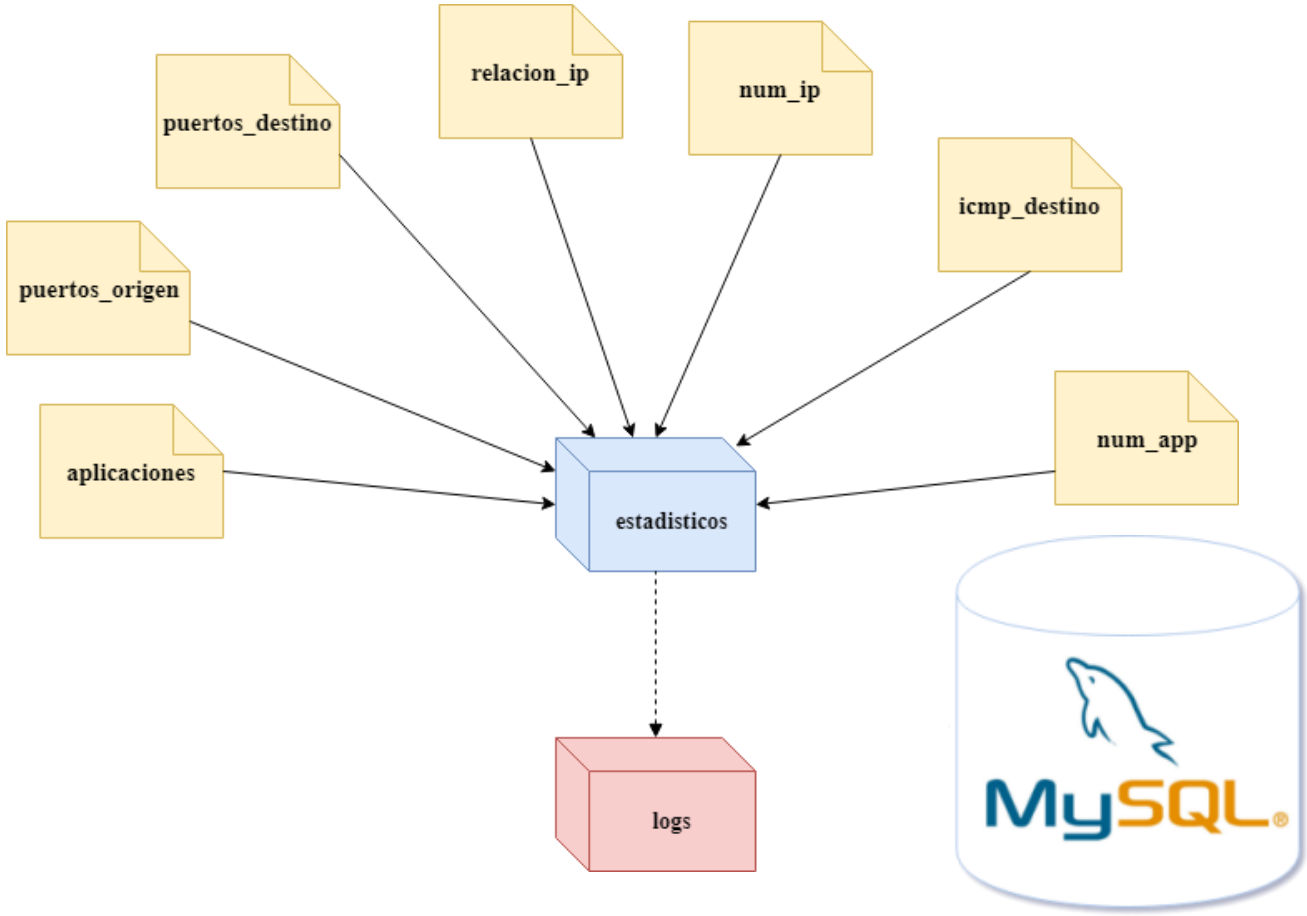




IP_SRC	PORT_SRC	IP_DST	PORT_DST	APP	PKTS	BYTES	T_INI	T_END
IP1	20	30	IP2	APP1	32	142	12	27
...								
IP4	50	60	IP6	APP5	36	125	45	56

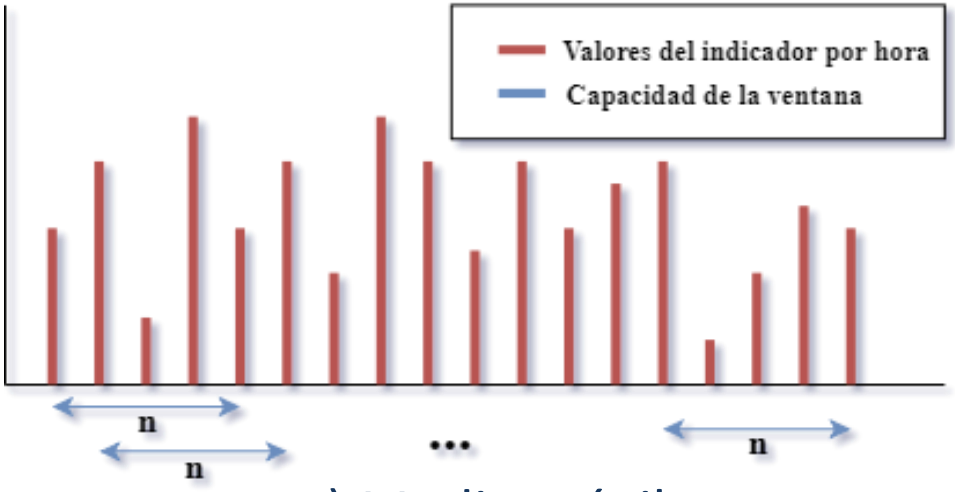
Diseño del sistema (II)

- Generación de **indicadores:** en franja horaria
  - 8 indicadores por cada IP a analizar



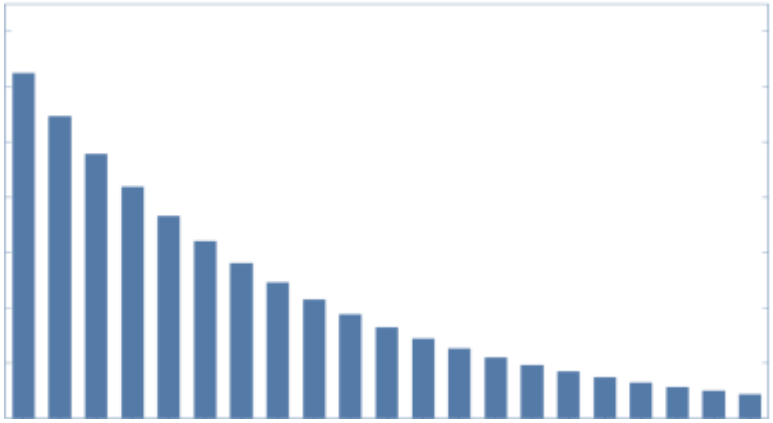
Diseño del sistema (III)

- Detector de anomalías
  - Basado en comportamientos estadísticos
  - Doble detector: $|x_i - \mu| > \mu \pm k \times \sqrt{\sigma^2}$



a) Media móvil

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

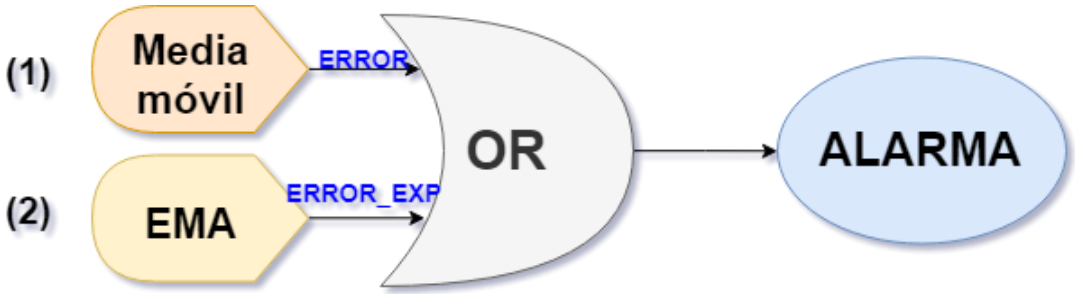


b) Media móvil exponencial (EMA)

$$EMA(t) = \begin{cases} x_1, & t = 1 \\ \alpha \times x_i + (1-\alpha) \times EMA(t-1), & t > 1 \end{cases}$$

Implementación y evaluación

- Diseñada fuera de línea (piloto de pruebas)
  - Generación de indicadores
  - Detección de anomalías
  - Generación de alarmas

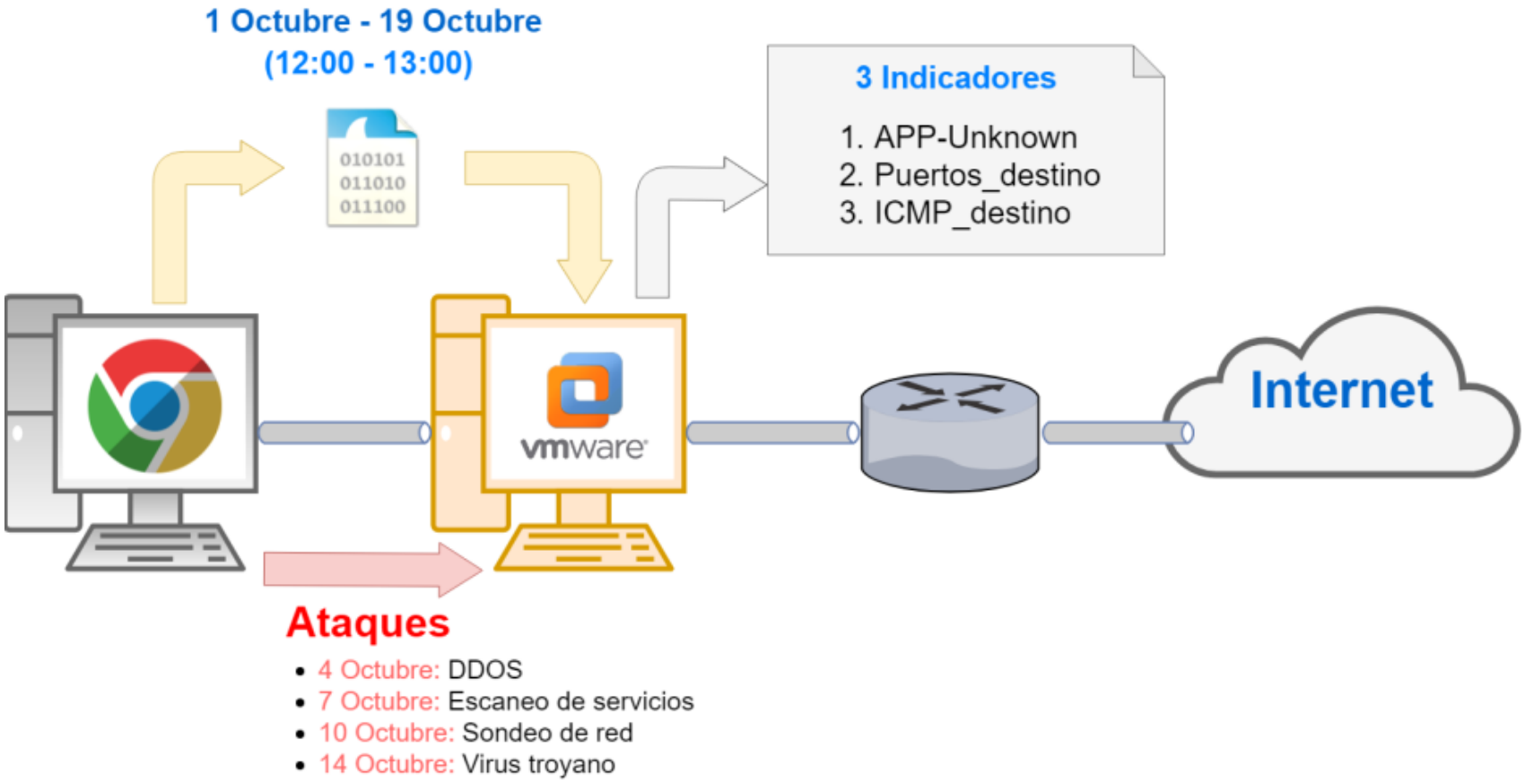


- Evaluación sistema
  - Escenario de validación
    - Tráfico normal y tráfico de ataques
  - Métricas de rendimiento
    - Capacidad de detección, falsos positivos
    - *Accuracy*

$$Accuracy(\%) = \frac{\sum_i Acierto_i}{Nº\ Total\ de\ muestras}$$

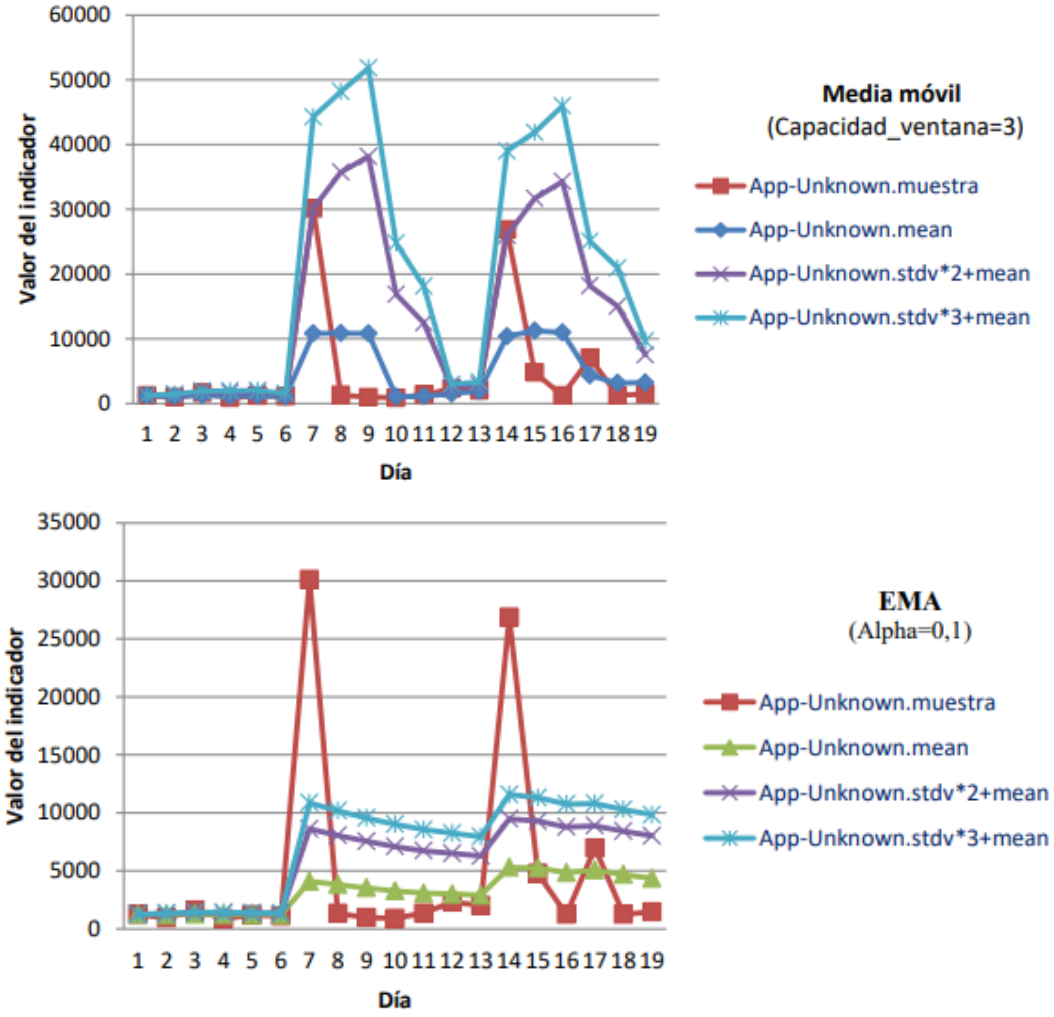
Escenario de pruebas

- Escenario final y pruebas realizadas



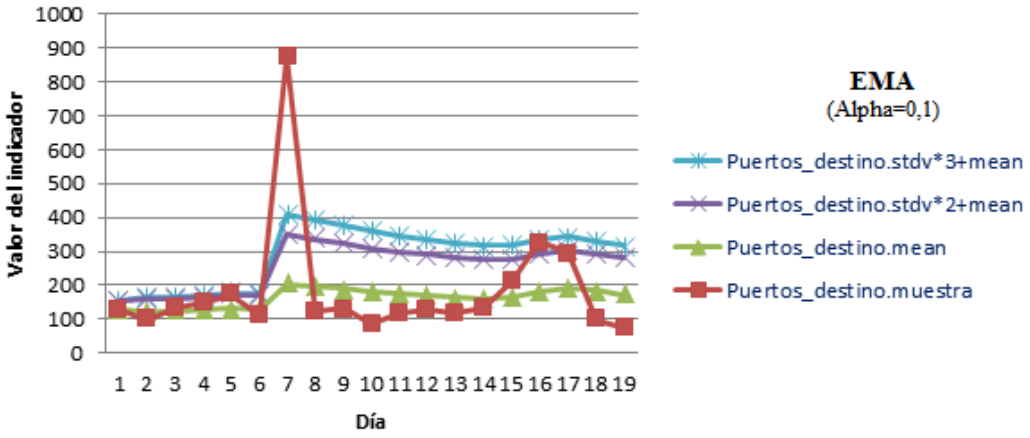
Resultados

- Evolución temporal indicadores: **App-Unknown**

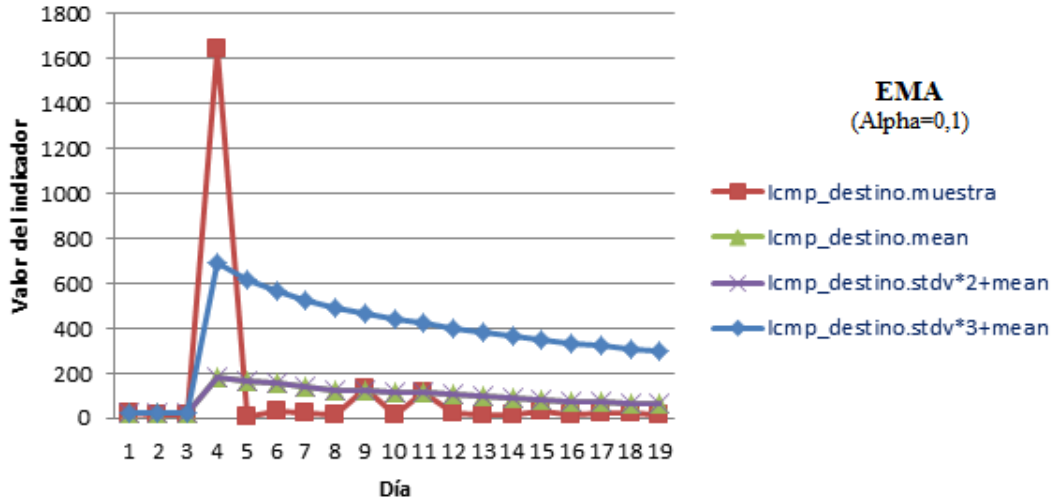


Resultados (II)

- Dst-Port



- Icmp-Port



Resultados (III)

Día	Tráfico	App-Unknown	Puertos_destino	Icmp_destino
1	Bueno			
2	Bueno			
3	Bueno	Alerta		
4	Malo			Alerta
5	Bueno			
6	Bueno			
7	Malo	Alerta	Alerta	
8	Bueno			
9	Bueno			
10	Malo	-	-	-

Día	Tráfico	App-Unknown	Puertos_destino	Icmp_destino
11	Bueno			
12	Bueno			
13	Bueno			
14	Malo	Alerta		
15	Bueno			
16	Bueno		Alerta	Alerta
17	Bueno			
18	Bueno			
19	Bueno			

Indicador	Unknown	Puertos_destino	Icmp_destino
CD(Tasa detección)	50	25	25
TFP(Tasa falsos positivos)	7,14	7,14	7,14
Accuracy (3)	84,21	78,95	78,95

Conclusiones

- **Sistema de detección flexible y escalable**
  - Indicadores según el escenario
  - Posibilidad DPI
  - Rendimiento aceptable (Primer paso)

Líneas de avance

- Implementación en línea
- Definición de nuevos indicadores
- Evaluación de nuevos escenarios de ataque
- Mejora en el sistema de detección

¡Gracias!