Detección de anomalías en los registros de tráfico ofrecidos por IPFIX

Agustín Walabonso Lara Romero

Universidad de Sevilla

2019

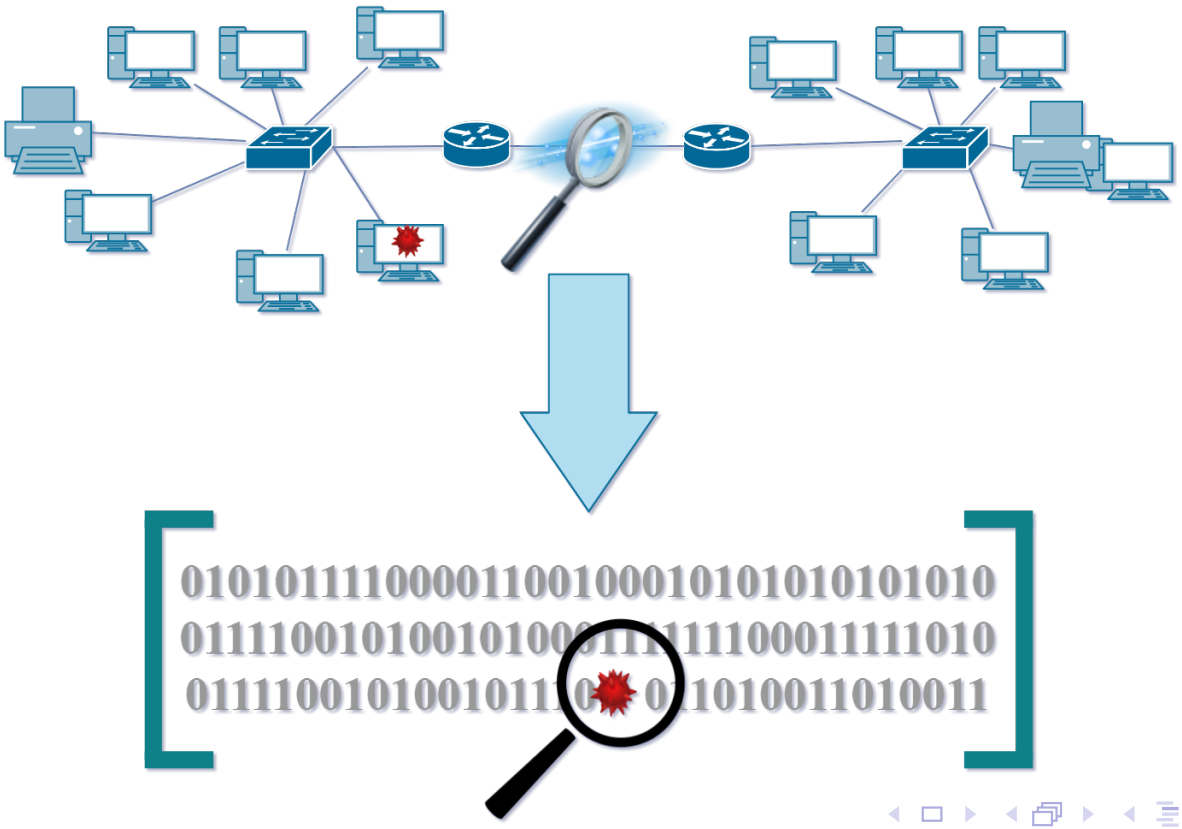
Índice

Introducción

Definición del problema

Patrones de comportamiento

Detecciones de anomalías



Introducción

Motivación y objetivos

Gran volumen de información

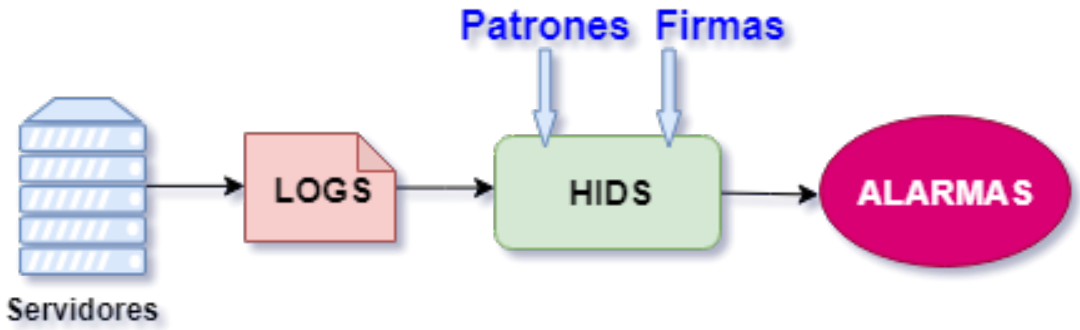
Sistema de detección

Escalabilidad

Marco teórico

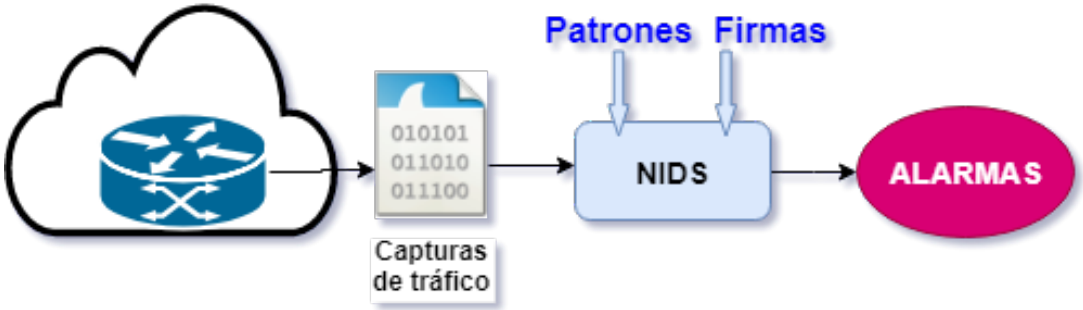
Arquitecturas comunes en ciberseguridad

Basadas en sistemas HIDS



No protege a los usuarios

Basadas en sistemas NIDS

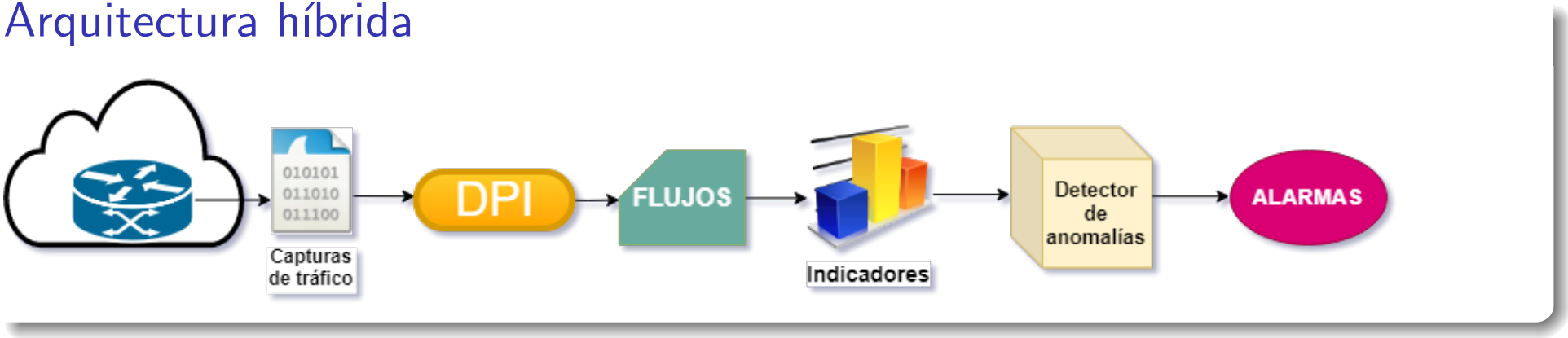


Sobrecarga al sistema de detección

Marco teórico

Solución de arquitectura propuesta

Arquitectura híbrida

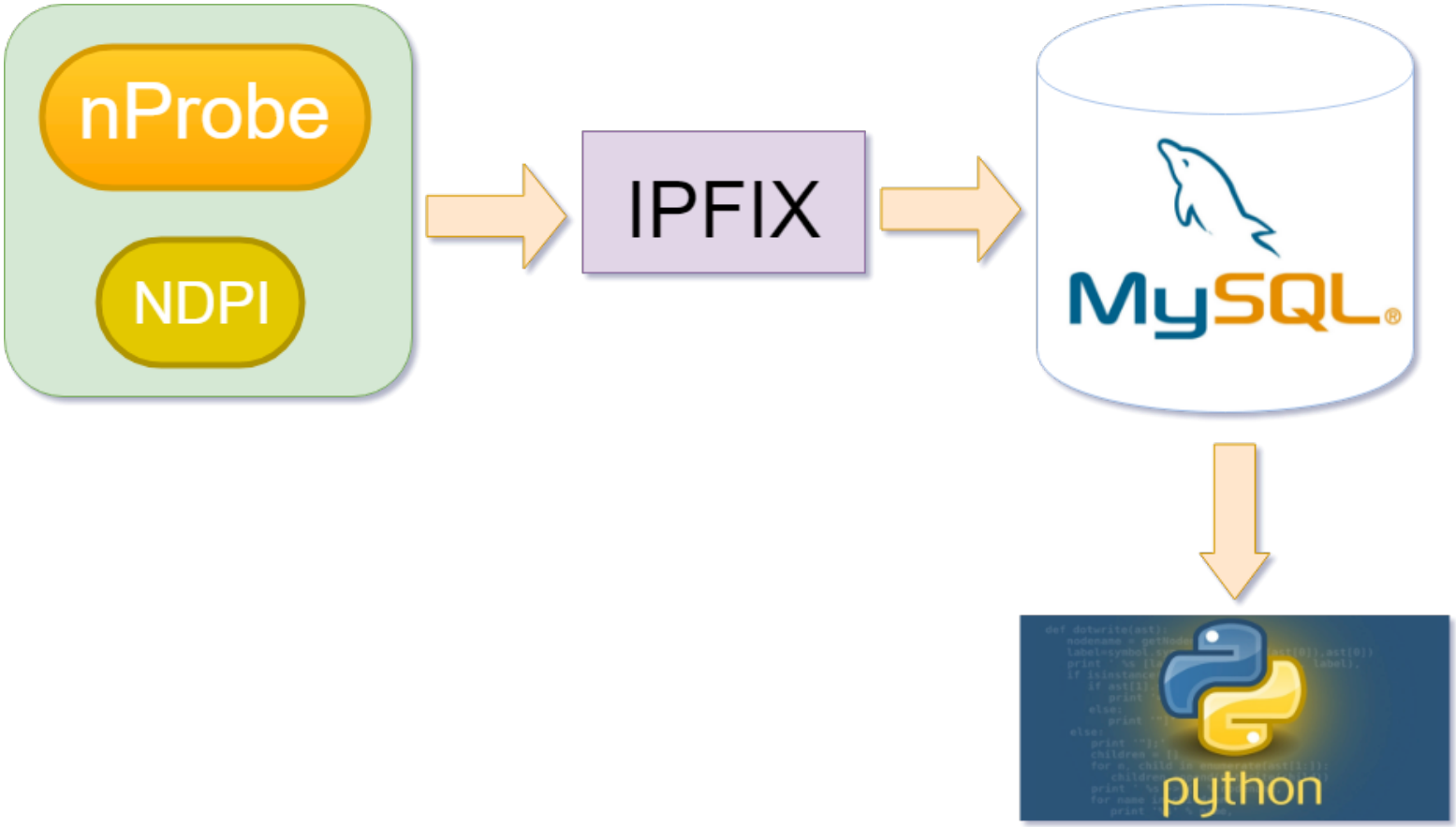


Protección a los usuarios

Enriquecimiento de la información

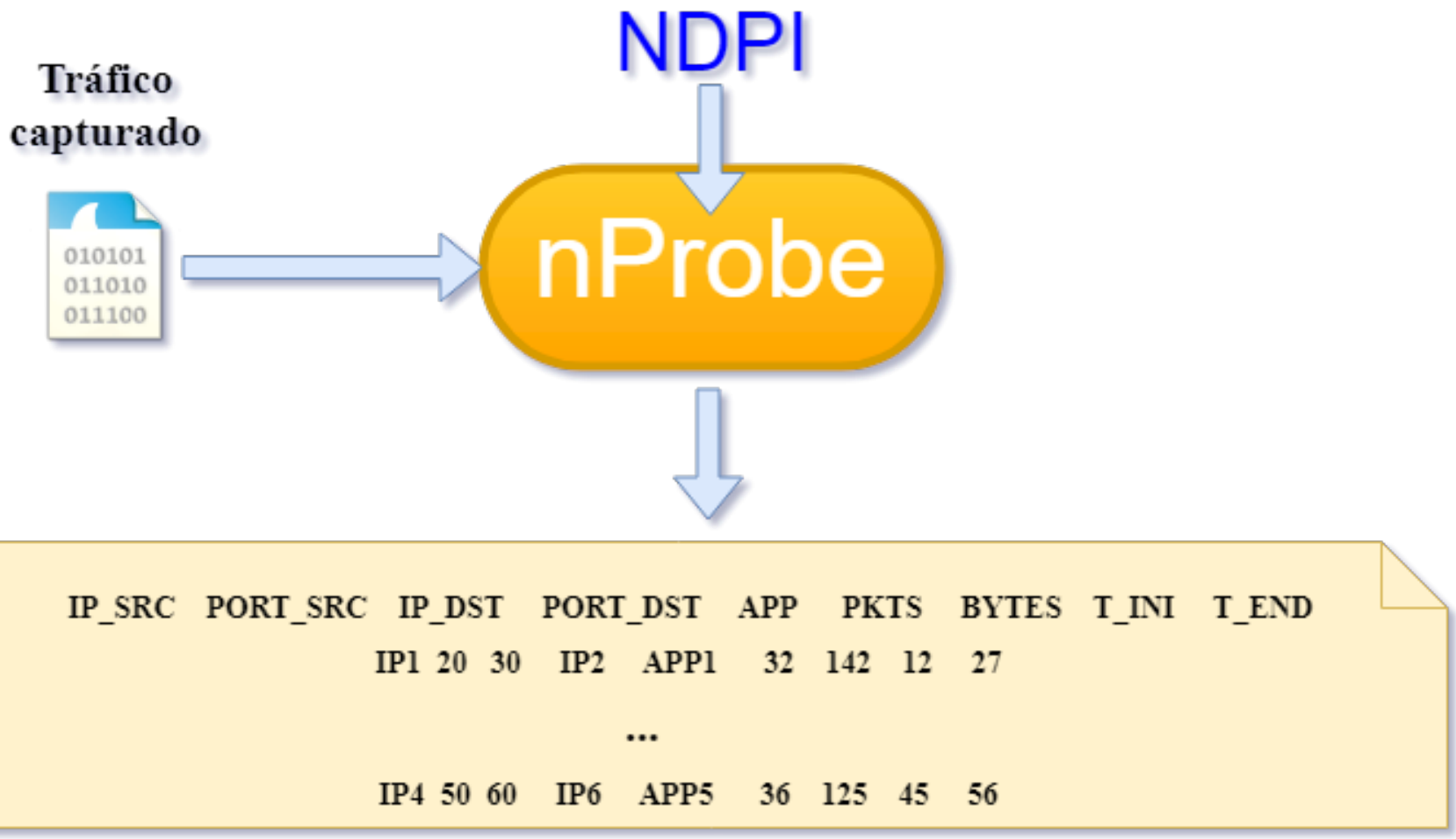
Diseño del sistema

Tecnologías

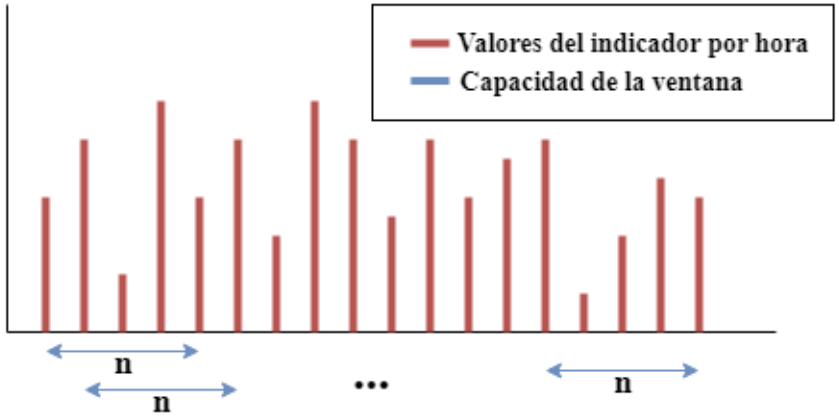


Diseño del sistema

Exportación IPFIX

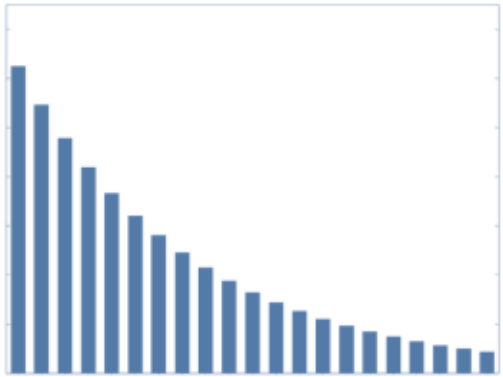


Cálculo de indicadores por franja horaria



a) Media móvil

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

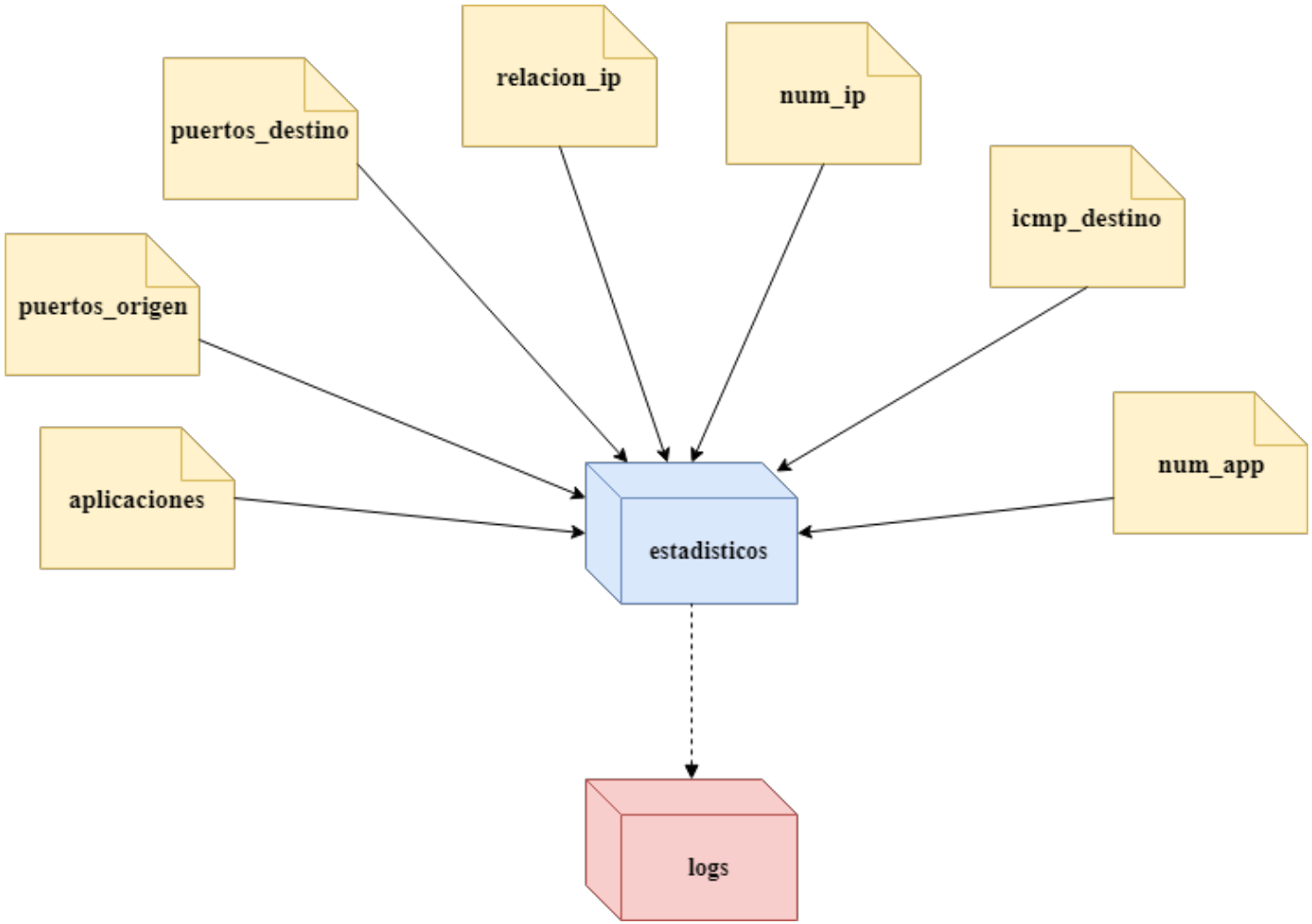


b) Media móvil exponencial

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

Diseño del sistema

Almacenamiento de los indicadores



Diseño del sistema

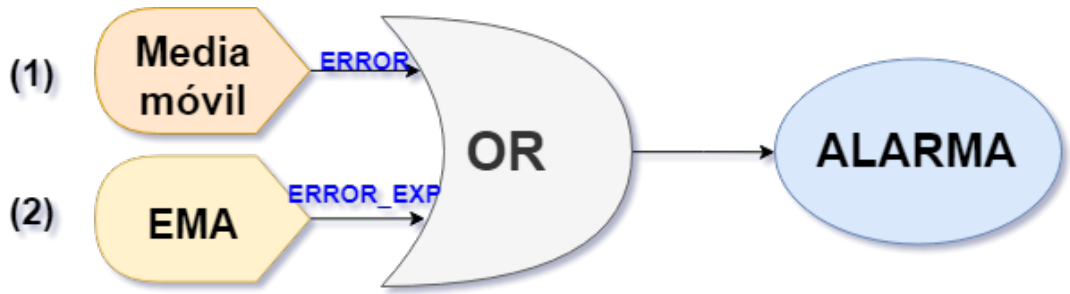
Detectores

Media móvil

$$|x_i - \mu| > \mu \pm K \times \sqrt{\sigma^2} \tag{1}$$

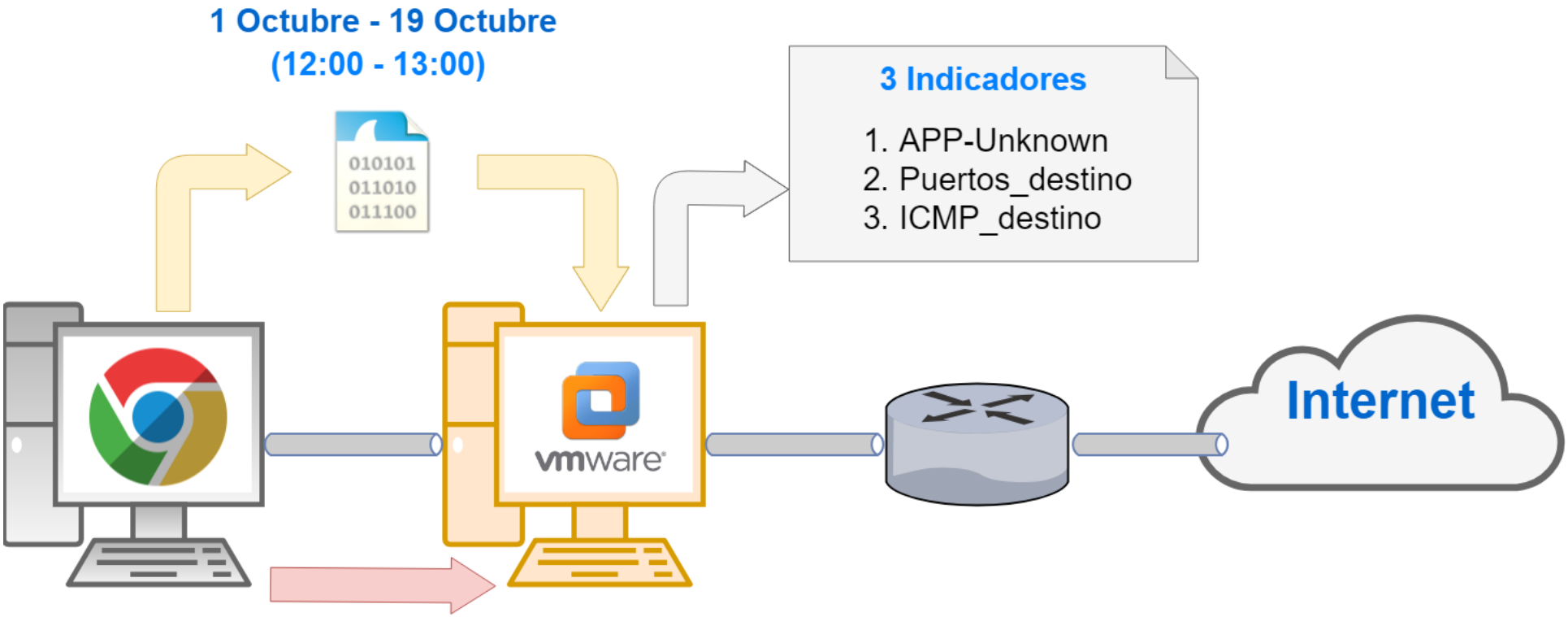
Media móvil exponencial EMA

$$|x_i - \mu_{exp}| > \mu_{exp} \pm K \times \sqrt{\sigma^2_{exp}} \tag{2}$$



Pruebas y resultados

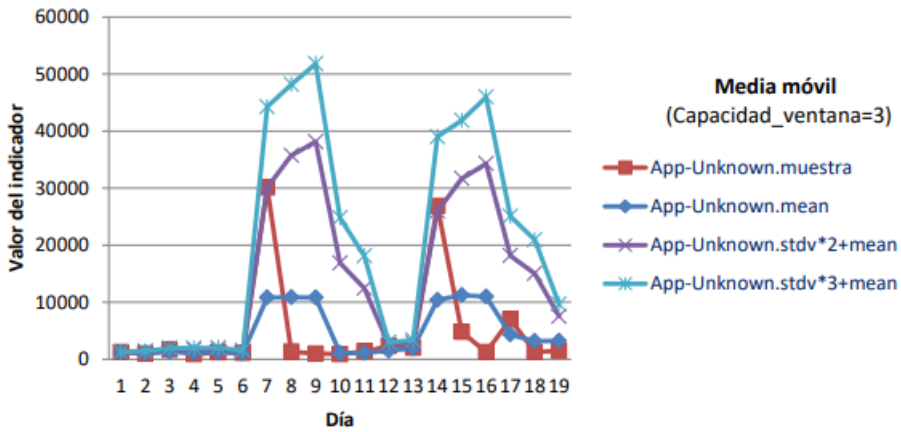
Escenario de pruebas



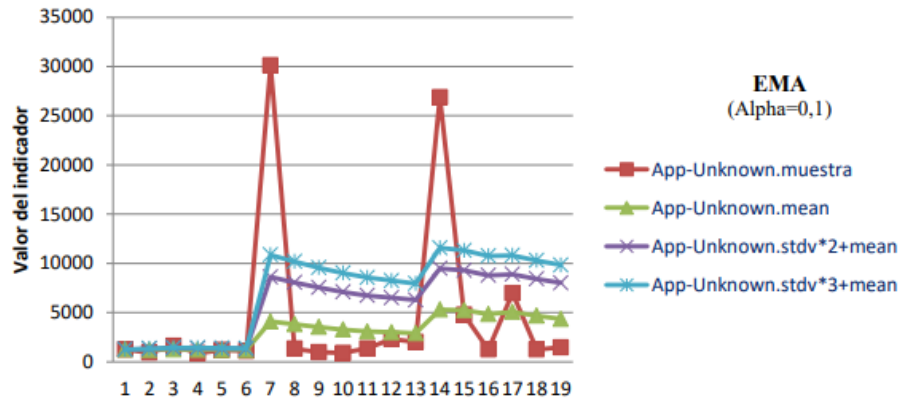
Pruebas y resultados

Indicador aplicación desconocidas

Detecciones: 7 y 14



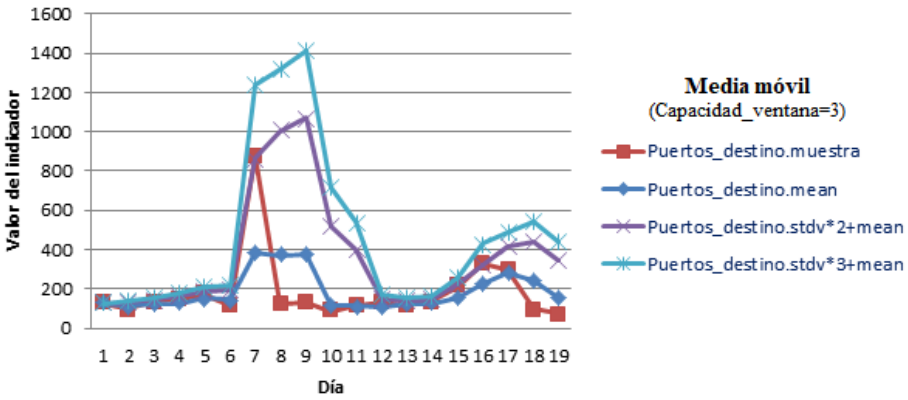
Detecciones: 3, 7 y 14



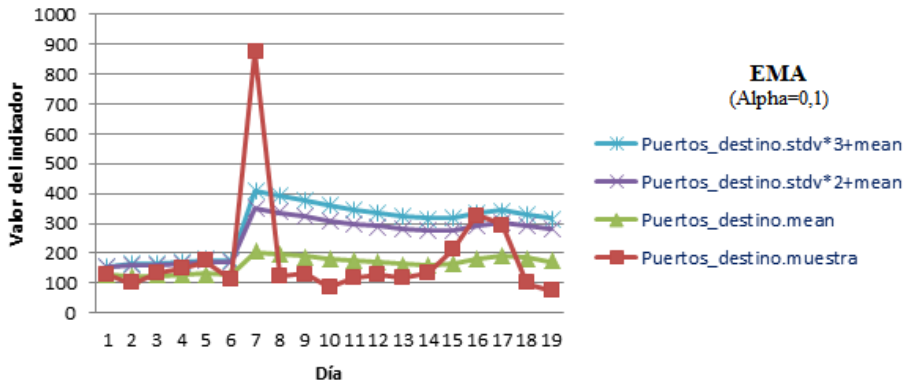
Pruebas y resultados

Indicador puertos destinos

Detecciones: 7 y 16



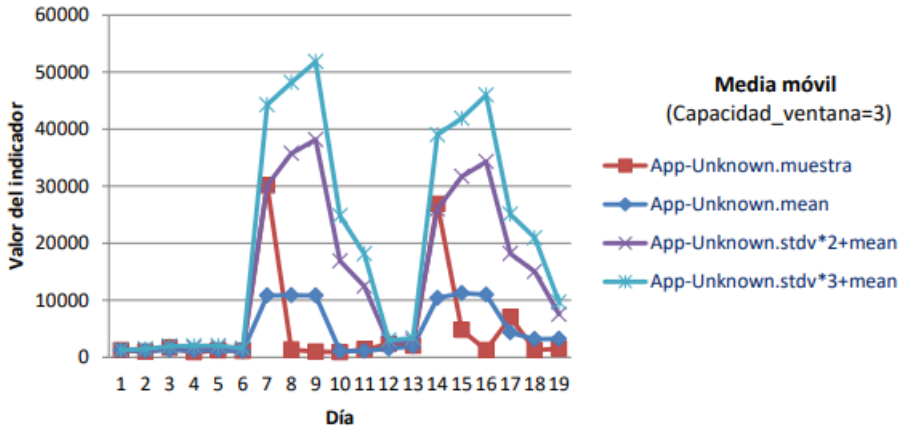
Detecciones: 7 y 16



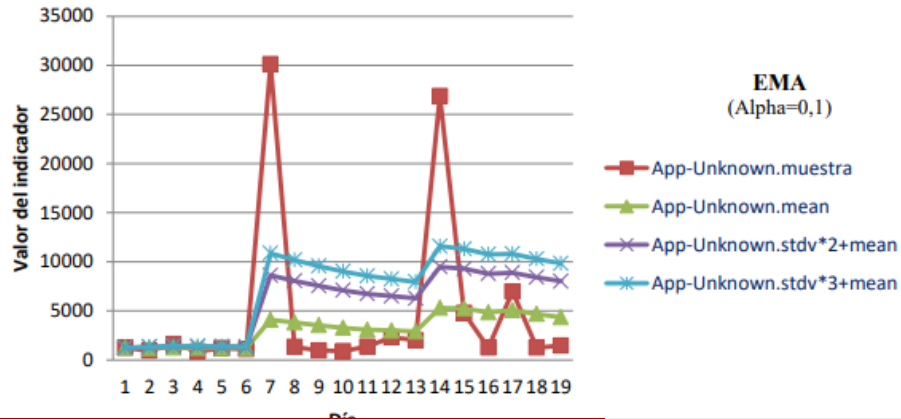
Pruebas y resultados

Indicador icmp destinos

Detecciones: 4 y 16



Detecciones: 4



Pruebas y resultados

Clasificación del tráfico

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	-	-	-
11	Bueno			
12	Bueno			
13	Bueno			
14	Malo	Alerta		
15	Bueno			
16	Bueno		Alerta	Alerta
17	Bueno			
18	Bueno			
19	Bueno			

Pruebas y resultados

Fiabilidad del sistema

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

Table: Resultados de la fiabilidad del sistema

Accuracy:

$$Accuracy(\%) = \frac{\sum_i Acierto_i}{N^o\ Total\ de\ muestras} \quad (3)$$

Conclusiones y líneas futuras

Conclusiones

- DPI
- Sistema escalable y configurable
- Buenos resultados
- Posibilidad de monitorizar la red

Conclusiones y líneas futuras

Líneas futuras

- Redes neuronales
- Fusión con firewall
- Dashboard

¡Gracias!