Detección de Intrusiones en Entornos Windows: Nuevas perspectivas

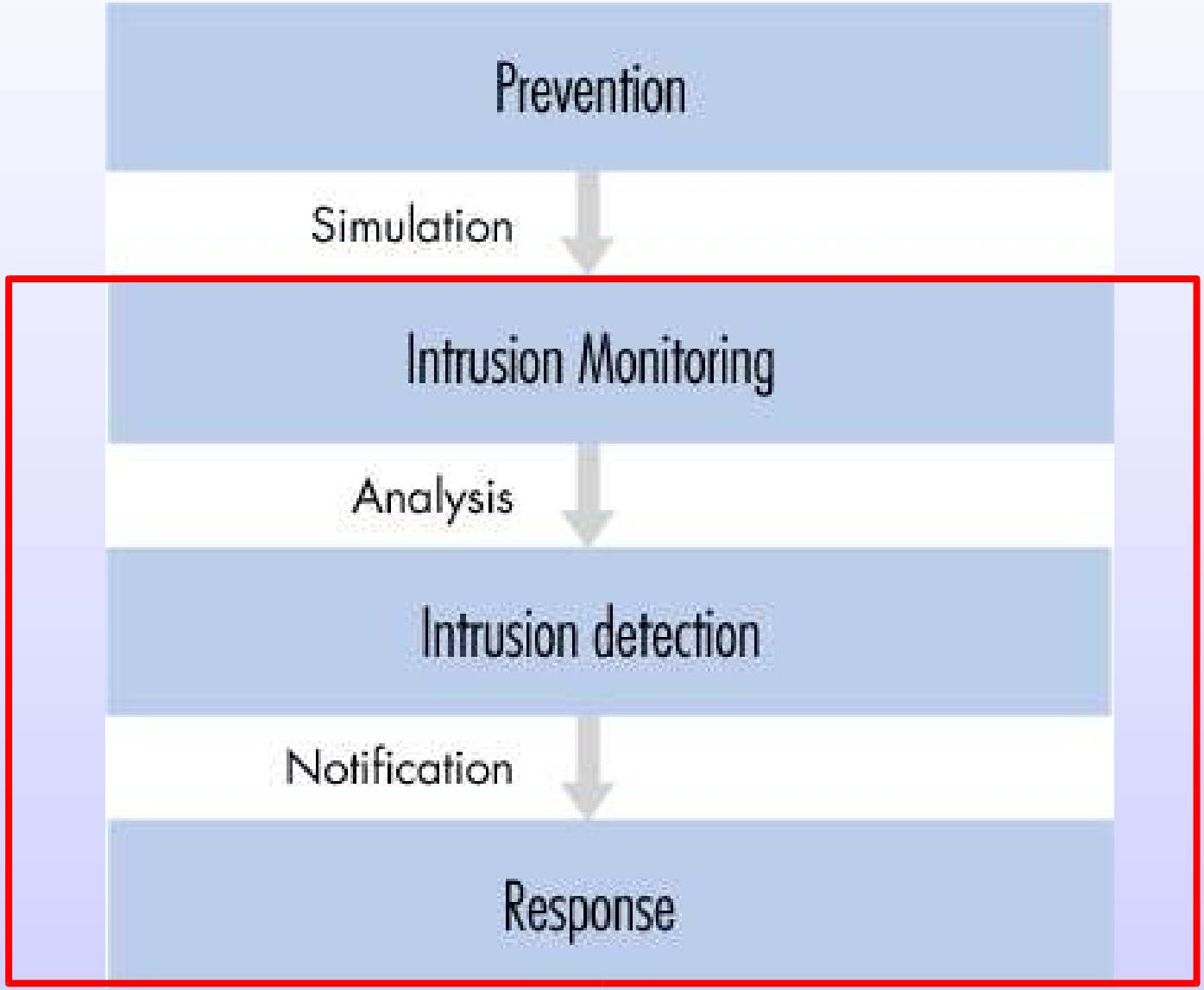
Robert Rallo y Jordi Duch

Dep. D'Enginyeria Informàtica i Matemàtiques
ETSE – Universitat Rovira i Virgili

Agenda

- Los Sistemas de Detección de Intrusiones
  - Conceptos básicos
  - Tipología
  - Arquitectura y Componentes
  - Ubicación
- Sistemas IDS para windows.
- Nuevas tendencias para los IDS
  - Inconvenientes básicos que plantea un IDS
  - Sistemas inteligentes
  - Sistemas distribuidos a gran escala:airCERT

El siguiente paso ...



IDS: Definición y Conceptos

- Detección de actividades inapropiadas o anómalas en un sistema informático.
- Básicamente de dos tipos: Host-based, Network based.
- HIDS: Monitorización de actividades en la propia máquina.
- NIDS: Monitorización de actividades en la red.

- Actúan como sistemas de alarma. Generalmente requieren la intervención de los responsables de seguridad de la institución

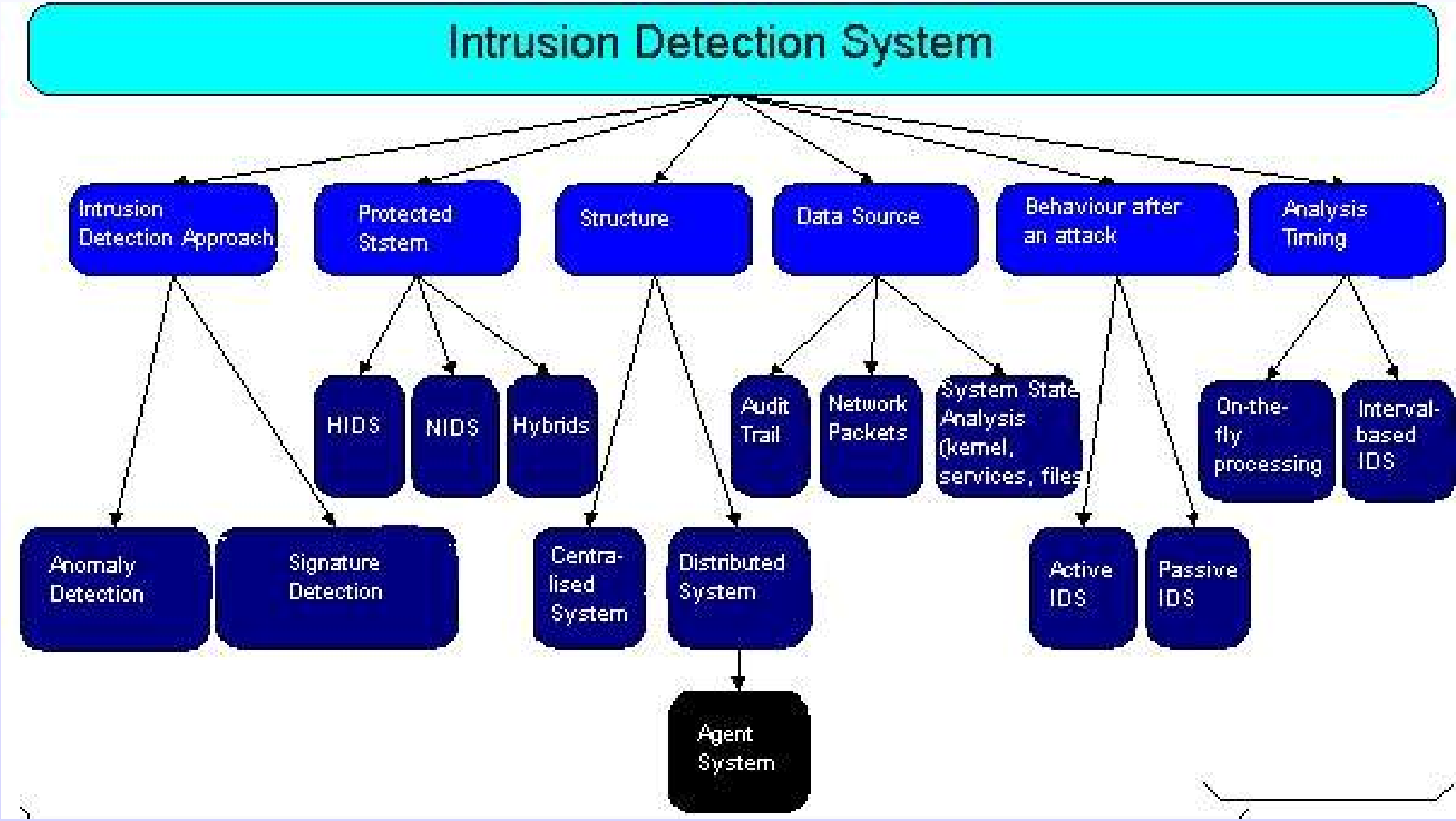
Tipos de IDS

- En función del tipo de tráfico, actividades o sistemas monitorizados:
  - basados en red
  - basados en el host
  - basados en una aplicación concreta
- En función del mecanismo de detección:

  Basados en firmas (Signature-based)

  Detectores de anomalías (Anomaly –based)

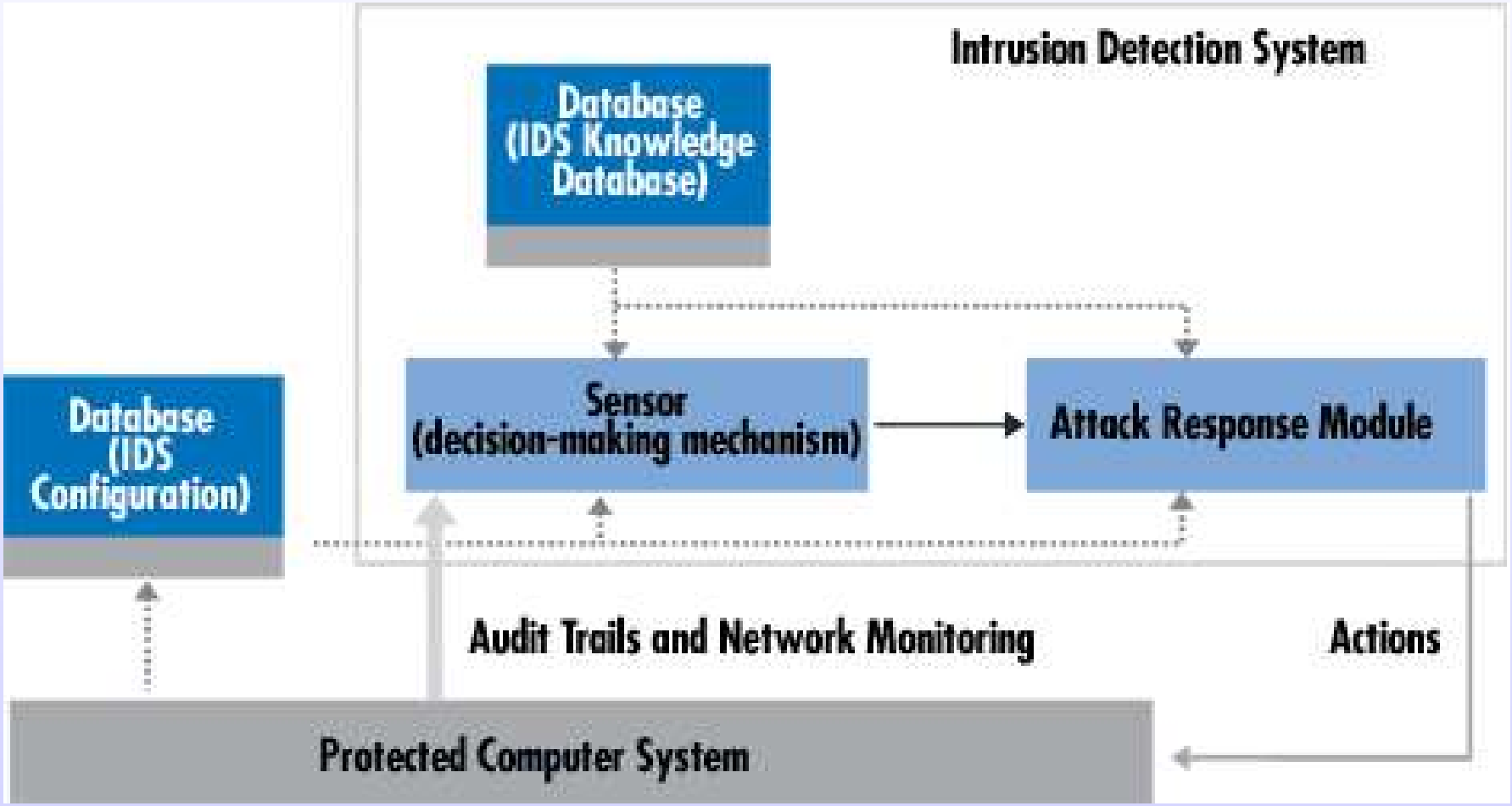
Clasificación de los IDS



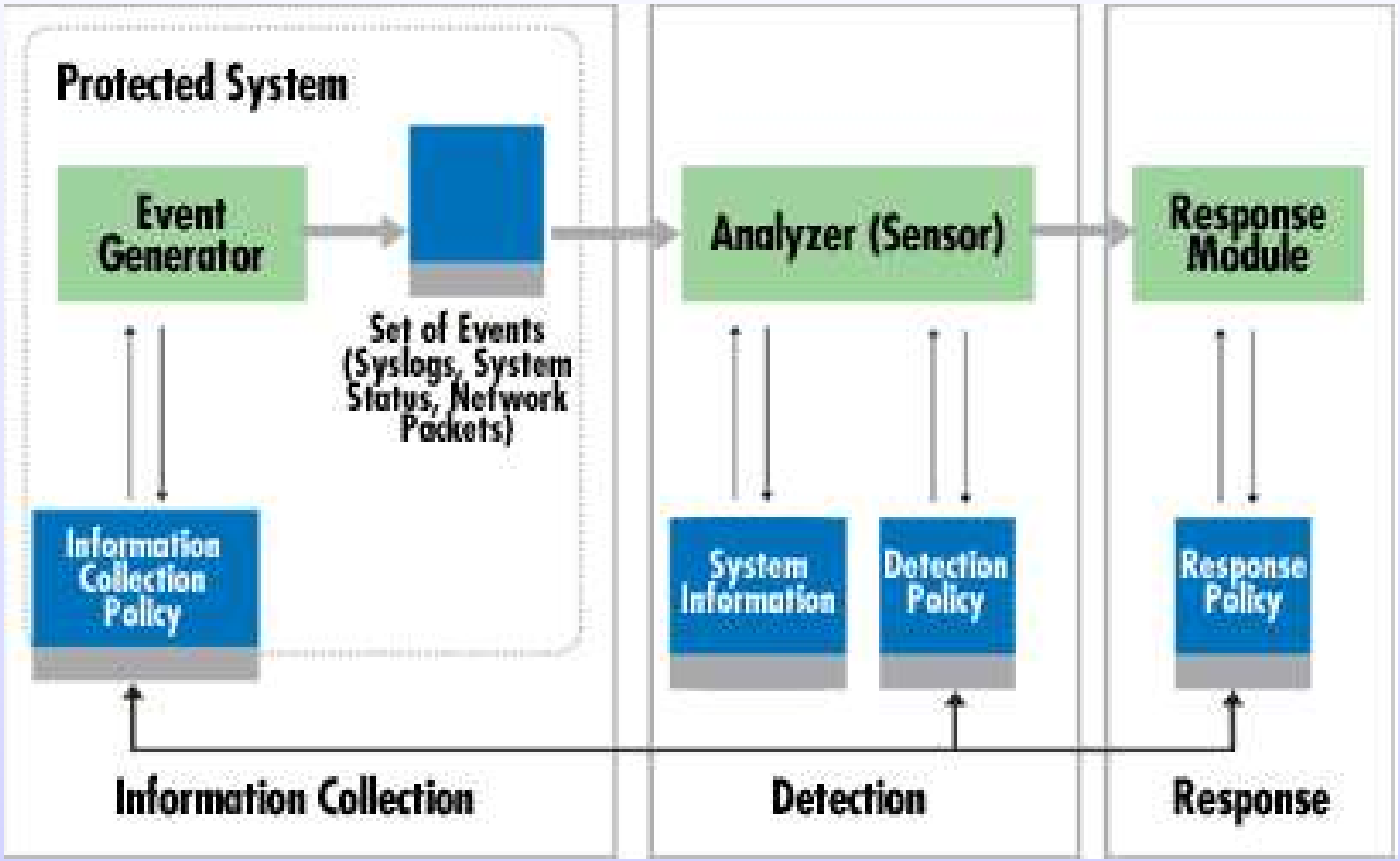
IDS Activo

- Rotura de la conexión TCP mediante la inyección de paquetes de “reset”
- Generación automática de filtros de paquetes en routers o firewalls para detener un ataque (filtrado del protocolo y direcciones del atacante)
- En casos graves pueden llegar incluso a la desconexión automática de routers, firewalls o los servidores atacados.
- Activación de “contramedidas”, en las que el sistema atacado puede:
  - recopilar activamente información sobre el ataque (resolución DNS, consultas WHOIS, etc)
  - Atacar al sistema ofensivo, por ejemplo DoS
- Plantea problemas éticos e incluso legales !!

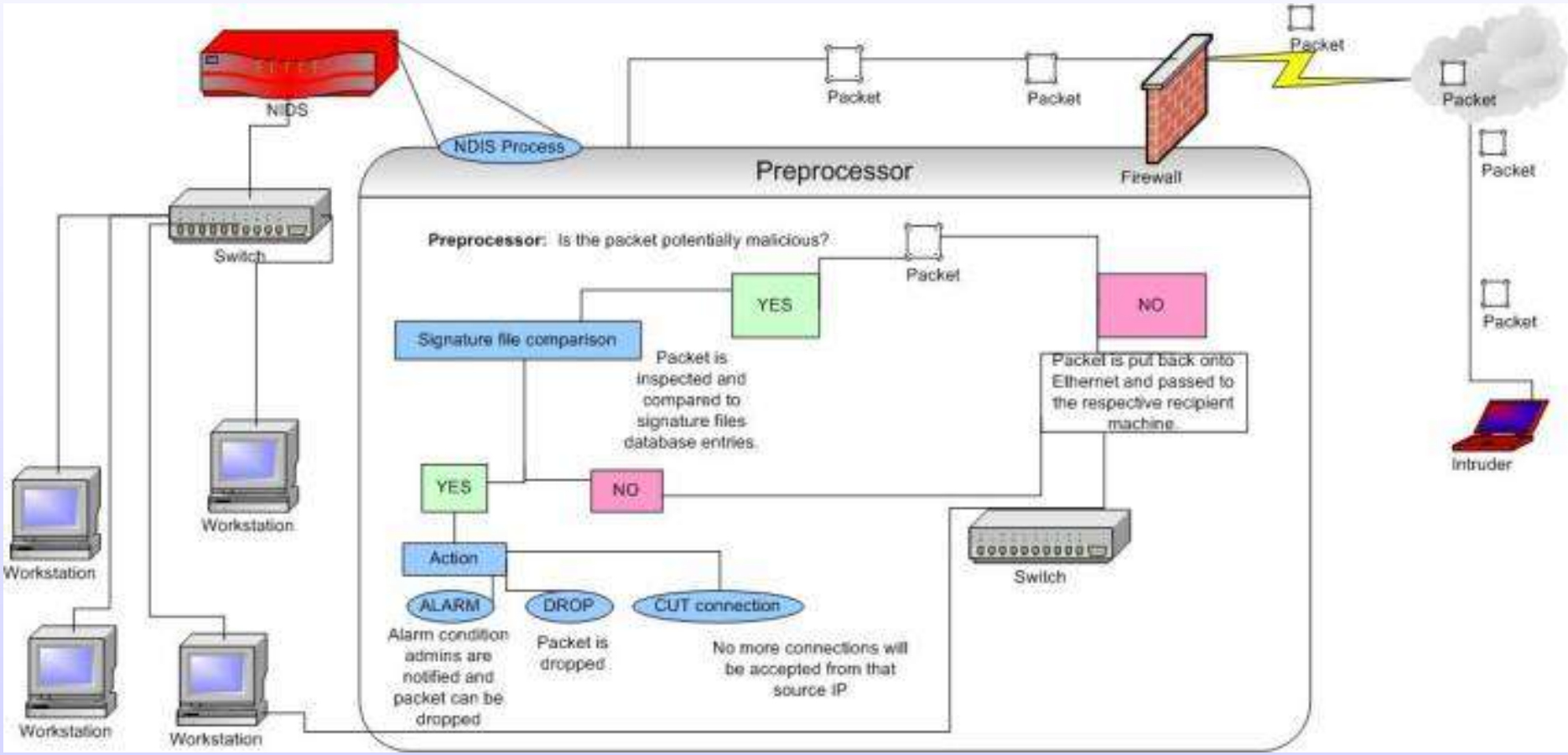
Arquitectura Interna de un IDS



Componentes de un IDS



Funcionamiento del IDS



Ubicación del IDS

- ¿qué queremos proteger?
- Maximizar la efectividad y la interoperabilidad con otros sistemas de protección (efecto combinado)
- Protección del sensor
- Protección de la comunicación con la consola de análisis
- Posibilidades:
  - En la red “interna”, después del firewall
  - En la DMZ
  - Antes del firewall

IDS detrás del firewall

- PROS
  - Permite controlar actividades anómalas, tanto provenientes del exterior como de nuestra propia red
  - Actúa como respaldo del propio firewall
- CONS
  - Modelo no-escalable
  - Muy sensible al tráfico interno (especialmente el windows)
  - Port-mirroring necesario en los conmutadores

IDS en la DMZ

- PROS

  Esquema adecuado para proteger los “servicios visibles” de nuestra organización

- CONS

  Nivel muy alto de “falsos positivos”

  Es necesario distinguir entre diversos niveles de compromiso en las actividades detectadas.

  escaneos aleatorios vs. Actividades realmente “peligrosas”

  Requieren un ajuste en profundidad de las reglas del IDS

IDS antes del firewall

- PROS

  Permite controlar desde un único punto los ataques hacia nuestra red interna y los servidores públicos

- CONS

  El tráfico interno es invisible al IDS

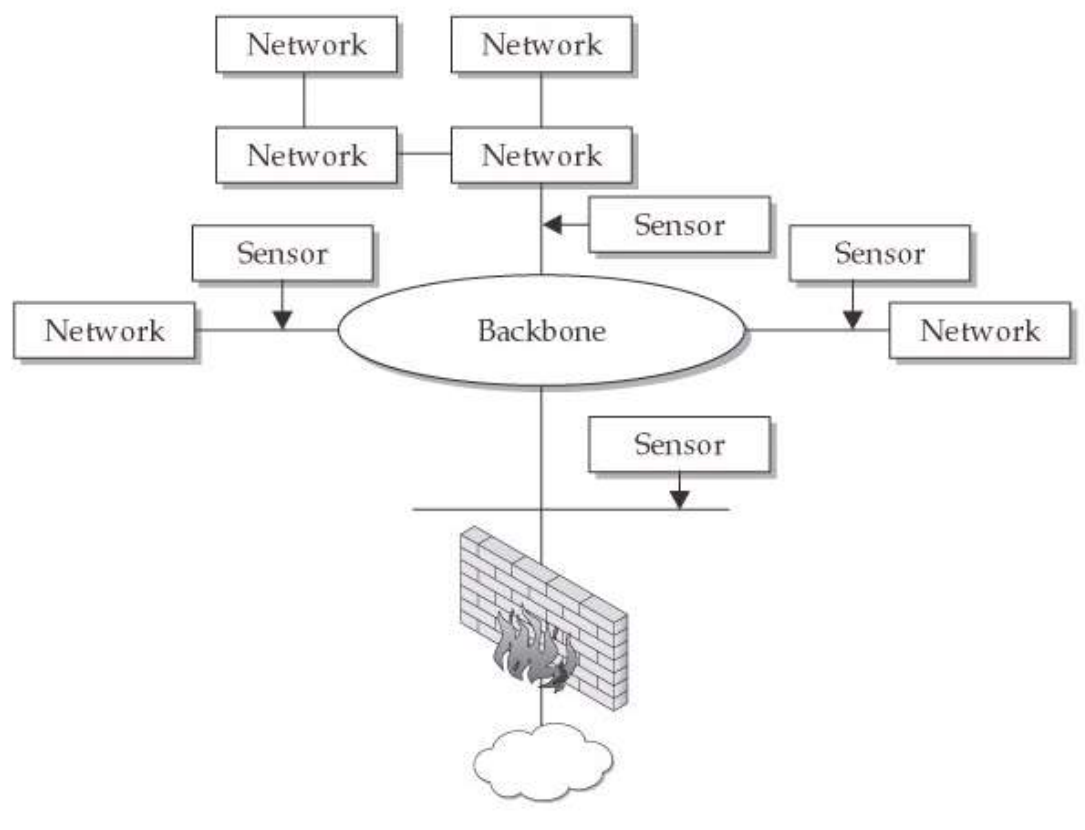
  El “ruido de fondo” de ataques aleatorios genera gran cantidad de alarmas

  En determinadas condiciones puede convertirse en un “cuello de botella” para el tráfico de red.

  Es necesario el ajuste del IDS para un correcto funcionamiento

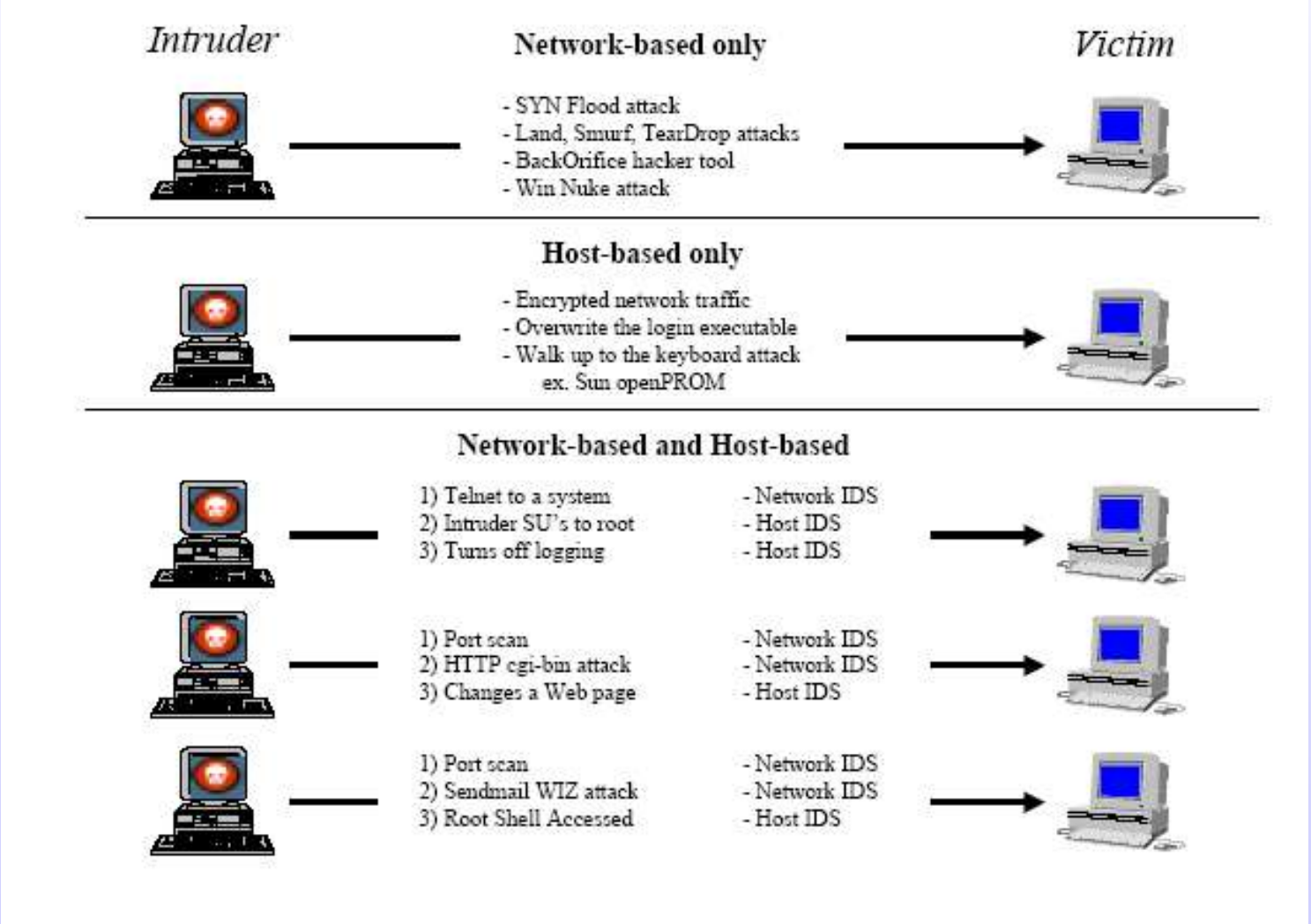
Ubicación del sensor

- Modelo híbrido
- Desplegados en una VLAN de sensores
- Combinación de NIDS y HIDS

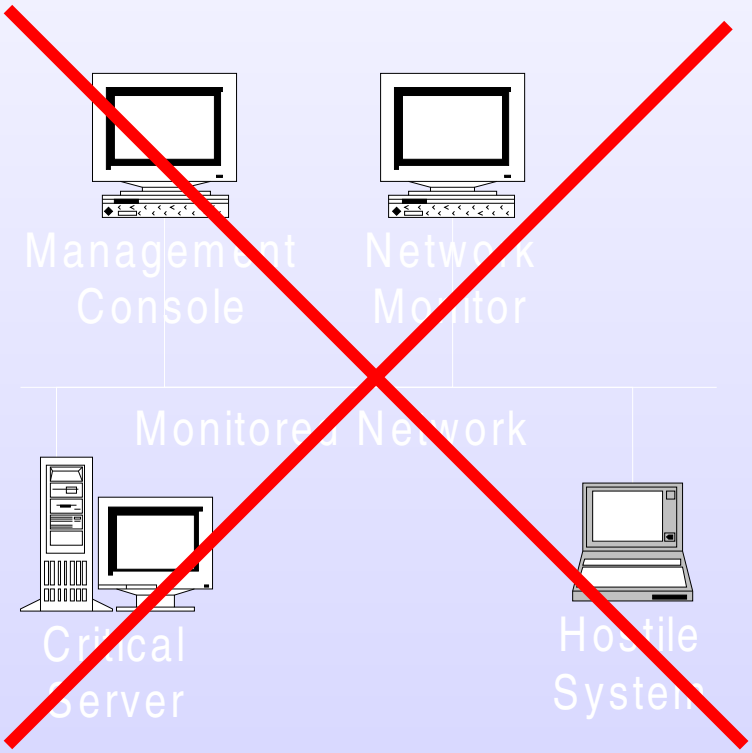


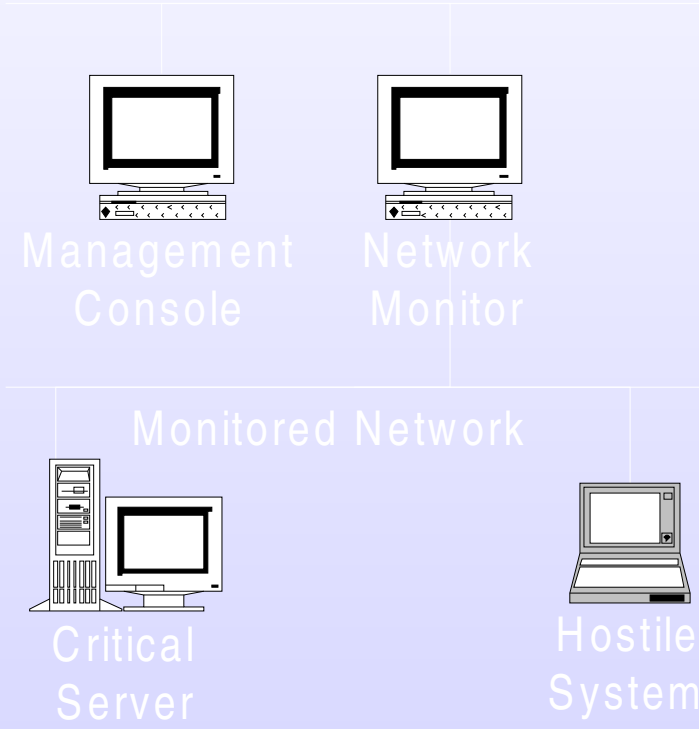
HIDS & NIDS

- La combinación de ambos produce los mejores resultados



Arquitectura de un IDS





Problemas derivados de una incorrecta arquitectura.

- *La consola de gestión ubicada en el mismo segmento físico de red que el IDS*
- Ataque MAC:
  - Identificar la máquina sobre la que esta corriendo el IDS
  - Modificar la dirección MAC del router
  - Modificar la MAC de la consola o la estación de gestión

Configuración alternativa: uso de TAPs

- Desviamos todo el tráfico de cada subred (a nivel del firewall o router) hacia el IDS

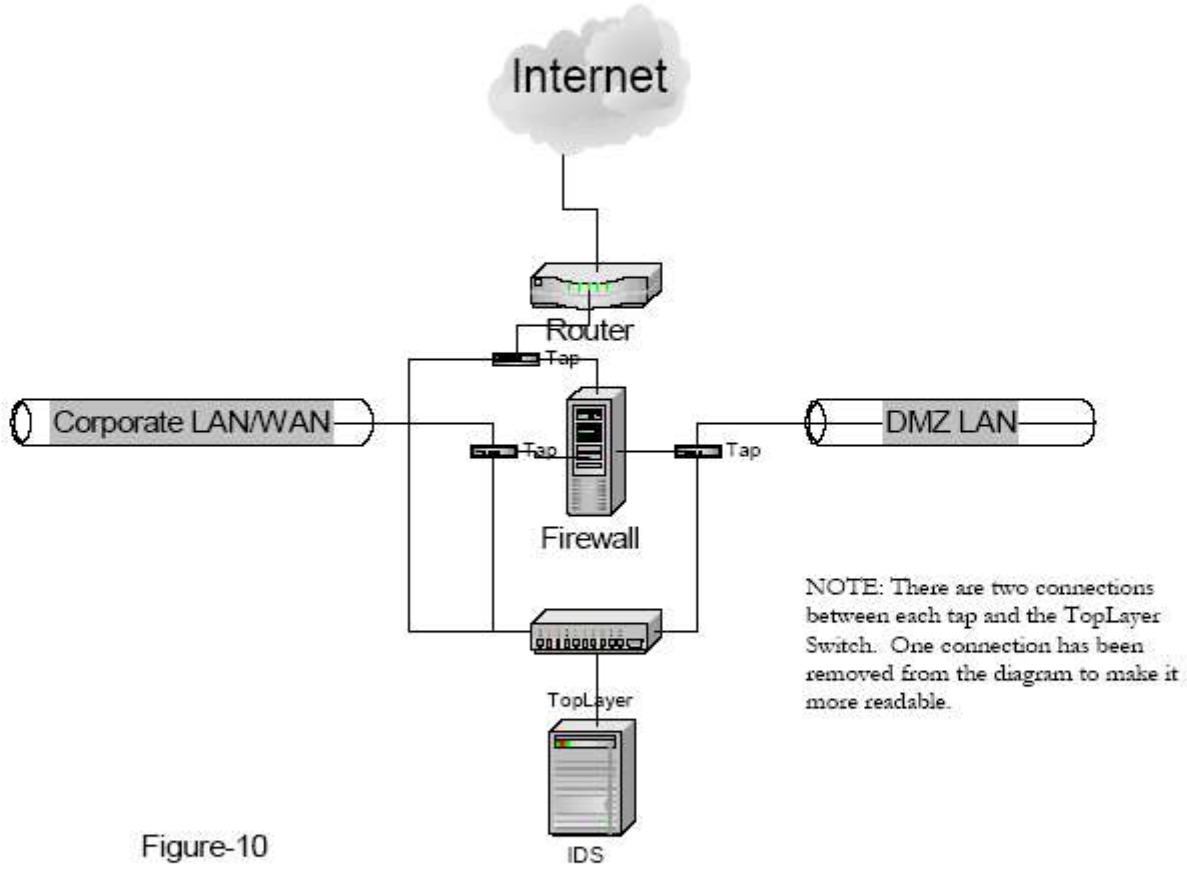


Figure-10

Pasos en el diseño e instalación de un IDS

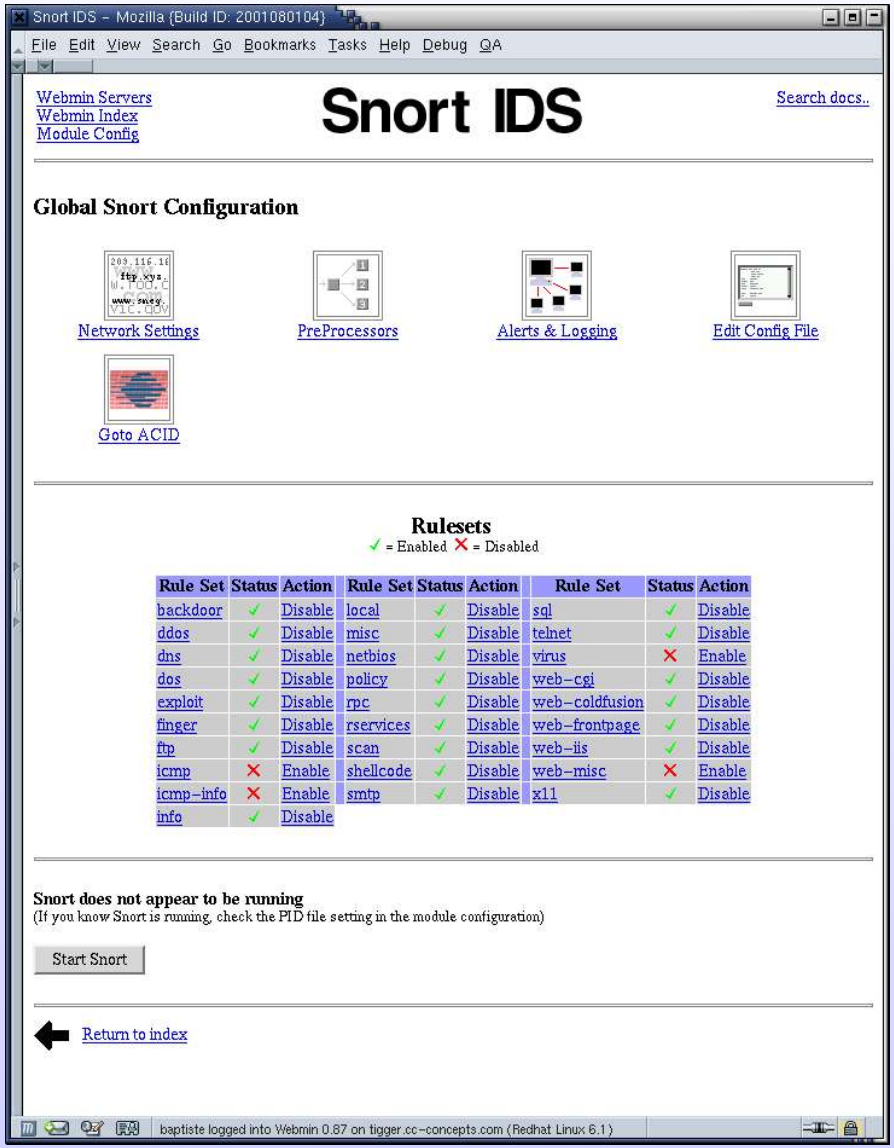
- Diseño de la arquitectura del IDS
  (ubicación de los sensores)
- Instalación del IDS
- Instalación de la consola de Gestión
- Protección del sensor
  (protección del sistema operativo)
- Instalación del sistema de Análisis de datos y alarmas
- Ajuste y configuración de los distintos sensores
  (tipos de reglas, acciones a monitorizar, etc ...)

Complementos a un IDS

- Consola de gestión
- Entorno de Análisis
- Gestión centralizada de Logs
- Honeypots y honeynets (reales y virtuales)
- ...

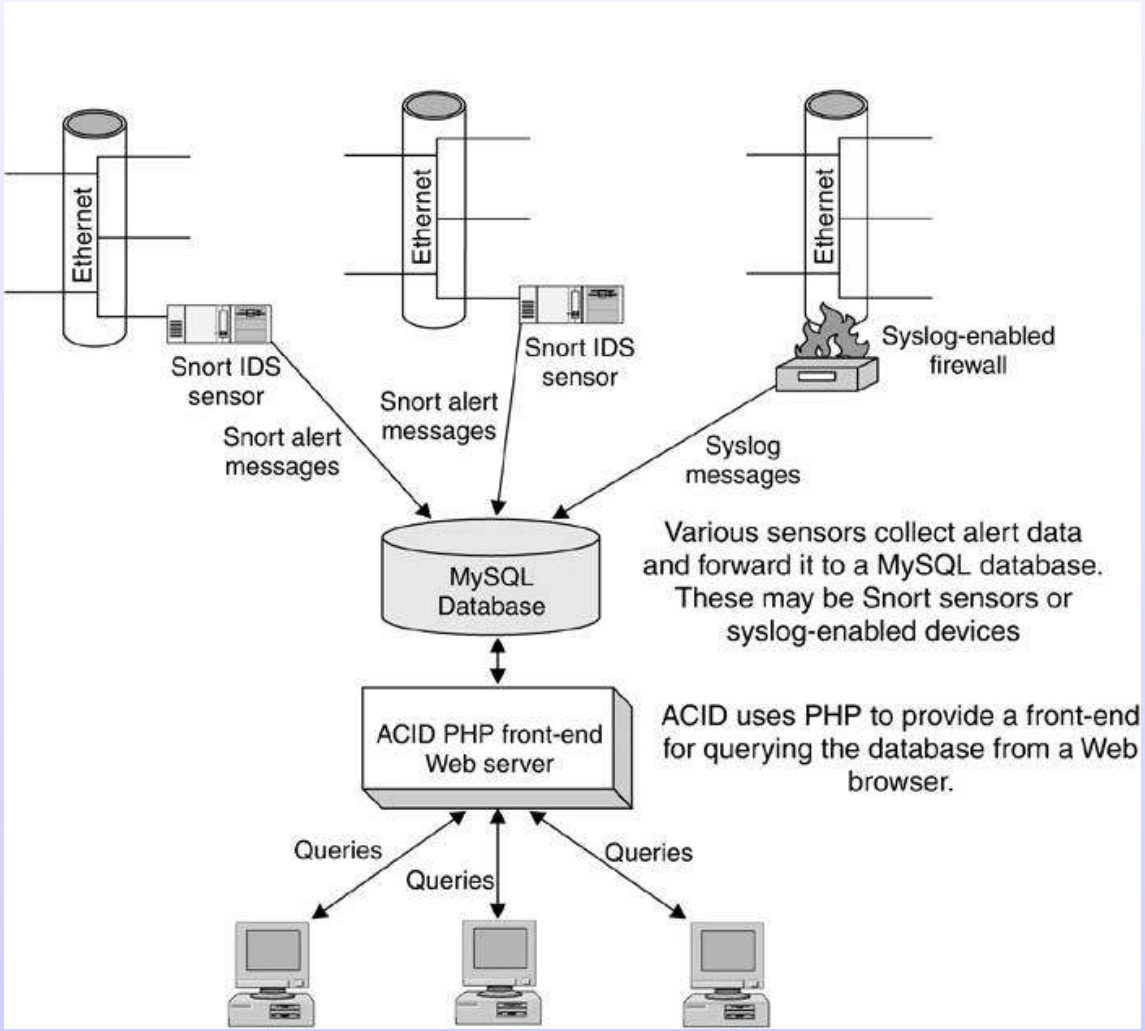
Snort i Webmin

- Integración en la aplicación web
- Gestión sencilla del sensor
- http://msbnetworks.net/snort



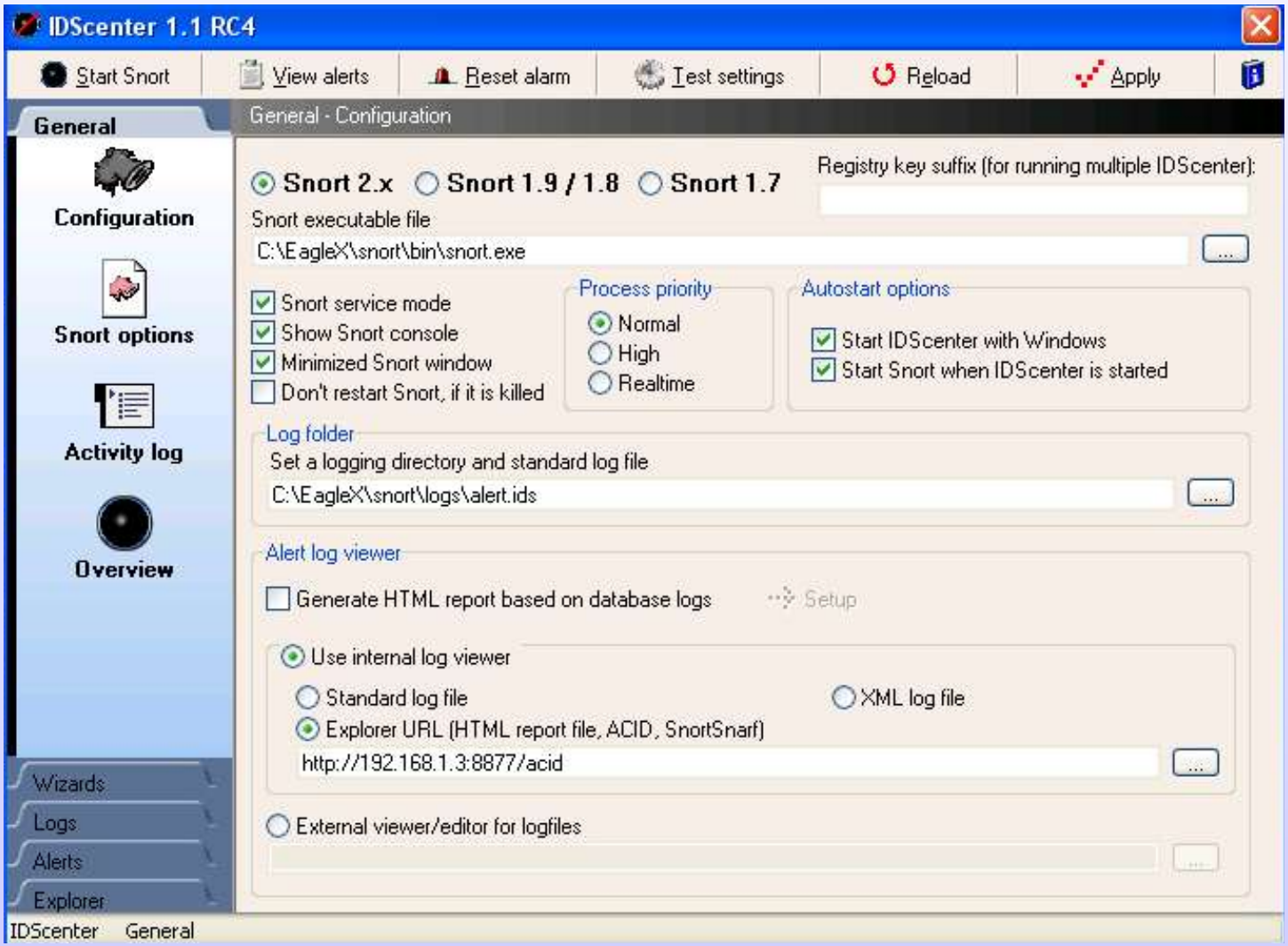
SNORT y ACID

- És el más usado, proporciona una consola unificada de análisis para una red de sensores



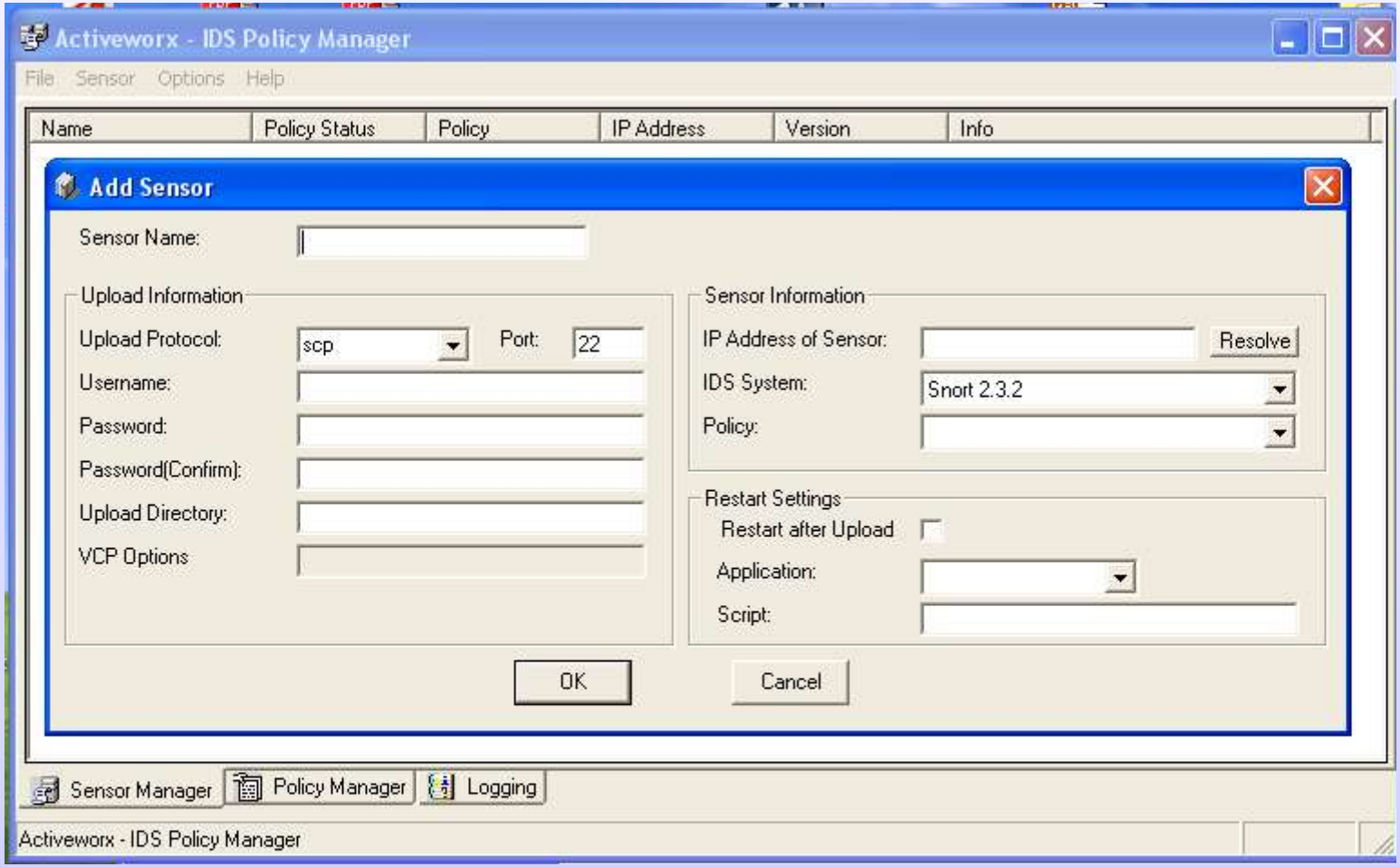
IDSCenter

- Aplicación windows
- Proporciona una consola de gestión para SNORT



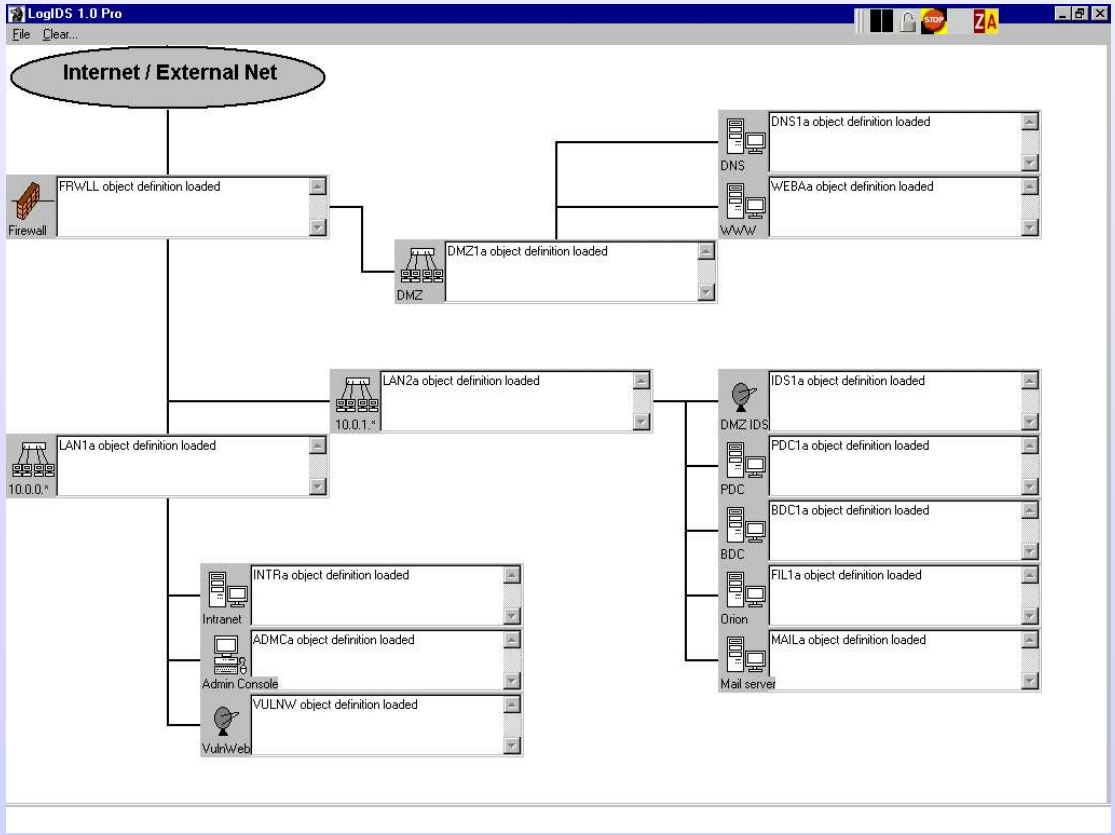
IDSPolicy Manager

- http://www.activeworx.org/programs/idspm/



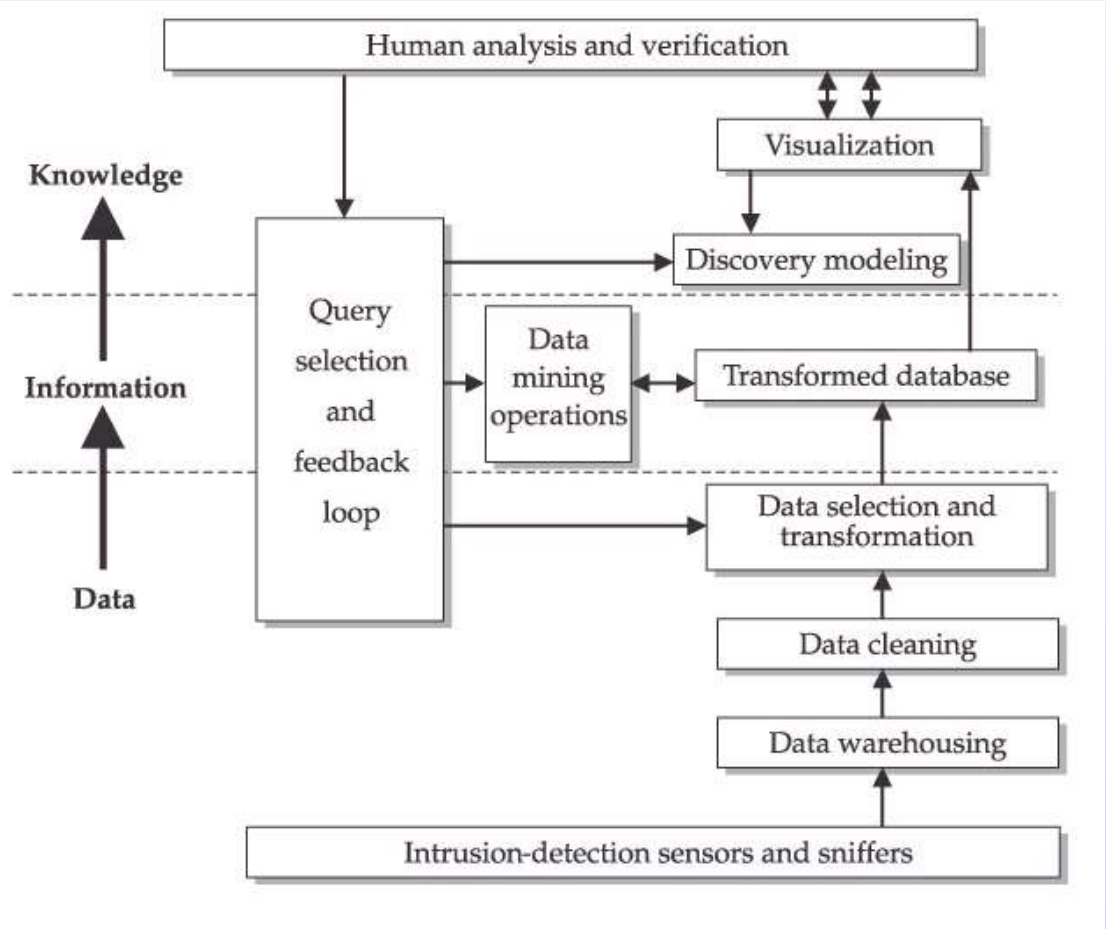
Gestión integrada de LOGS

- Objetivo: combinar los datos proporcionados por distintos tipos de sensores (NIDS, HIDS, ...)
- logIDS



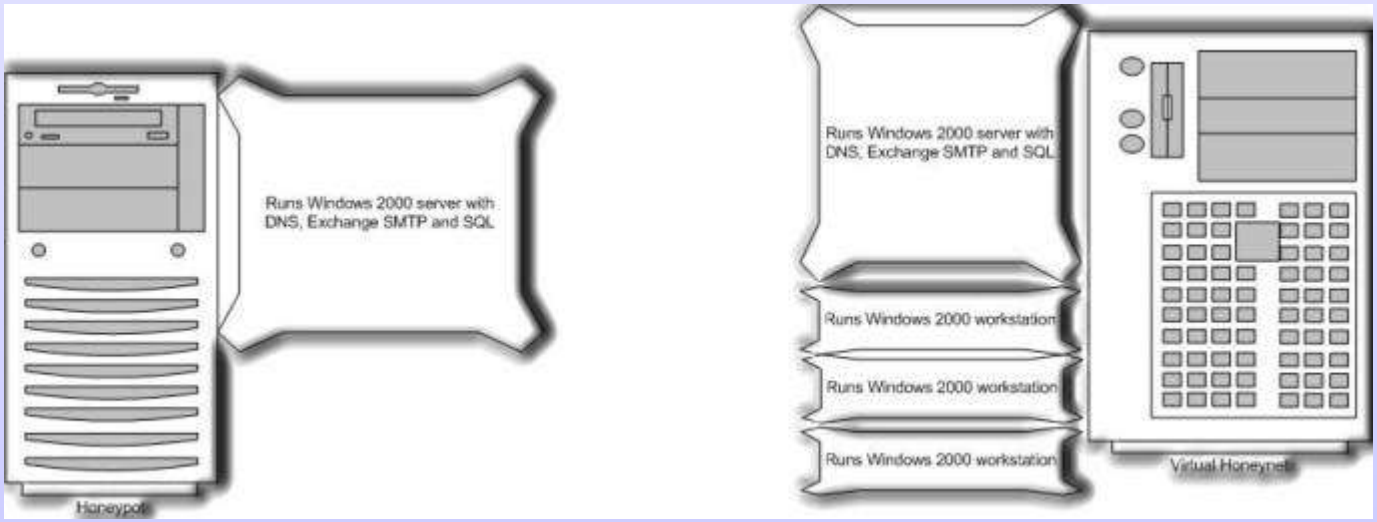
Correlación y fusión de Datos

- El problema principal de la integración de sensores reside en la gran cantidad de datos a procesar



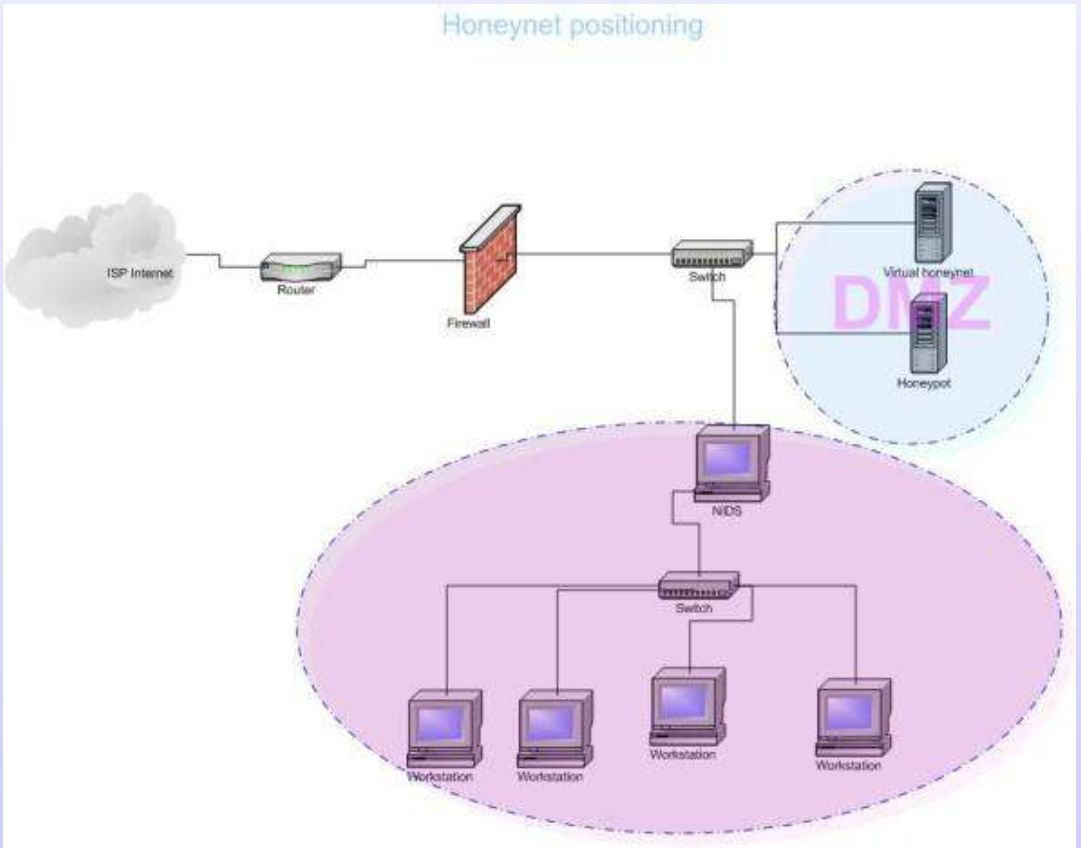
Honeypots y HoneyNets

- Permiten “focalizar” el interés del intruso en sistemas “aparentemente poco seguros”
- Permiten la detección rápida de intentos de intrusión (antes que lleguen a sistemas vitales)
- Pueden ser máquinas reales o virtuales (VMWare o VirtualPC)



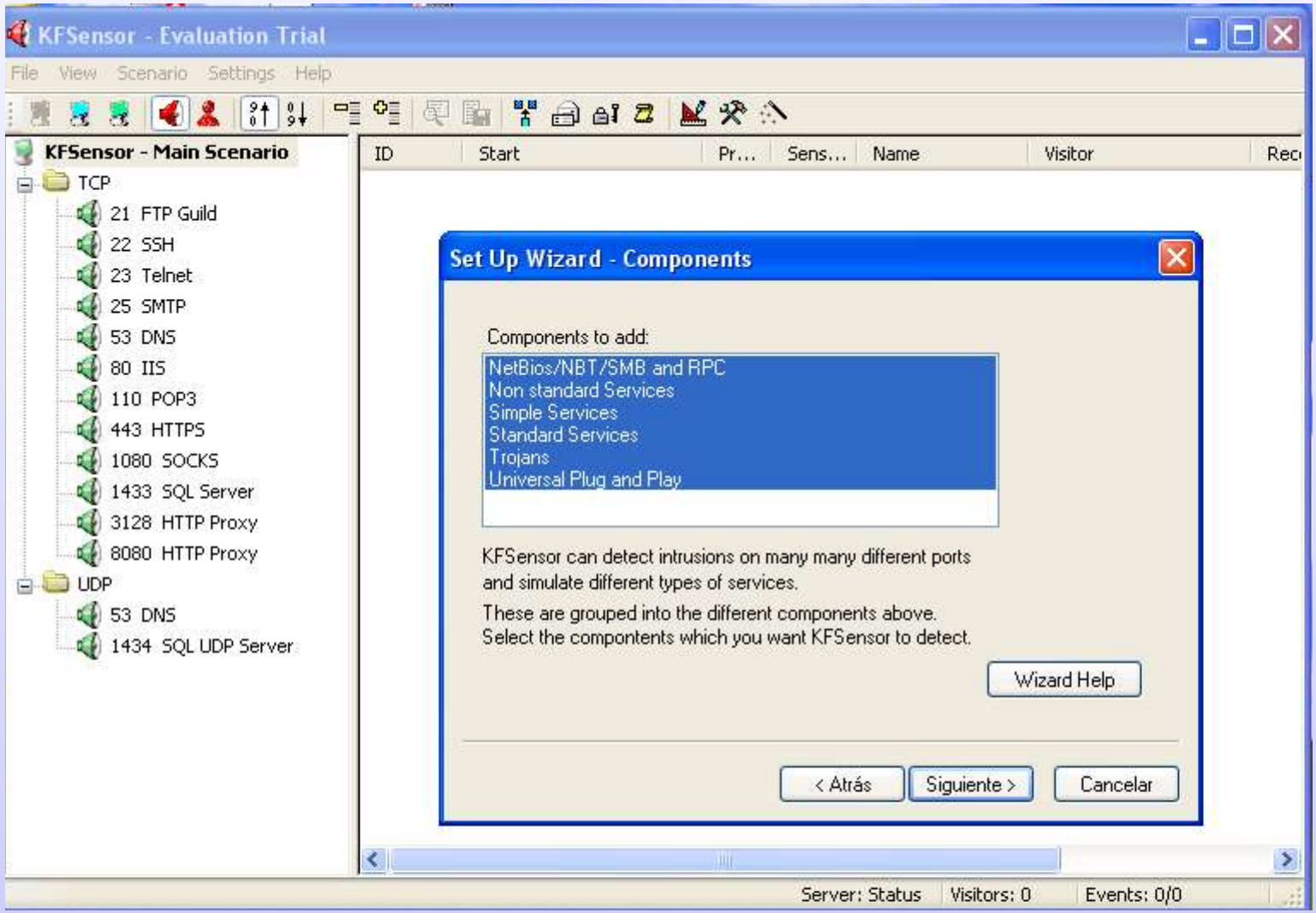
Ubicación del honeypot

- Los situaremos “cerca” de:
  - los sistemas a los que queremos proteger
  - en la puerta de entrada a nuestra red



Caso práctico Honeypot: KFsensor

http://www.keyfocus.net



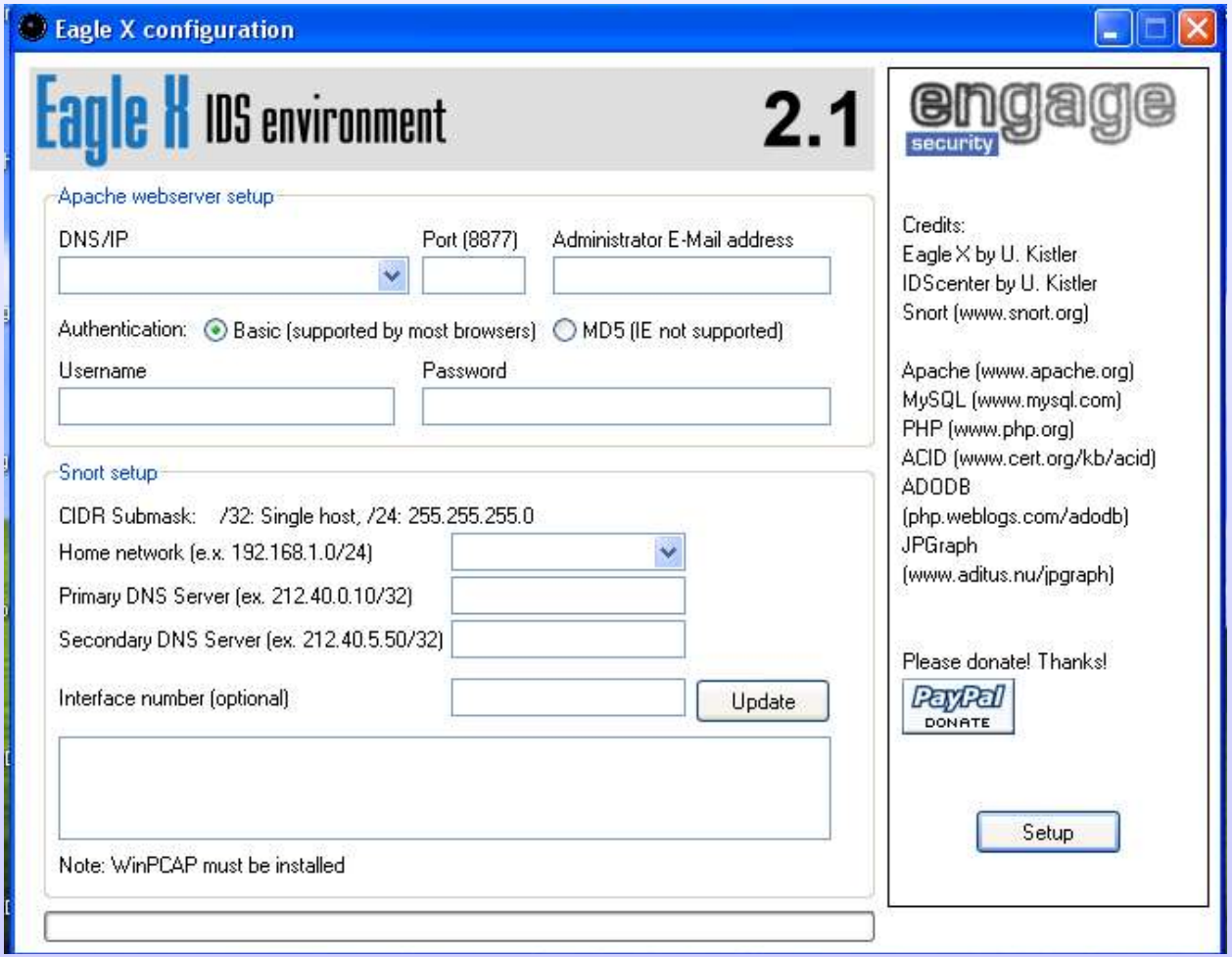
IDSs en Windows

Ejemplos prácticos ...

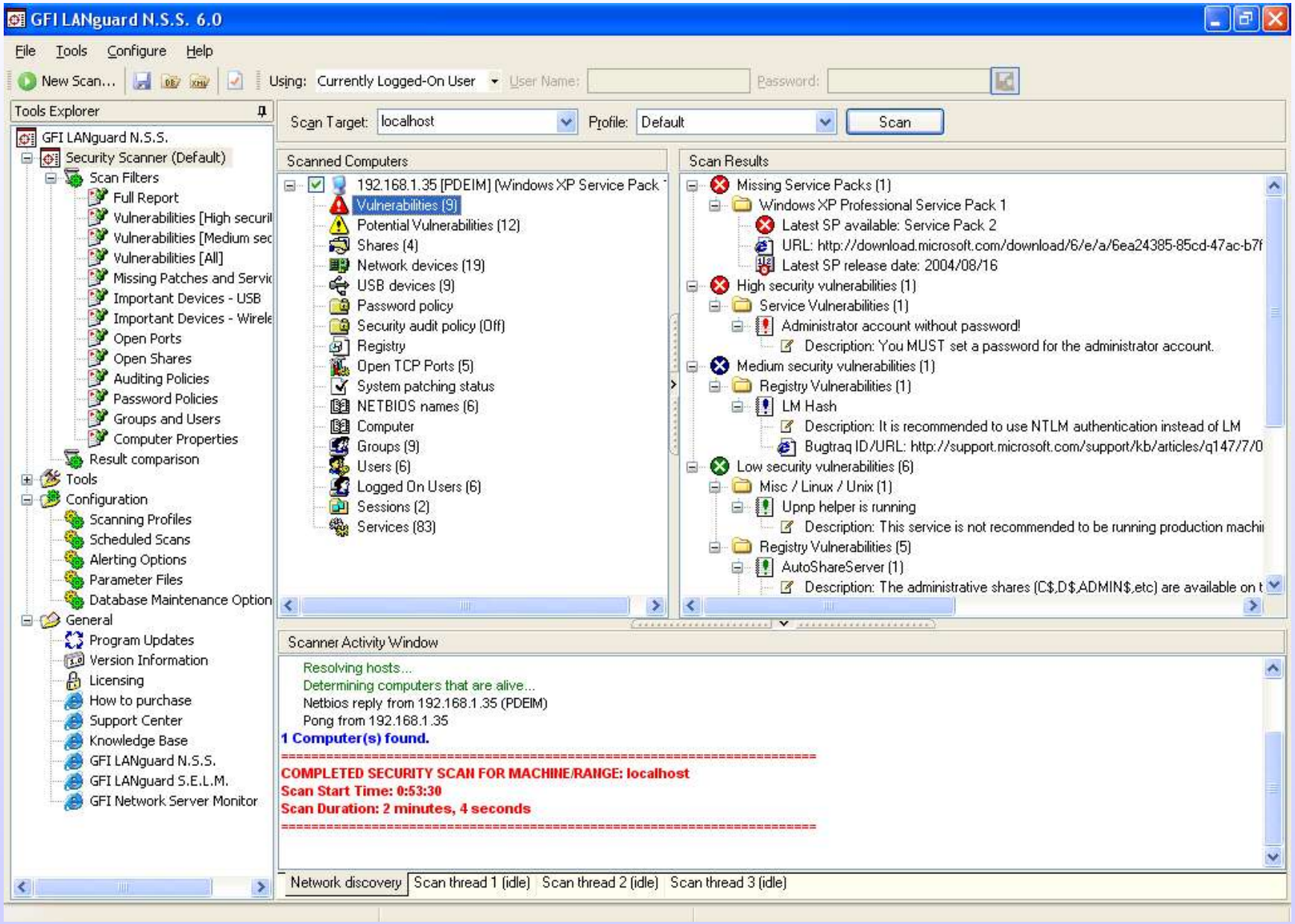
Paquetes “todo en uno...”

- EagleX

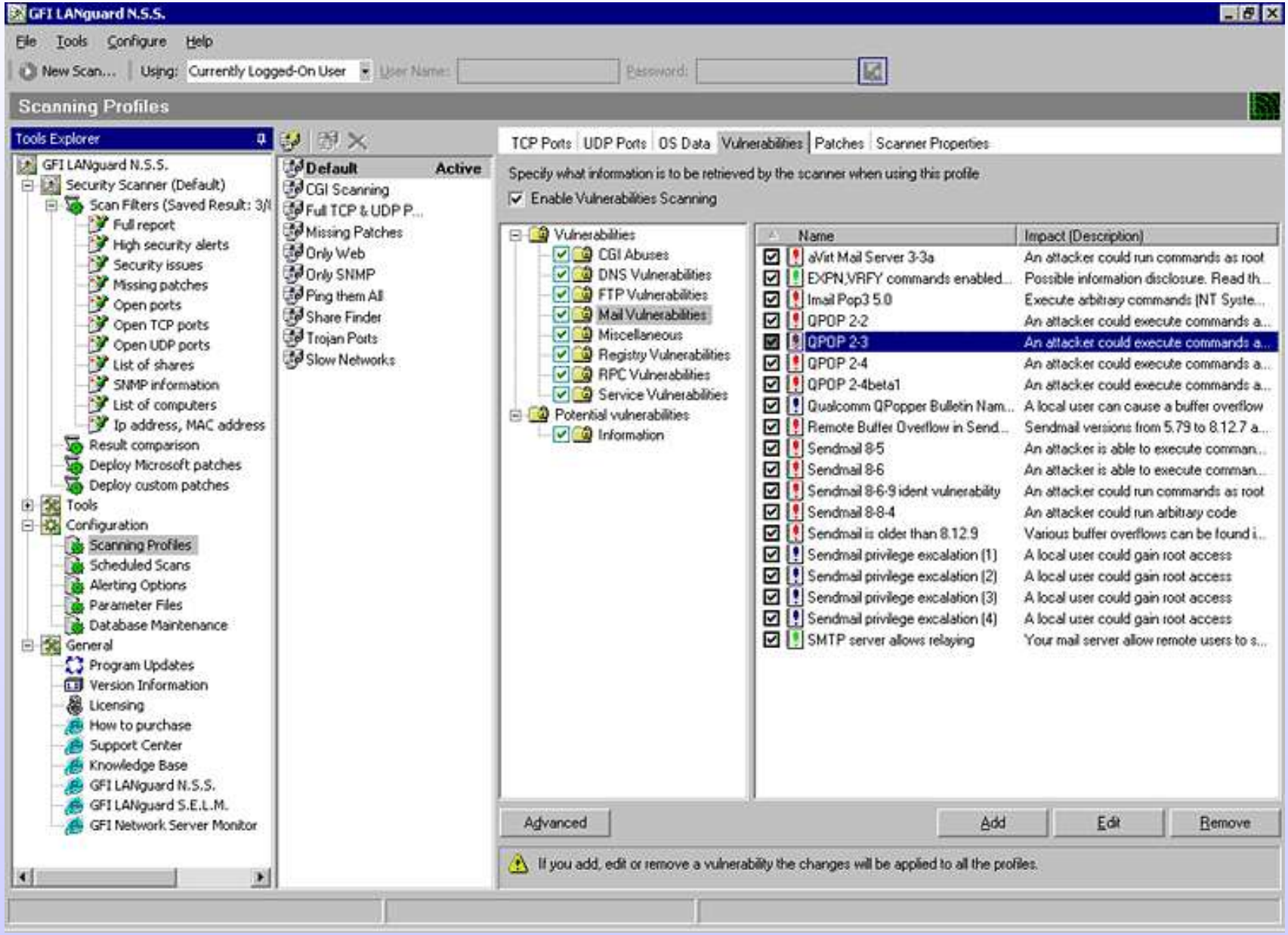
  http://www.engagesecurity.com/products/eaglex



Ejemplo práctico: LanGuard



Network Server Monitor



Ejemplos prácticos: Otros IDS para windows

- Intelligent IDS

  www.securityprofiling.com
- ThreatSentry

  www.privacyware.com

NFR sentivist

- http://www.nfr.com
- IDS , IPS
- Back Officer Friendly honeypot

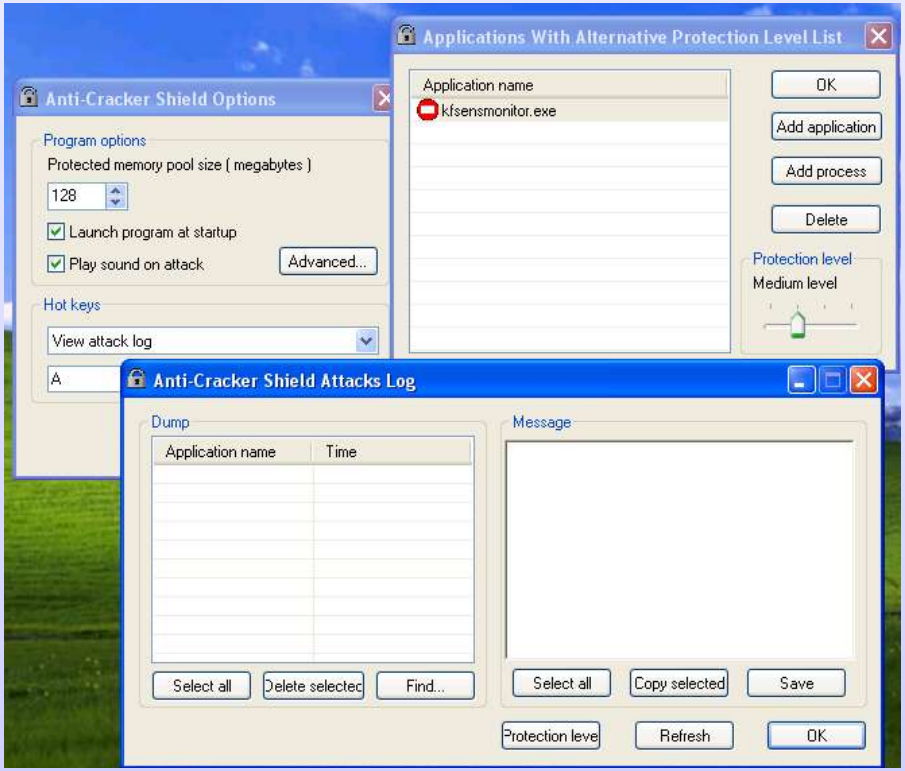
HIDS

- Anti-cracker shield

  http://www.softsphere.com

- securIT Intrusion Detection Toolkit

  http://iquebec.ifrance.com/securit



Firewalls personales

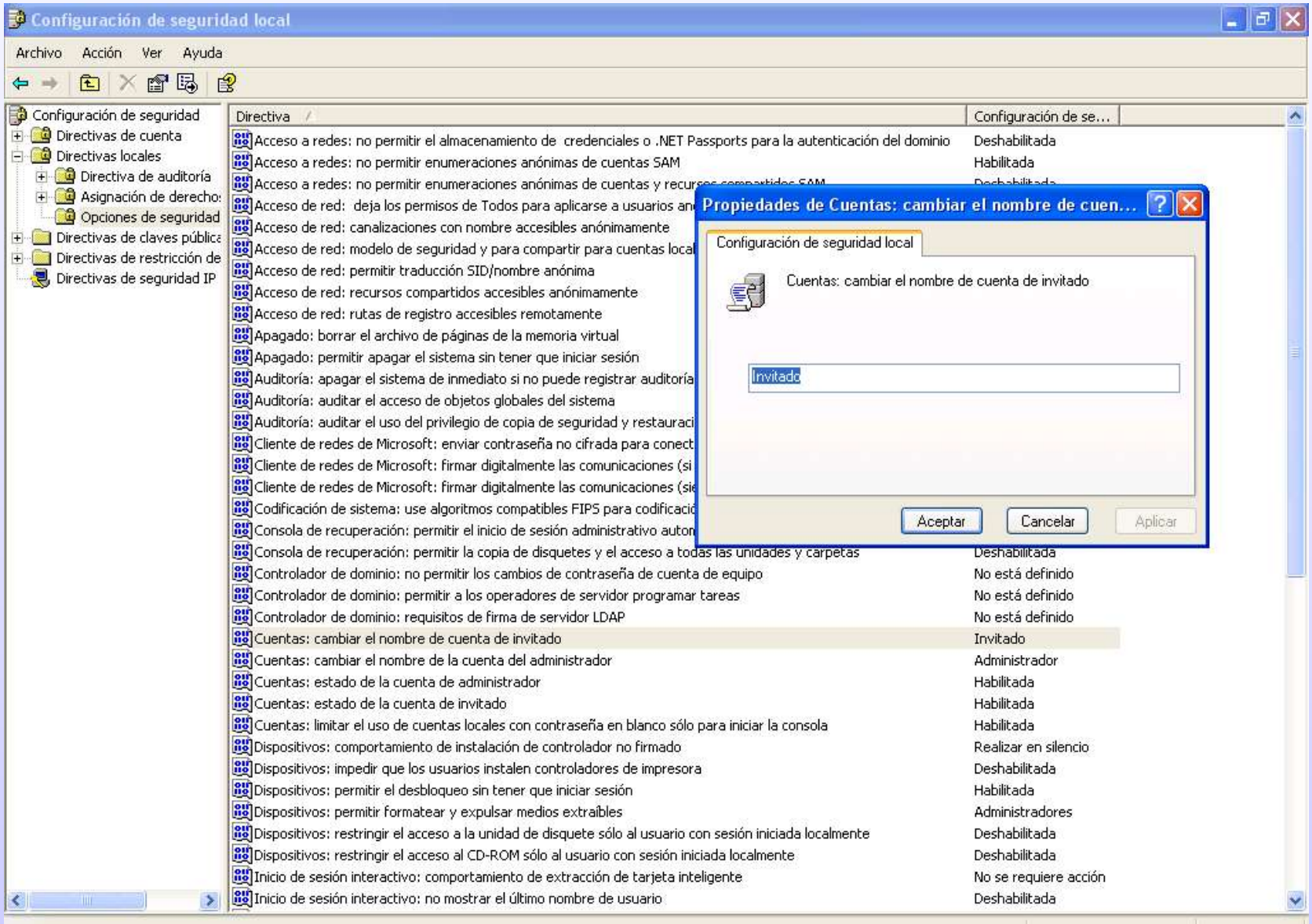
- Algunos incluyen capacidades de IDS
- Pueden registrar eventos en un sistema de log centralizado
- Por ejemplo:

  Kerio Personal Firewall

  ZoneAlarm

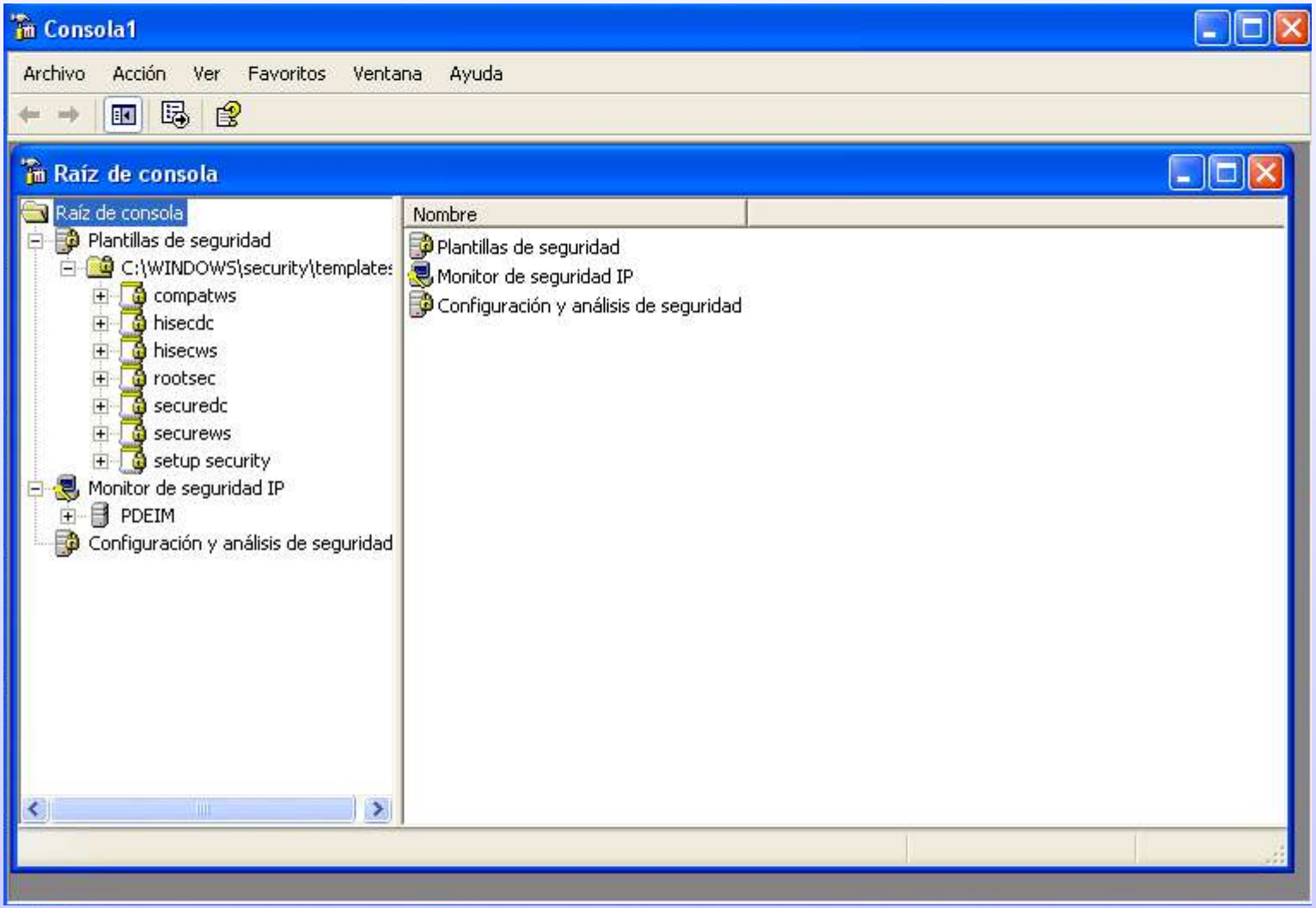
Herramientas de Windows

- Configuración de Seguridad Local



Consola de Gestión de Windows

- Permite añadir “plantillas” de seguridad



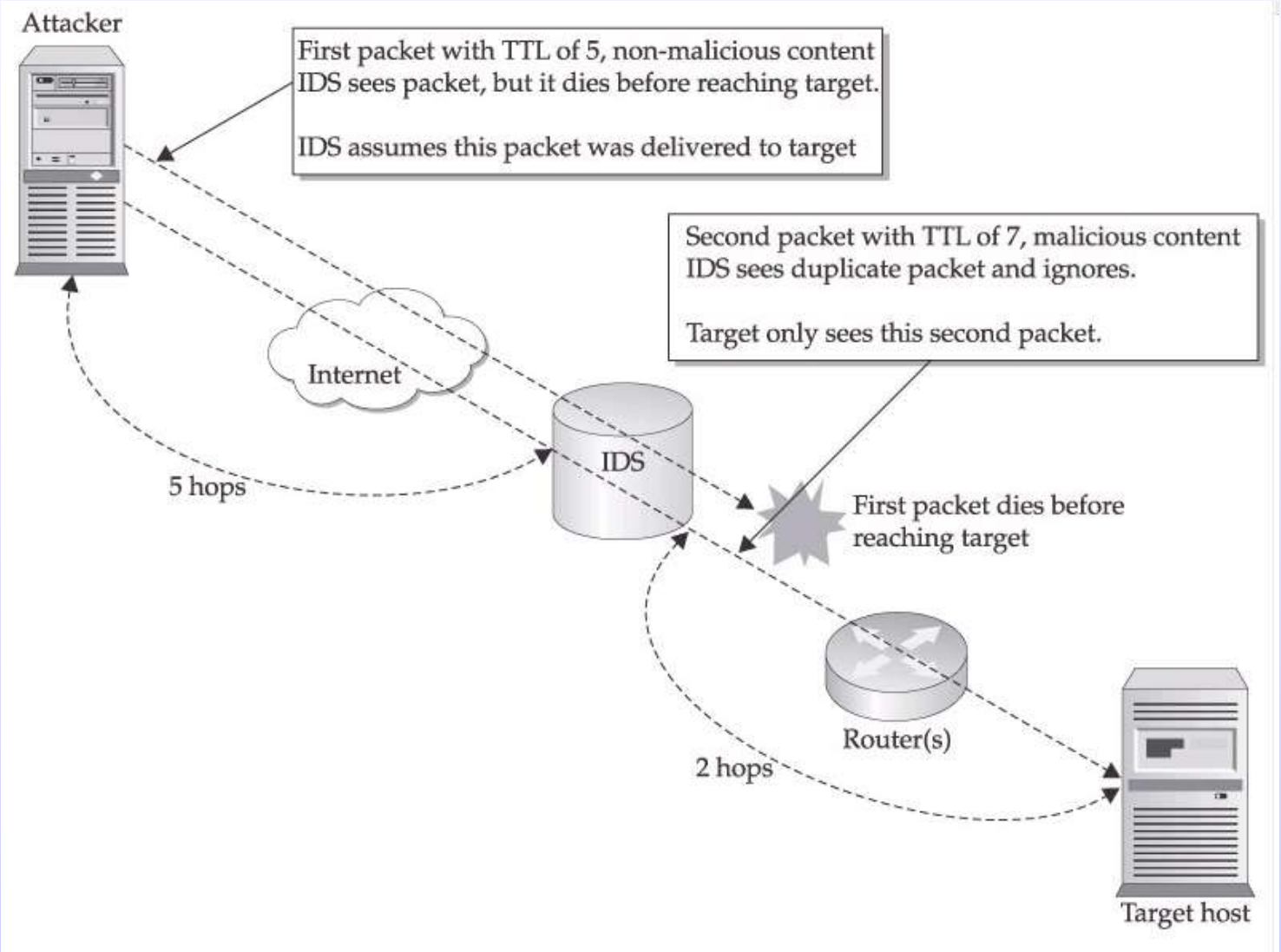
Nuevas tendencias en los IDS

Inconvenientes básicos del IDS

- Falsos positivos:
  - Sistemas de gestión de Red
  - Port scanners (nessus, nmap, ...)
  - Actividad del usuario (aplicaciones P2P, ...)
  - URLs largas (buffer overflow)
- Necesidad de ajuste del IDS a las características de nuestra organización

Como evadir al IDS ...

- Por ejemplo usando el ttl:



Técnicas de Evasión

- Evolucionan al mismo ritmo (o superior!!) que la tecnología de los IDS.
- Algunos ejemplos:

  nmap: ralentizar el escaneo de puertos, generación de gran cantidad de paquetes “falsos” para enmascarar la fuente del escaneo

  nikto: web scanner (http://www.cirt.net/code/nikto.shtml), permite evitar IDS con ficheros de reglas antiguos

  sslproxy: tráfico cifrado a través del IDS

  ...

Mecanismos de Detección

El IDS toma sus decisiones en base a:

- Detección de anomalías:
  - Análisis directo del tráfico (NIDS).
  - Análisis de procesos y parámetros del sistema (HIDS).
  - No precisa conocimiento previo
- Detección de patrones de ataque (firmas):
  - Precisa conocimiento “a priori” de las trazas de una intrusión.
- Estrategia combinada:
  - Mezcla de los anteriores

Detección de Anomalías

- El principio de detección se basa en:
  - ¿qué es normal en cada situación?
  - grados de anomalías
- ¿cómo distinguimos?
- Los sistemas basados en la detección de anomalías se clasifican en:
  - Sistemas de autoaprendizaje
  - Sistemas programados.

Sistemas de “autoaprendizaje”

Aprenden a partir de ejemplos de “comportamiento normal”

- **Generadores de reglas:** analizan en tráfico y generan dinámicamente reglas que describen su comportamiento.

- **Analizadores estadísticos:** Crean un perfil estadístico de diversos parámetros del sistema y usan una medida de distancia que permite cuantificar la desviación respecto al “tráfico normal”

IDS basados en sistemas inteligentes

- Sistemas basados en redes neuronales:

  Los descriptores del comportamiento “normal” del sistema se usan para “entrenar” una red neuronal

  Una vez completado el entrenamiento, el sistema es capaz de clasificar los nuevos patrones de tráfico

  No requieren “supervisión”

Inconvenientes principales:

  Dificultades en su diseño (arquitectura)

  Entrenamiento on-line (adaptabilidad, plasticidad)

Sistemas programados

- Requieren la presencia de un “profesor”
- El usuario debe determinar que situaciones son anómalas
- Se clasifican en:
  - Sistemas estadísticos
  - Sistemas de “Denegación por defecto”

Sistemas estadísticos

- Construyen un perfil que caracteriza el comportamiento normal del sistema en función de sus parámetros de operación
- Pueden ser:

basados en estadísticas simples: un componente de análisis usa medidas estadísticas simples para generar decisiones en el sistema de detección.

basados en reglas simples: el usuario proporciona un conjunto de reglas que se aplican a las estadísticas recopiladas.

basados en tolerancia: Una vez el sistema ha recopilado información suficiente el usuario puede definir diversos niveles de tolerancia que provocaran la generación de alarmas.

Denegación por defecto

- Se explicitan la circunstancias bajo las cuales se considera que el sistema opera de forma normal (segura). Cualquier desviación de esta descripción es considerada como una intrusión
- Se basa en la definición de políticas de seguridad.
- Modelado mediante máquinas de estado
  - Las políticas se codifican como un conjunto de estados y transiciones
  - Se usan redes de Petri

Detección de "firmas"

- Toma decisiones en base a un modelo de intrusión y de sus trazas características.
- Detectan la intrusión sin necesidad de conocer el comportamiento "normal" del sistema.
- Buscan patrones "sospechosos".
- Podemos encontrar:
  - Sistemas expertos
  - Sistemas basados en el reconocimiento de patrones en cadenas de caracteres
  - Sistemas basados en reglas

Sistemas Combinados

- Son un híbrido de las dos técnicas anteriores.
- Las decisiones se toman tanto en función del comportamiento normal del sistema, como del comportamiento del intruso (tipo de intrusión).
- Generalmente, son sistemas capaces de aprender (adaptarse) a los comportamientos normales e intrusivos.

Problema: Tipos de intrusiones

- Conocidas: Podemos caracterizarlas mediante patrones “estáticos”. Fácilmente detectadas por los sistemas basados en reconocimiento de firmas.
- Generalizables: pequeñas variaciones de intrusiones conocidas. Detectadas por sistemas combinados con capacidad de aprendizaje
- **Desconocidas**: Algunas son reconocidas por los IDS basados en detección de anomalías.

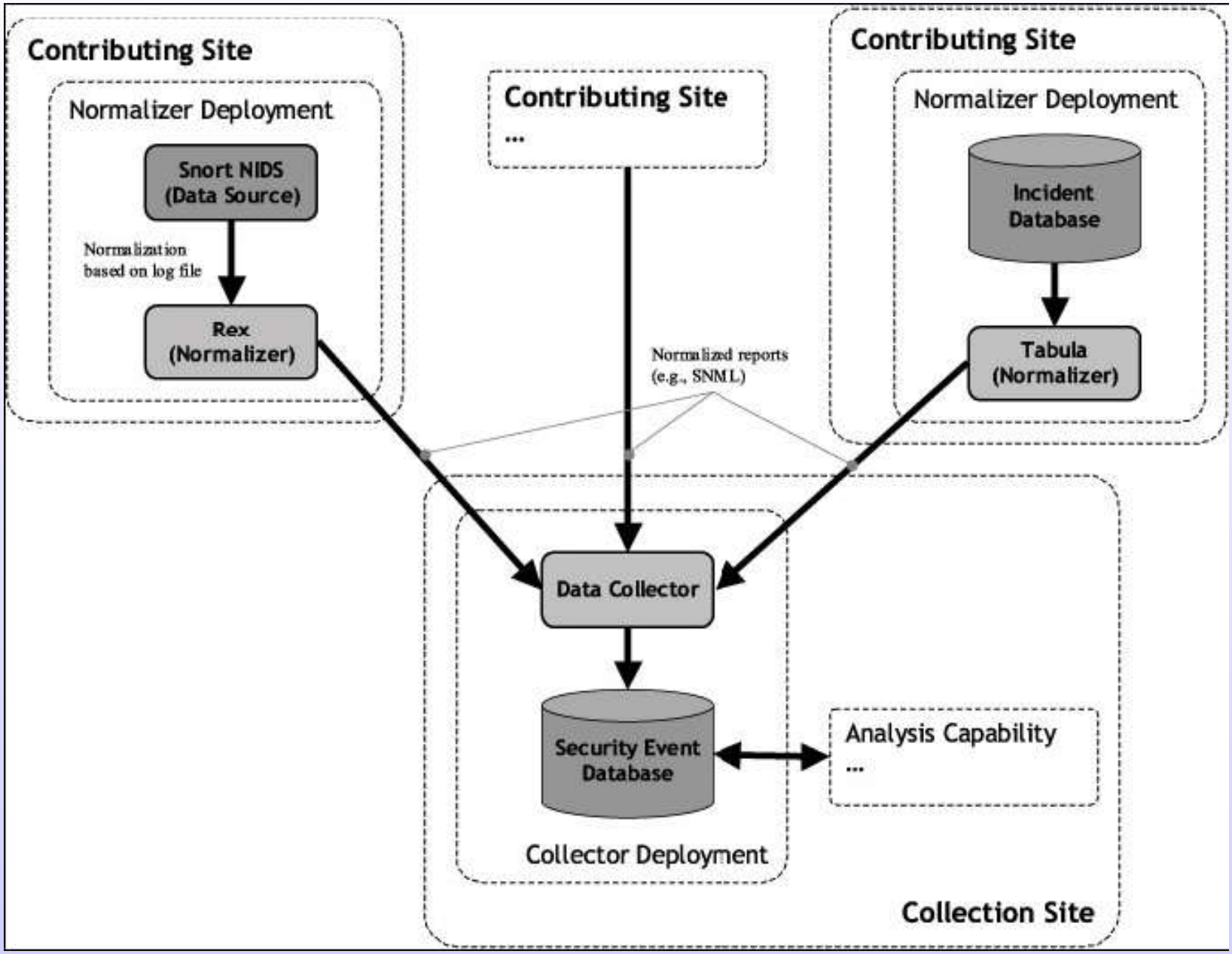
Tendencias actuales

- La investigación actual en el campo de los IDS se focaliza en los siguientes aspectos:
  - IDS con respuesta “Activa”.
  - IDS Distribuidos a gran escala (airCERT).
  - Seguridad del IDS. (IDS resistentes a ataques)
  - Comunicaciones cifradas host-red.
  - Eficiencia (coste de la captura y detección)

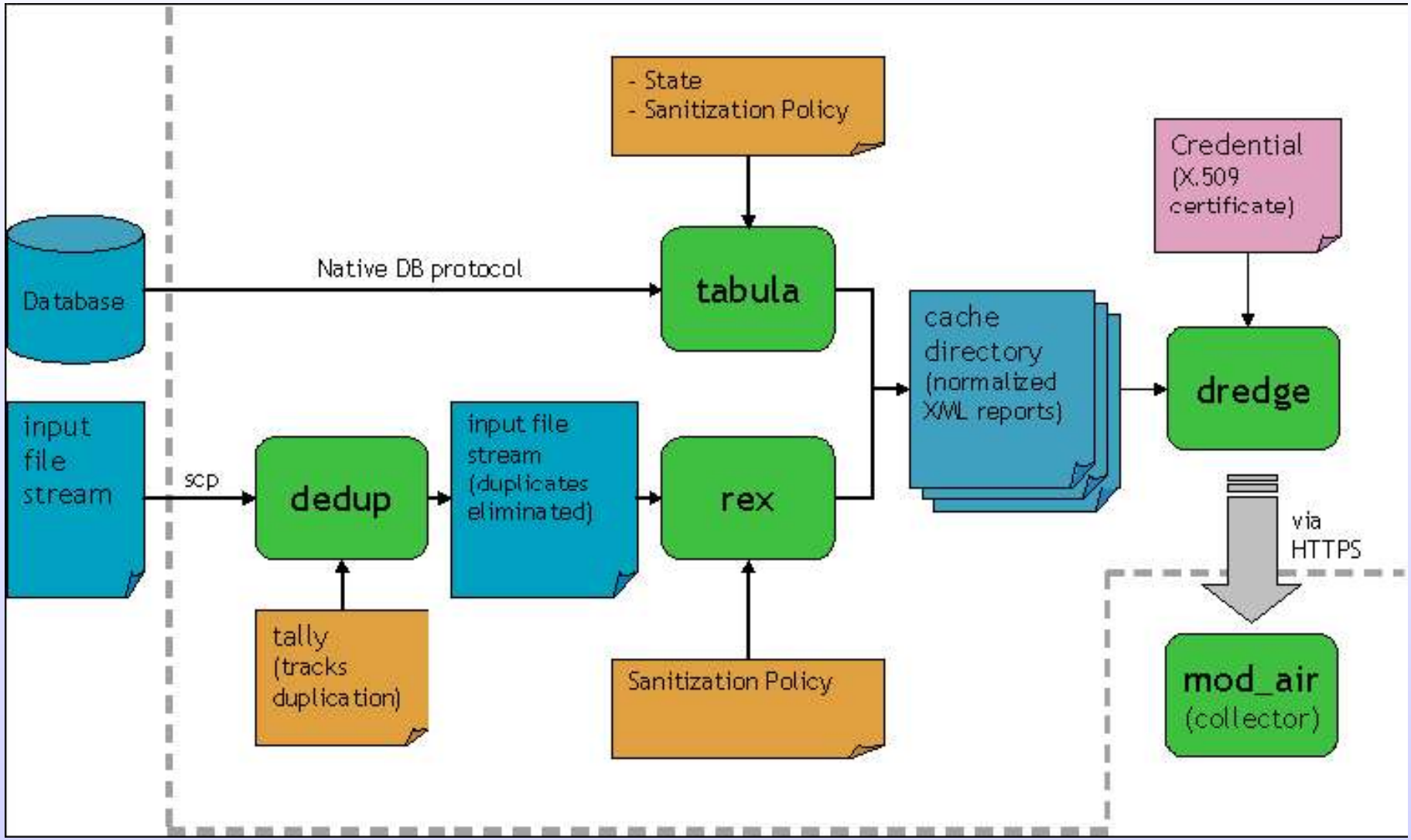
airCERT

- Intercambio de información en IDS distribuidos a través de diversos dominios administrativos
- Proporciona una visión a gran escala del incidente
- Permite reconocer tendencias de intrusión que de otra manera pasarían desapercibidas
- Permite compartir datos y conocimiento sobre mecanismos de intrusión
- http://www.cert.org/kb/aircert/
- http://aircert.sourceforge.net

IDS distribuidos



Normalización de los datos



Distribución de datos