Detección de anomalías en los registros de tráfico ofrecidos por IPFIX

Agustín Walabonso Lara Romero

Universidad de Sevilla

2019

Índice

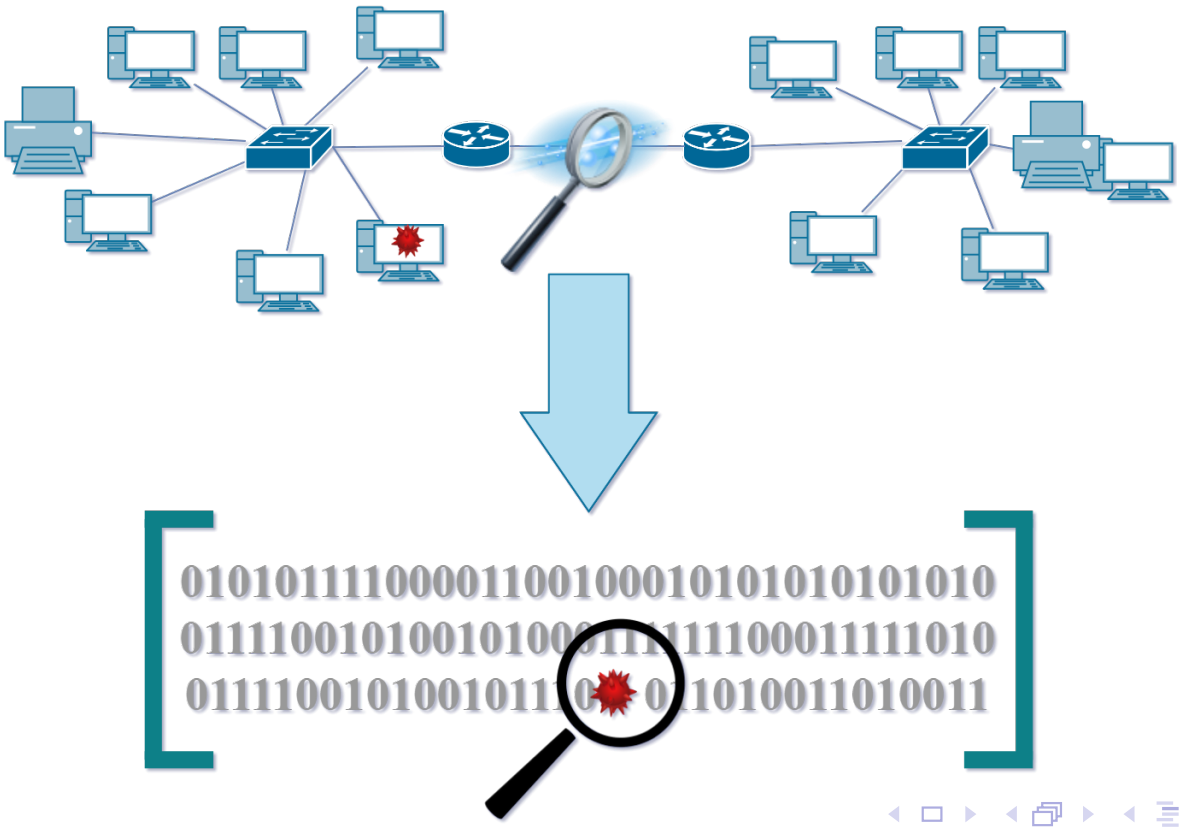
1. Índice
2. Introducción
   - Definición del problema
   - Motivación y objetivos
3. Marco teórico
   - Arquitecturas comunes en ciberseguridad
   - Solución de arquitectura propuesta
4. Diseño del sistema
   - Tecnologías
   - Implementación general
   - Exportación IPFIX
   - Cálculo de indicadores (media móvil)
   - Cálculo de indicadores (EMA)
   - Base de datos
5. Resultados obtenidos
   - Indicador aplicación desconocida
   - Fiabilidad del sistema
6. Conclusiones y líneas futuras
   - Conclusiones
   - Líneas futuras

Introducción

Definición del problema

Patrones de comportamiento

Detecciones de anomalías



Introducción

Motivación y objetivos

Gran volumen de información

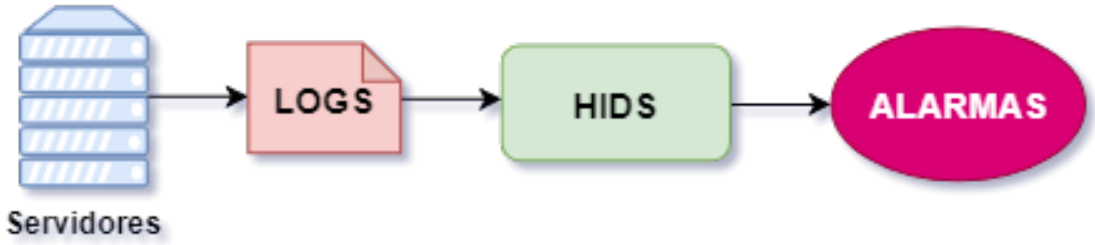
Sistema de detección

Escalabilidad

Marco teórico

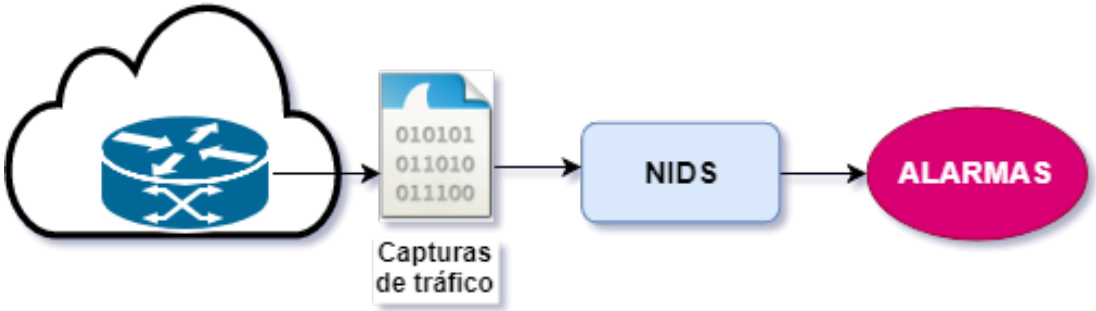
Arquitecturas comunes en ciberseguridad

Basadas en sistemas HIDS



No protege a los usuarios

Basadas en sistemas NIDS

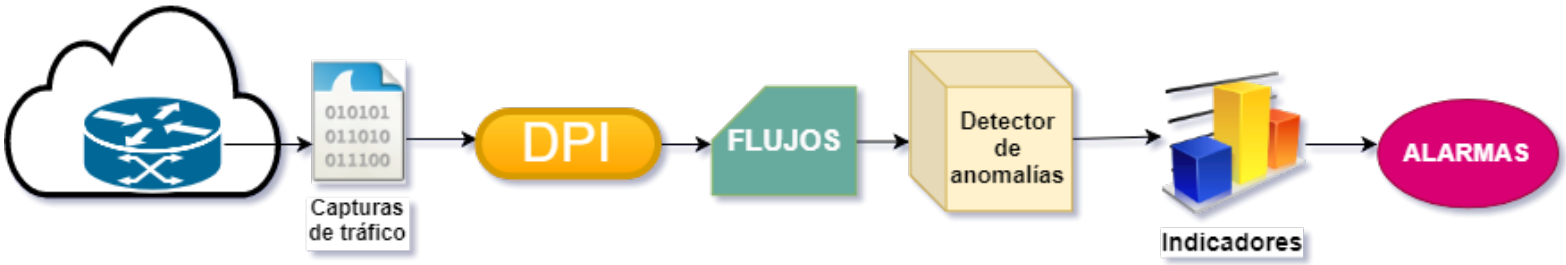


Sobrecarga al sistema de detección

Marco teórico

Solución de arquitectura propuesta

Arquitectura híbrida



Protección a los usuarios

Enriquecimiento de la información

Diseño del sistema

Tecnologías

nProbe

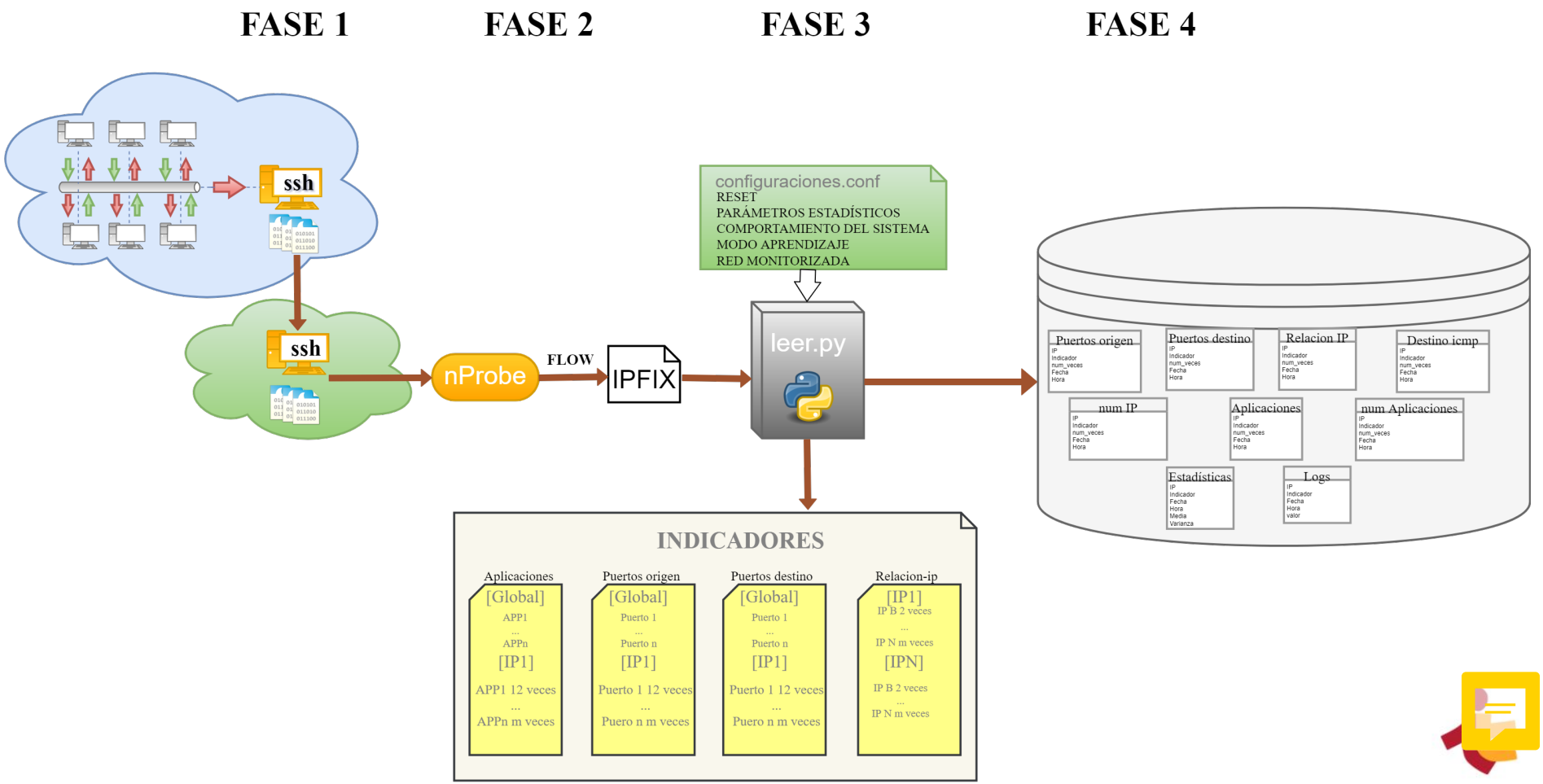
NDPI

IPFIX

MySQL®

Diseño del sistema

Implementación

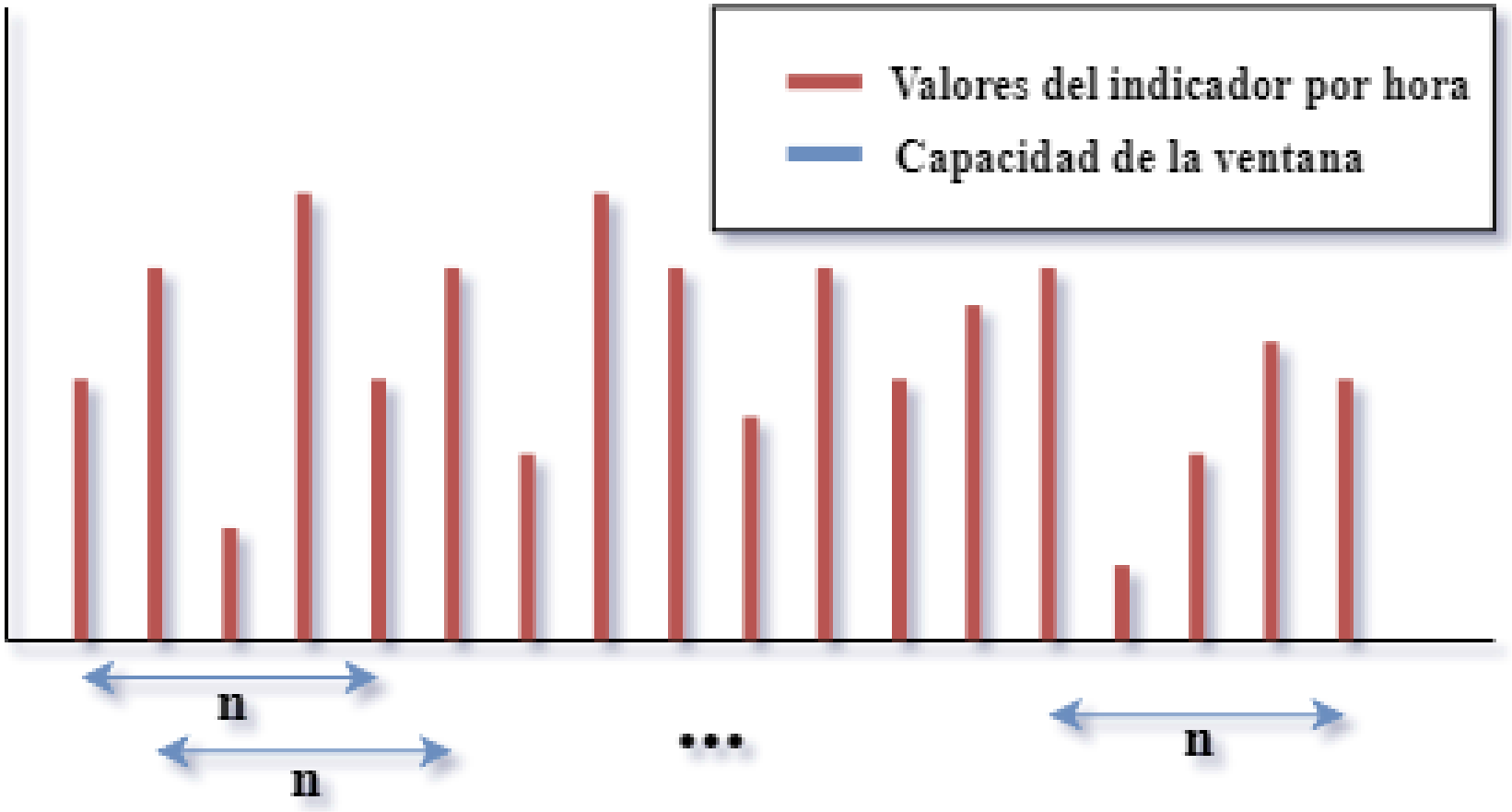


Diseño del sistema

Exportación IPFIX

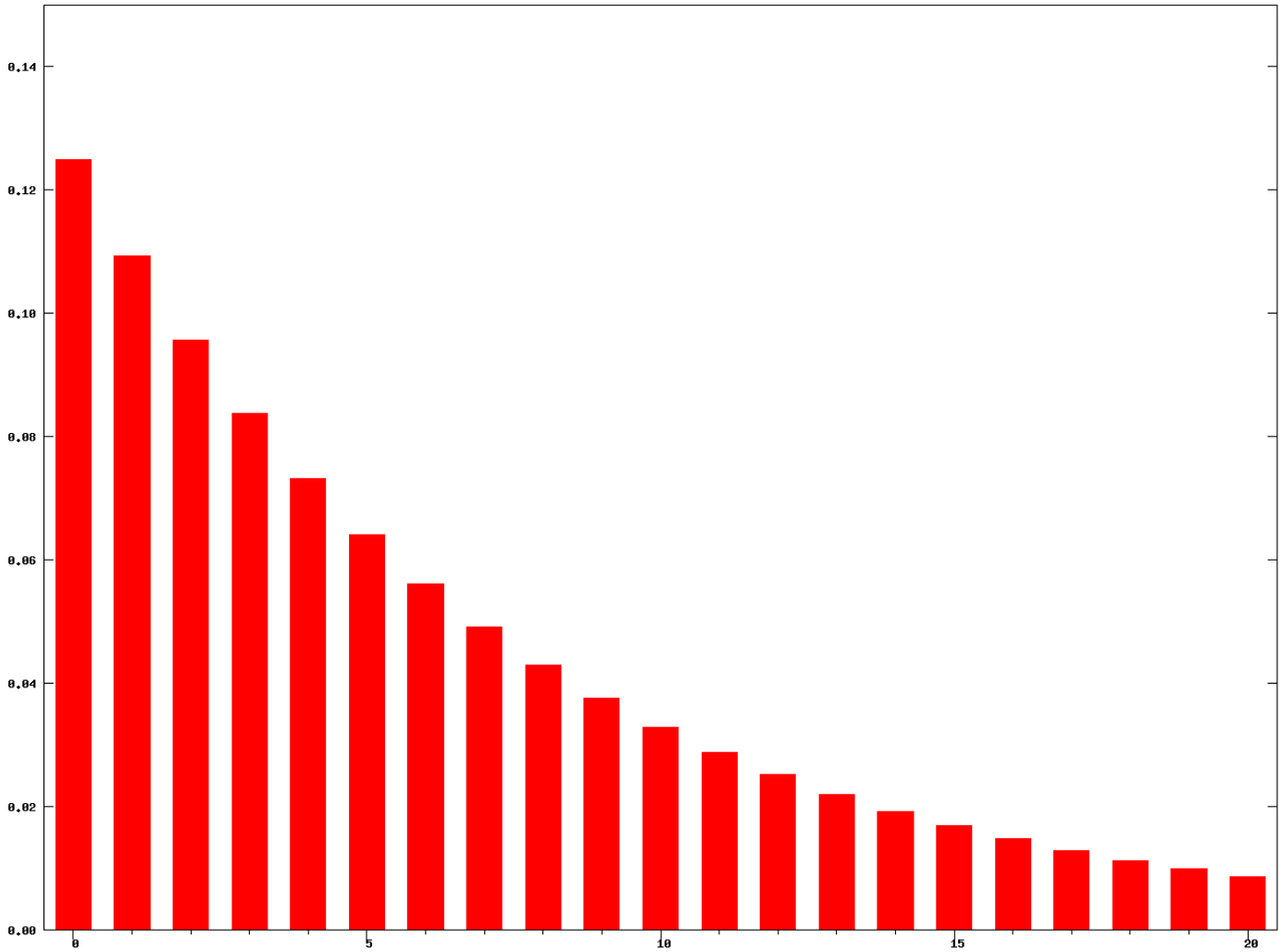
Diseño del sistema

Cálculo de indicadores (media móvil)



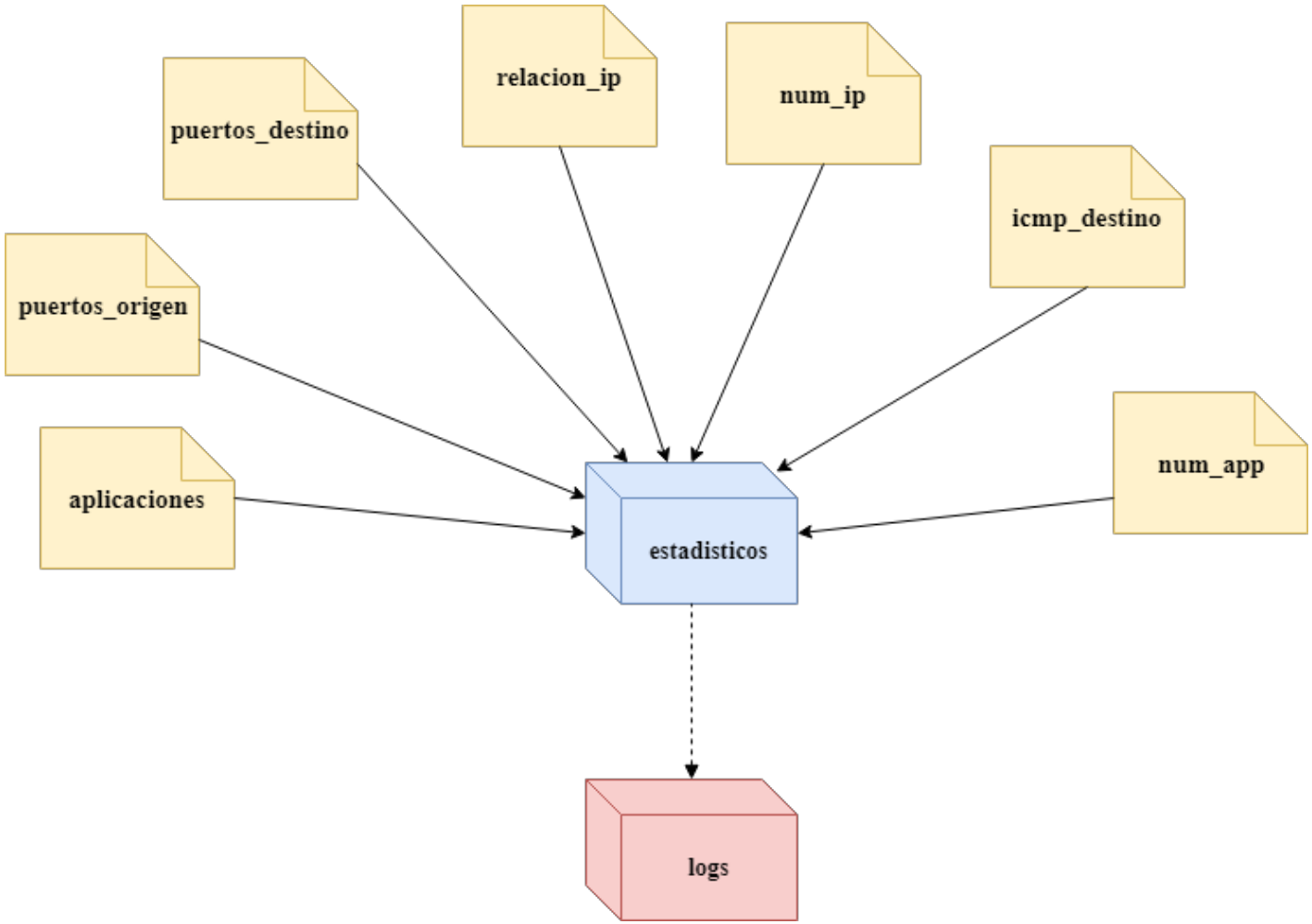
Diseño del sistema

Cálculo de indicadores (media móvil exponencial)



Diseño del sistema

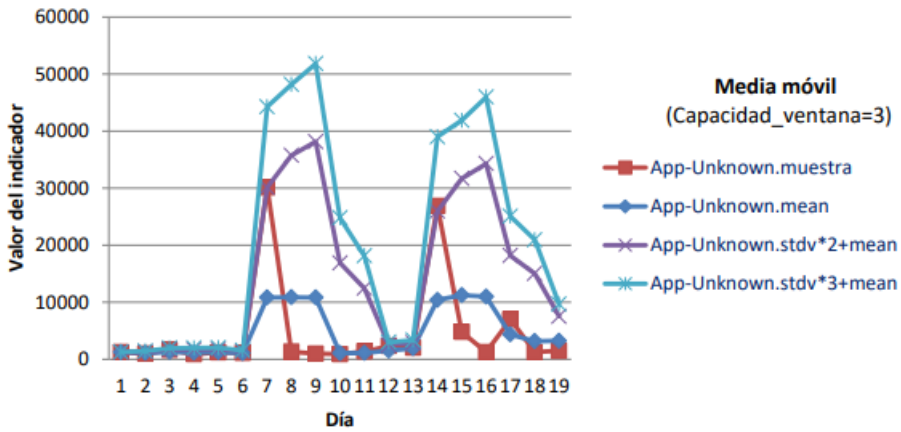
Base de datos



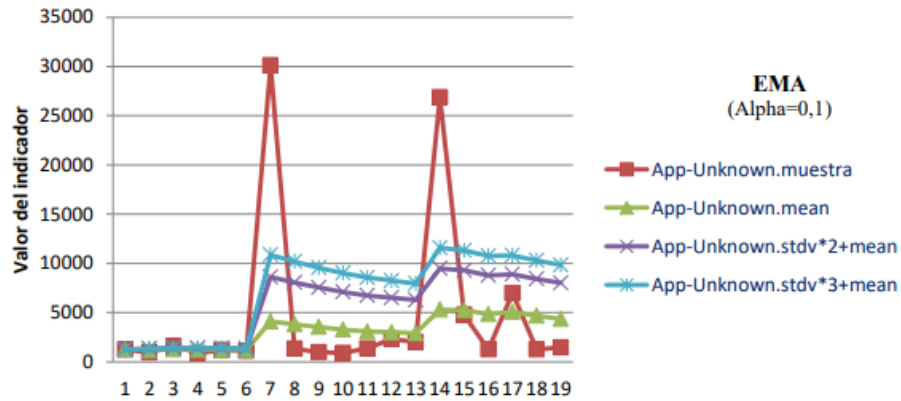
Resultados obtenidos

Indicador aplicación desconocida

Detecciones: 7 y 14



Detecciones: 3, 7 y 14



Resultados obtenidos

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	84,21	78,95	78,95

Table: Resultados de la fiabilidad del sistema

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!