Sistemas de Detección y Prevención de Intrusos – Estado del Arte

Charles Ware
cware@uy.ibm.com
Agosto 2011

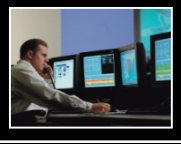
Agenda

- Concientización y estate del arte
- Historia
- Detección de Intrusos
- Prevención de Intrusos
- IDPS Vs Firewall
- Degustación de opciones
- Mejores Practicas de implementación
- Resumen
- Preguntas

Concientización y Estado del Arte

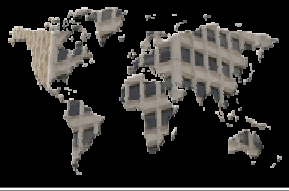
Aumento de la amenaza interna

Usuarios privilegiados causan un 87% de los incidentes de seguridad
3 de las10 principales amenazas a la seguridad de la empresa están relacionadas con información privilegiada



Perdida de la visión total de la empresa

Demasiados datos, formatos, dispositivos, posibles agujeros no visibles por la magnitud



Amenazas Externas

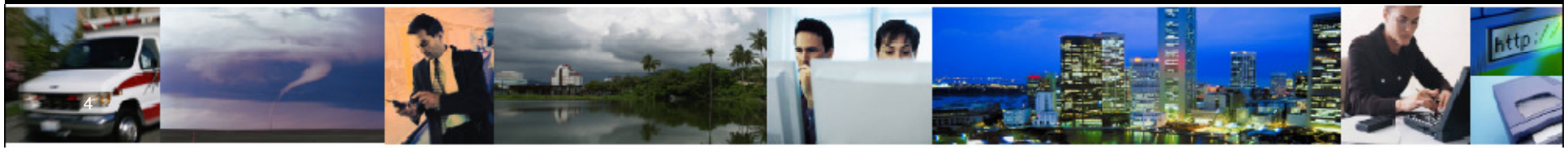
70% de todas las vulnerabilidades conocidas no poseen un parche

Creciente número de regulaciones

El incumplimiento da lugar a sanciones económicas y la pérdida de reputación corporativa

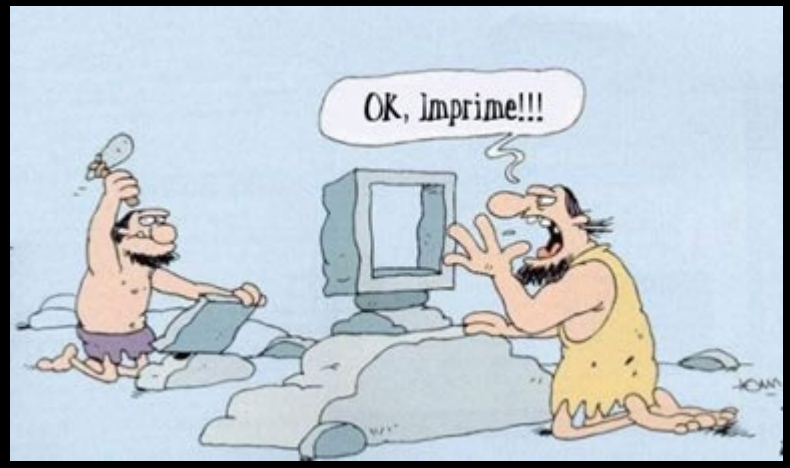
Falta de un punto central de administración de seguridad

Difícil control y administración de distintos tipos de dispositivos de seguridad



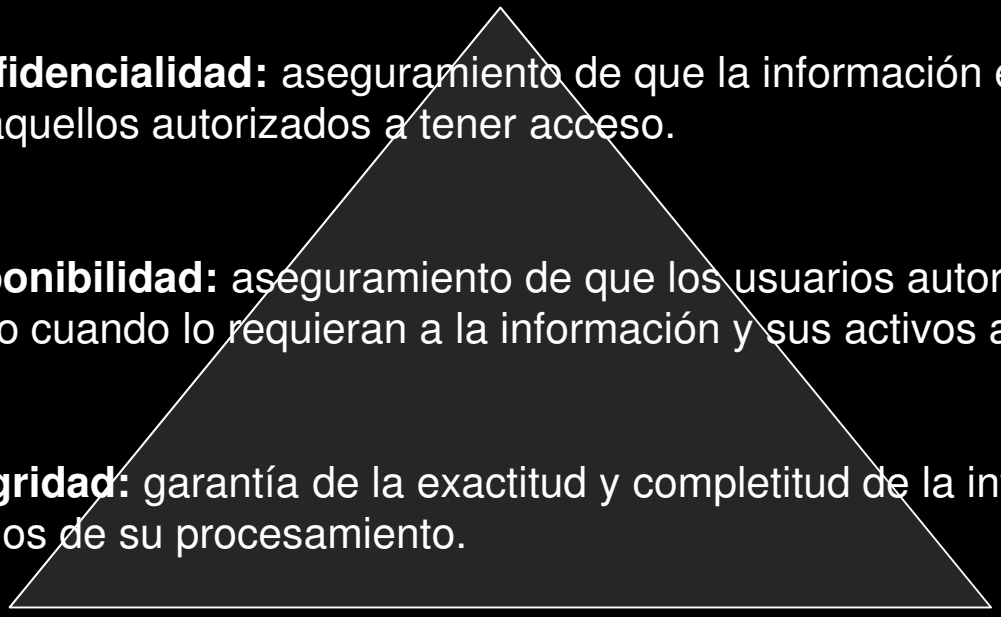
Historia

- 1970 – Reporte de dos volúmenes a la fuerza aérea de los Estados Unidos por J. P. Anderson
- 1980 – Teoría sobre los Sistemas de Detección de Intrusos por J. P. Anderson
- 1987 – Descripción de los Sistemas de Detección de Intrusos en tiempo real por Denning
- 1988 – Desarrollo de IDES por Havitz y Valdez
- 1990 – En la universidad de California el primer IDS llamado NSM (Network Security Monitor



Seguridad de la información

- La Seguridad de la Información se define como la preservación de la confidencialidad, integridad y disponibilidad.



• **Confidencialidad:** aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

• **Disponibilidad:** aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

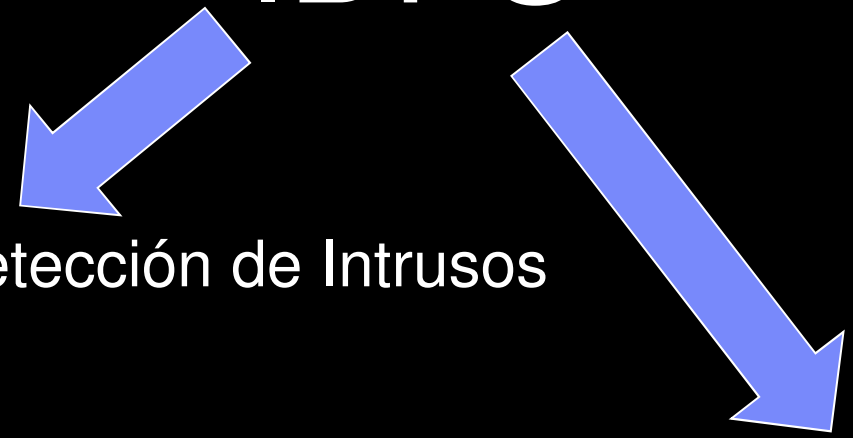
• **Integridad:** garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Sistema de Detección y Prevención de Intrusos - Definiciones

- Intrusión:
  - Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso (Anderson)

- Sistema de Detección y Prevención de Intrusiones:
  - Elemento que detecta, identifica y responde a actividades no autorizadas o anormales (Denning)

IDPS



Sistemas de Detección de Intrusos

Sistemas de Prevención de Intrusos

Sistemas de Detección de Intrusos

- **IDS es un sistema para detectar el uso indebido** de los recursos de red o el ordenador
- Tres funciones básicas:
  - **Monitorear**
  - **Detectar**
  - **Responder ante eventos** sospechosos que puedan entrar o salir de la compañía
- **Componente critico** en cualquier infraestructura de seguridad
- Los IDS monitorean tanto la red como los equipos en varios puntos proporcionando una visibilidad en la postura de seguridad

Sistemas de Prevención de Intrusos

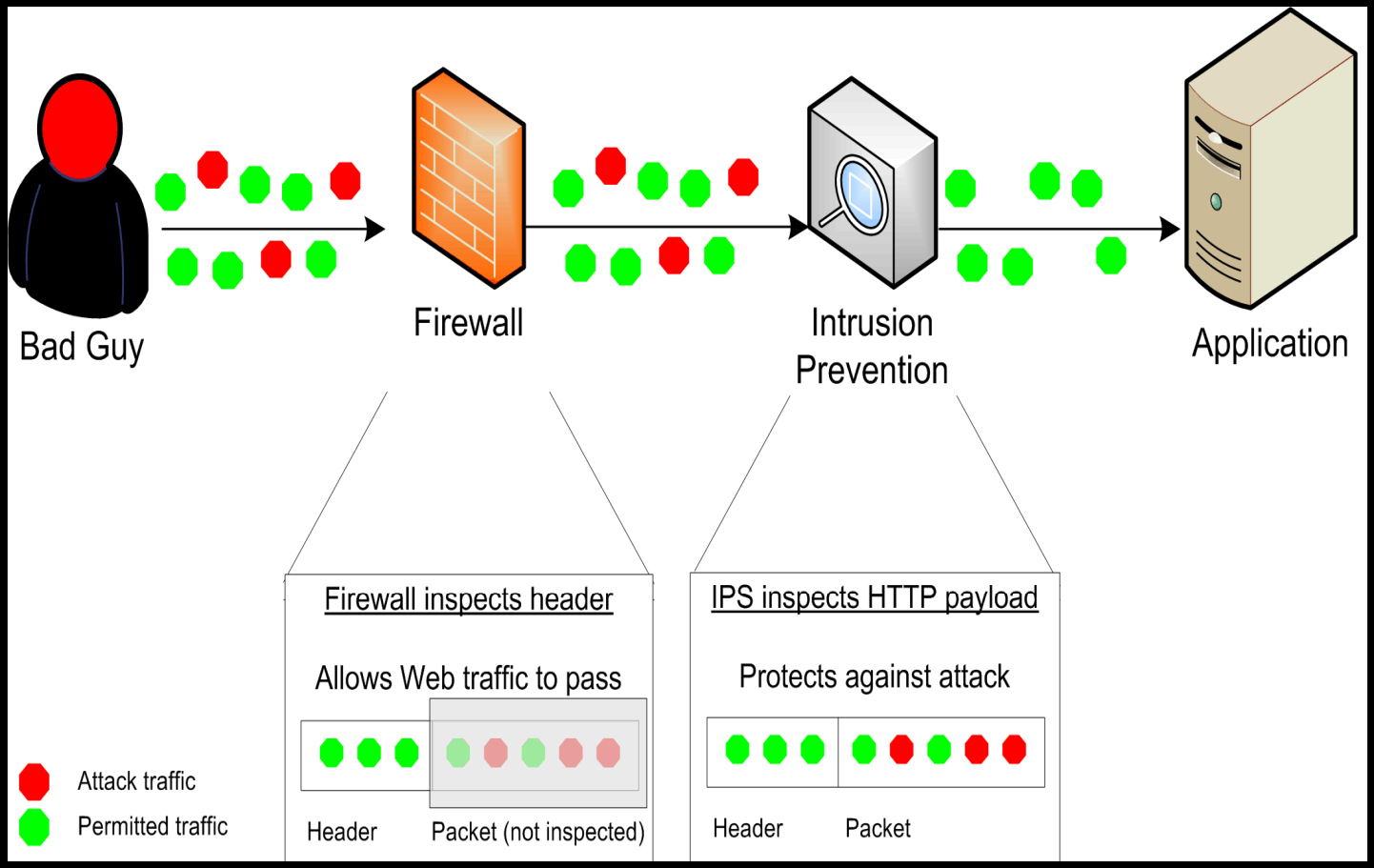
- IPS adopta **un enfoque preventivo** para la seguridad que se utiliza para identificar las posibles amenazas y responder a ellas rápidamente.
- Un IPS realiza un monitoreo y análisis mas complejo y eficaz, tales como ver y **responder** tanto a patrones de trafico como paquetes individuales.
- Monitorea el trafico e **interviene activamente** en caso de ver paquetes malignos. Examinado robusto de sesiones sospechosas o tomando acciones para una respuesta inmediata ante un posible ataque.
- Resumiendo un IPS:

- Detiene ataques en si mismo
- Cambios en el entorno de seguridad
- Cambios en el contenido del ataque

IDPS Vs Firewall

- Los firewalls están atento a los intrusos pero no a los ataques internos en la red
- Los IDPS ven ataques en los propios firewalls gracias a la detección basada en firmas las cuales son pasadas por altos en dichos equipos.
- Los IDPS investigan el contenido y los archivos de registros de Firewalls, Routers, etc.
- El firewall busca intrusos en la red a fin de que un ataque no suceda.
- El IDPS evalúa intrusiones sospechosas que han tenido lugar y genera un alerta de ello
- Estas herramientas son creadas para utilizarse en conjunto y no para sustituir una por otra

IDPS Vs Firewall – Claro ejemplo



Degustación de Opciones – Como funcionan estos Sistemas

Separemos las modalidades en que estos equipos o programas pueden detectar a los “malos”.

- **Detección basado en firmas**, las firmas detectan paquetes maliciosos en base a datos que no deberían estar presentes en los mismos. Las mismas deberían ser actualizadas para tener cada día menos falsos positivos.
- **Detección basado en anomalías**, mediante procesos que comparan que actividades son normales y cuales no para evitarlas. La ventaja fundamental es detectar infecciones nuevas por causa de anomalías tanto en la red, host o aplicaciones. Para este tenemos:
  - Perfiles dinámicos
  - Perfiles estáticos
  - Perfiles definidos
- **Análisis de estado de protocolos**, con un desarrollo en perfiles universales, verifican como determinados protocolos pueden ser usados o no.

Degustación de Opciones – Cuales son los diferentes tipos de equipos o programas que tenemos para estas soluciones?

Separemos en cuatro grandes grupos y hablemos de ellos:

- NIDPS
- HIDPS
- WIDPS
- IDPS en Ambientes Virtuales

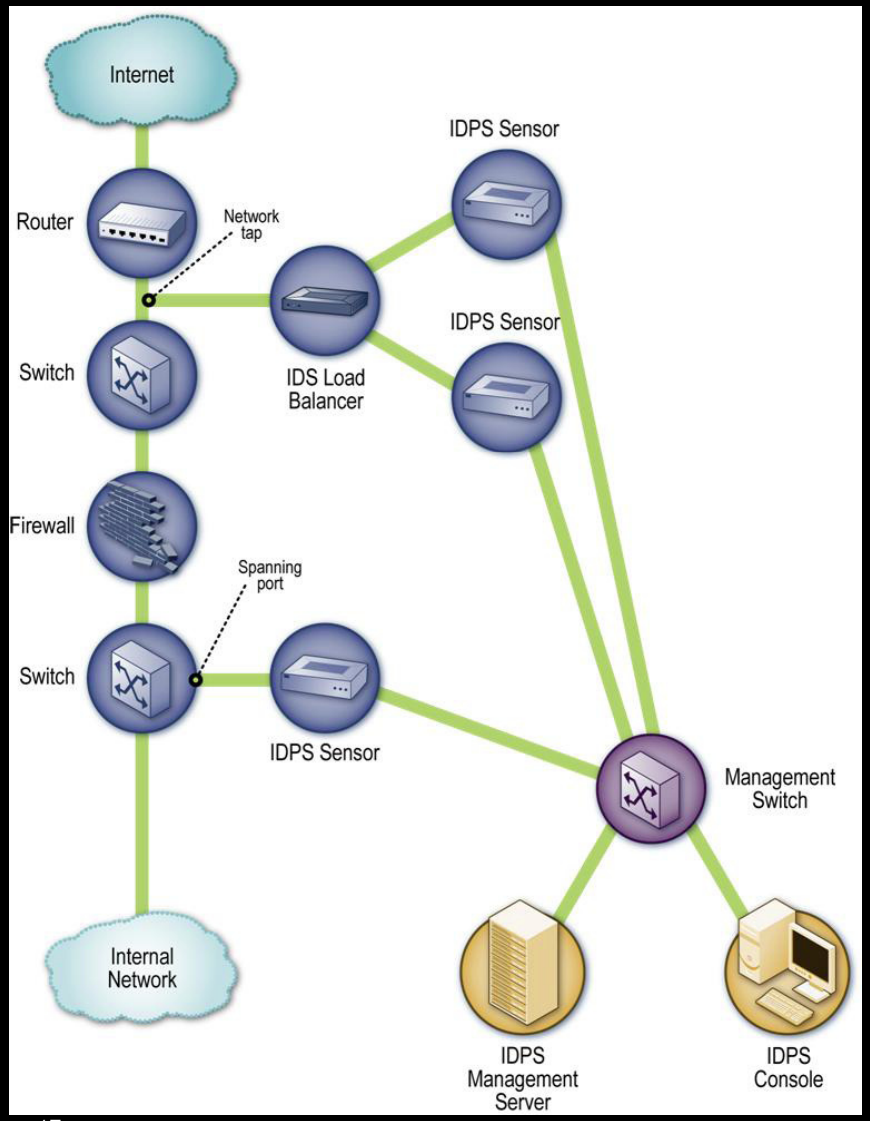
Network IDPS

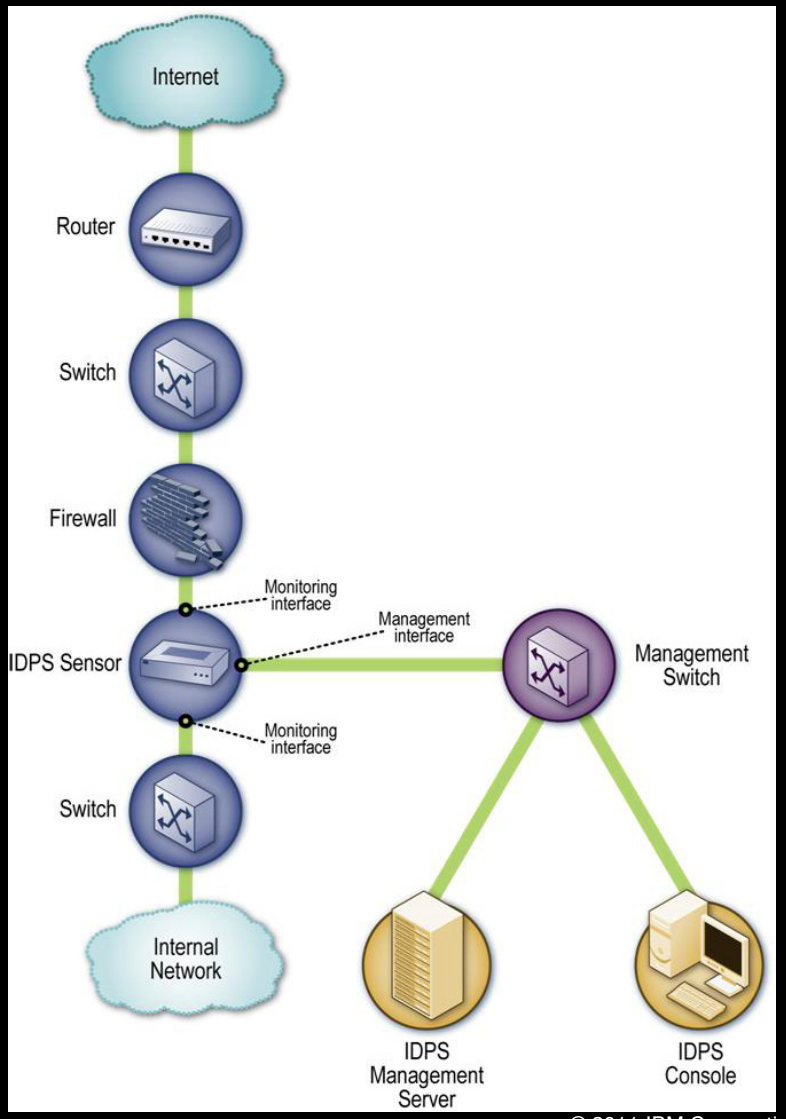
NIDPS – Network Intrusion Detection and Prevention System

- Los **NIDPS monitorean trafico** particular en los segmentos o equipos de **red**, y analizan protocolos de red, aplicación y transporte en búsqueda de actividades sospechosas.
- Se venden como Appliance o Software.
- Capacidad de recolectar información.
- Modos en los que se pueden instalar:

- **En línea**
- **Pasivo** en tres modalidades:
  - Spanning port
  - Network Tap
  - IDS Load Balancer

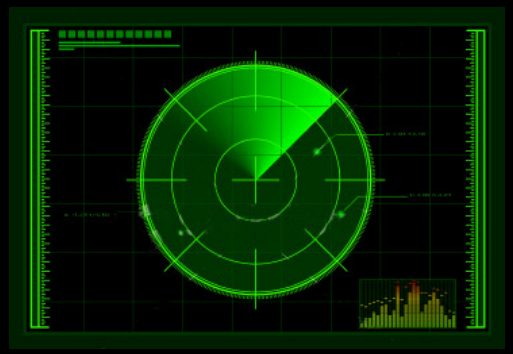
NIDPS – Esquema practico





Mejores practicas de Implementación para los NIDPS

- Tener una red separada para el trafico entre los NIDPS y el servidor de administración



- La ubicación de los sensores debe ser en las fronteras entre redes.

- Para el caso de los sensores en línea es recomendado ponerlo detrás de un firewall y lo mas cerca posible de la parte mas segura de la red, de este modo el procesamiento será mucho menor.

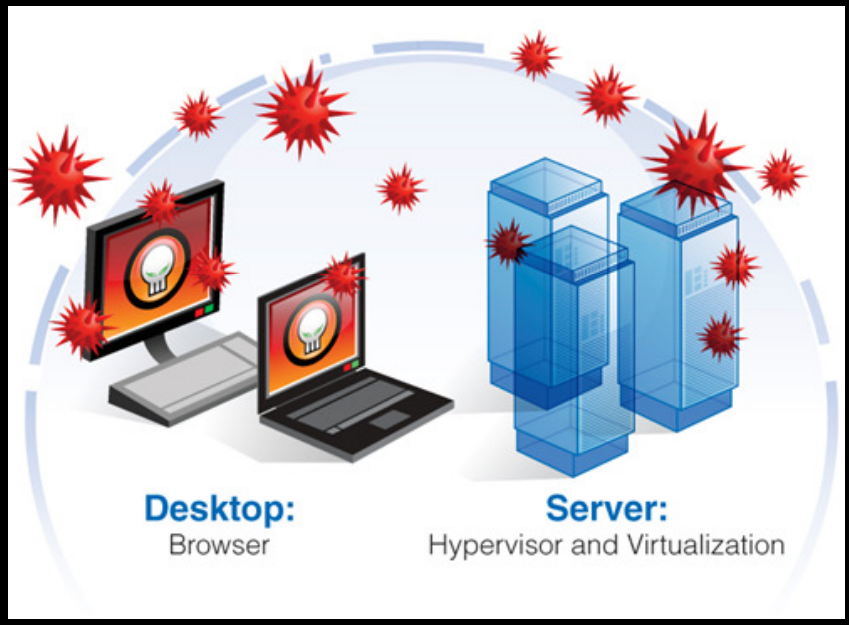
- Los dispositivos en línea también pueden estar cerca de las fronteras para disminuir el trafico interno por ejemplo de los Firewalls.

Host IDPS

HIDPS – Sistemas de Detección y Prevención de Intrusos en equipos finales

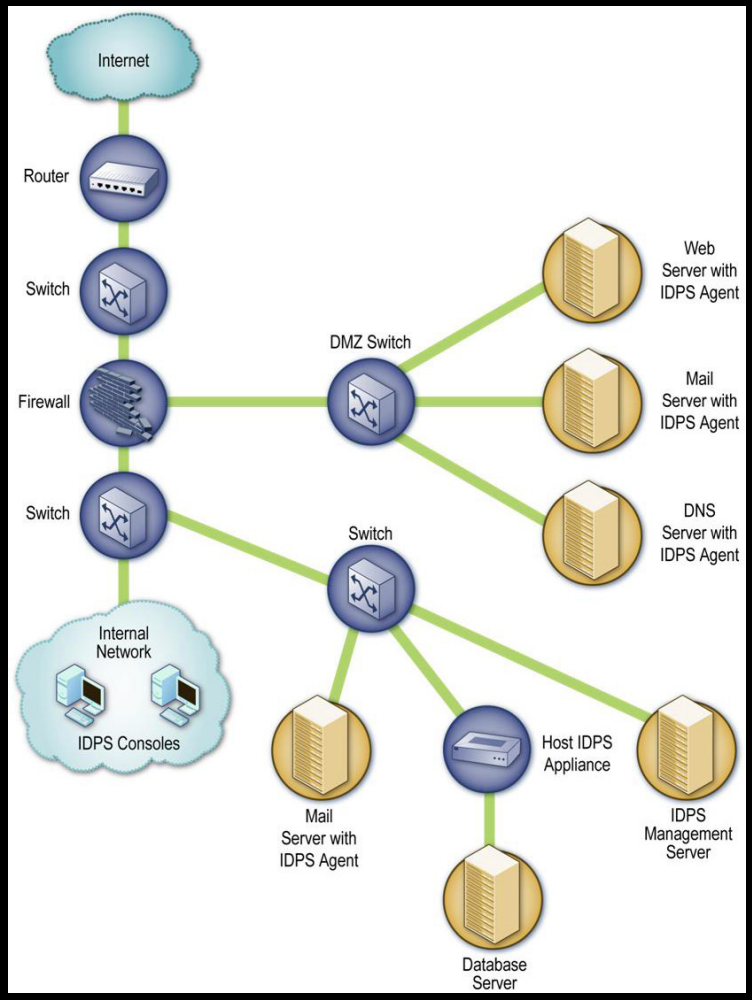
En el caso de los HIDPS

- Los host combaten intrusiones que la red ve una vez que el equipo ya se encuentra en peligro y quiere salir a la misma
- Un sistema de detección y prevención de intrusos complementario a el sistema de antivirus hoy en día es necesario para combatir la realidad de la inseguridad informática
- Los antivirus no son capaces de detectar todas las amenazas que hoy día acechan a los equipos de los usuarios finales
- Los portables son los principales "proveedores" de intrusos en la empresa.



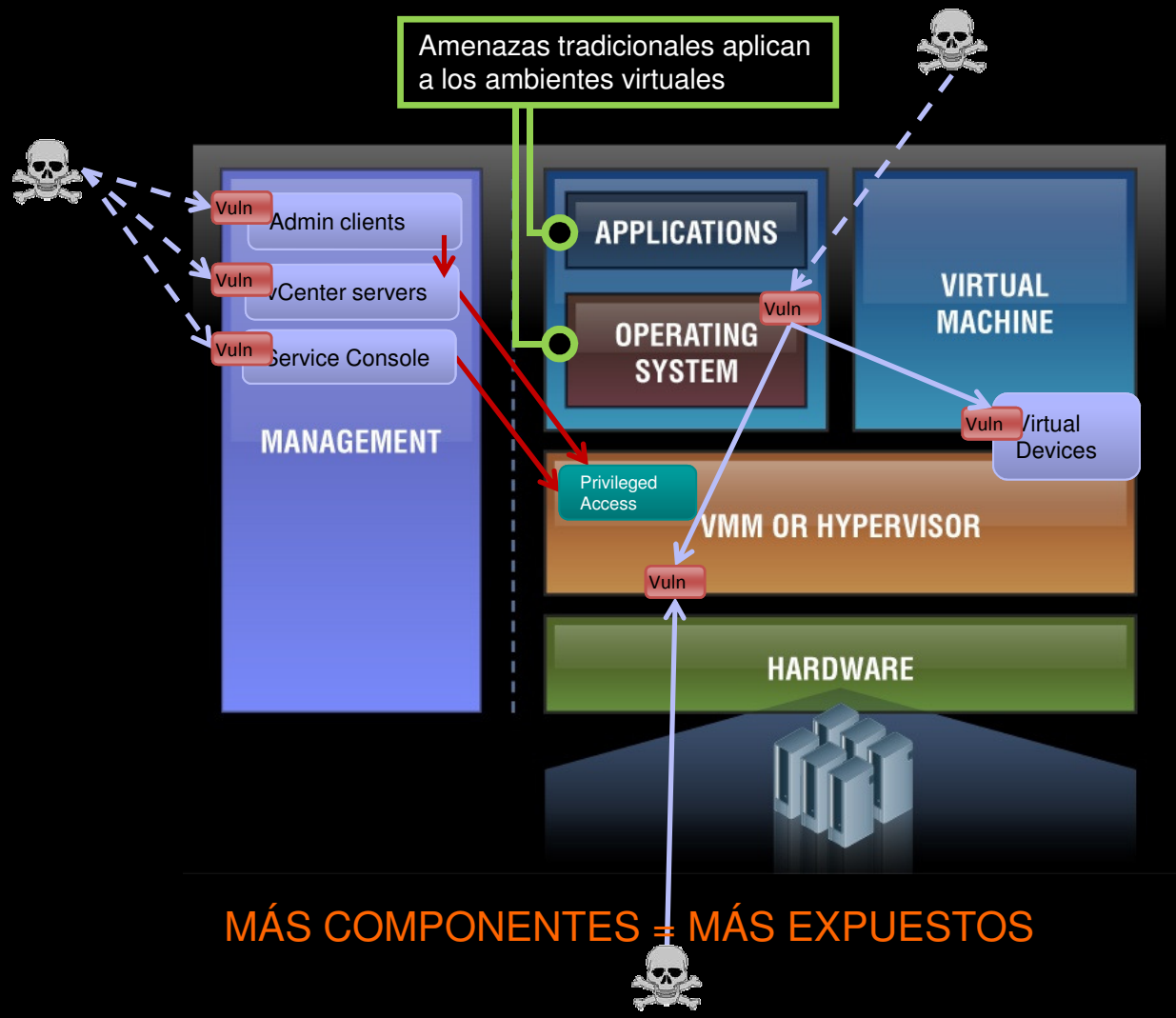
HIDPS – Sistemas de Detección y Prevención de Intrusos en equipos finales

- Los podemos ver de tres formas diferentes: en servidores, equipos de usuarios, o aplicaciones especificas
- El host IDPS monitorea, trafico inalámbrico y de red del equipo, logs del sistema, procesos corriendo, accesos a los archivos, cambios de configuración tanto de sistemas como aplicaciones, chequeo de integridad.
- El IDPS nos ayuda a prevenir virus, spam, spyware, worms, trojan horse, keyloggers, bots, buffer overflows, rootkits, etc.
- IDPS sobre Host ve el trafico encriptado que no puede ver en NIDPS.



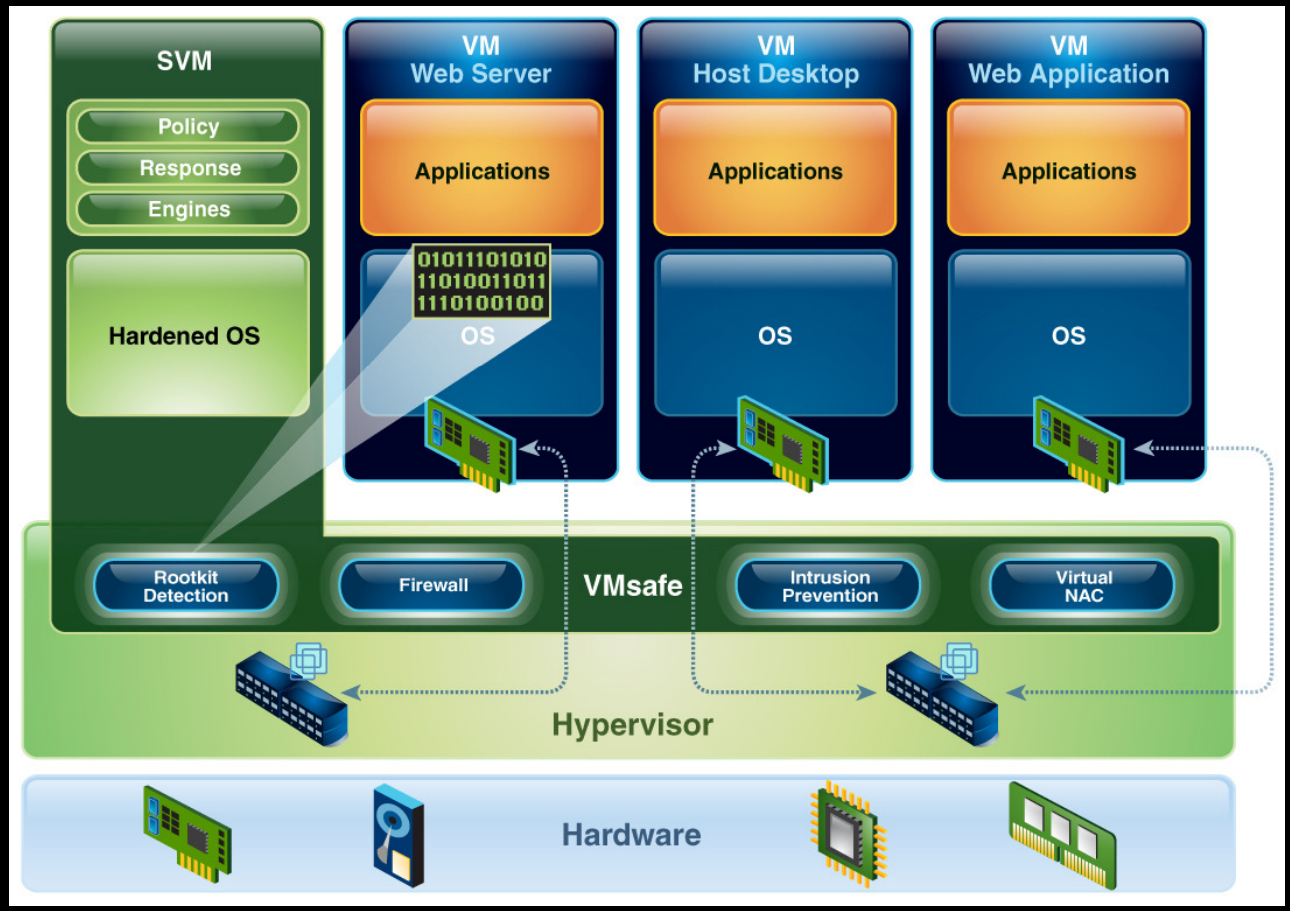
IDPS en Ambientes Virtuales

IDPS en Ambientes Virtuales - Problemática



23

IDPS en Ambientes Virtuales – Solución Actual



Mejores practicas de Implementación

En el caso de los IDPS en Ambientes Virtuales

- Nuevos escenarios:

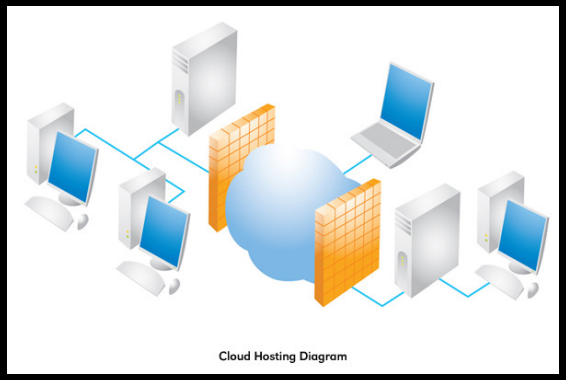
  - Ambientes virtuales

  - Cloud Computing

- Los ambientes virtuales están por fuera de las estructuras físicas de seguridad. Muchas vulnerabilidades si ser protegidas.

- Virtualizacion para fomentar el ahorro de energía.

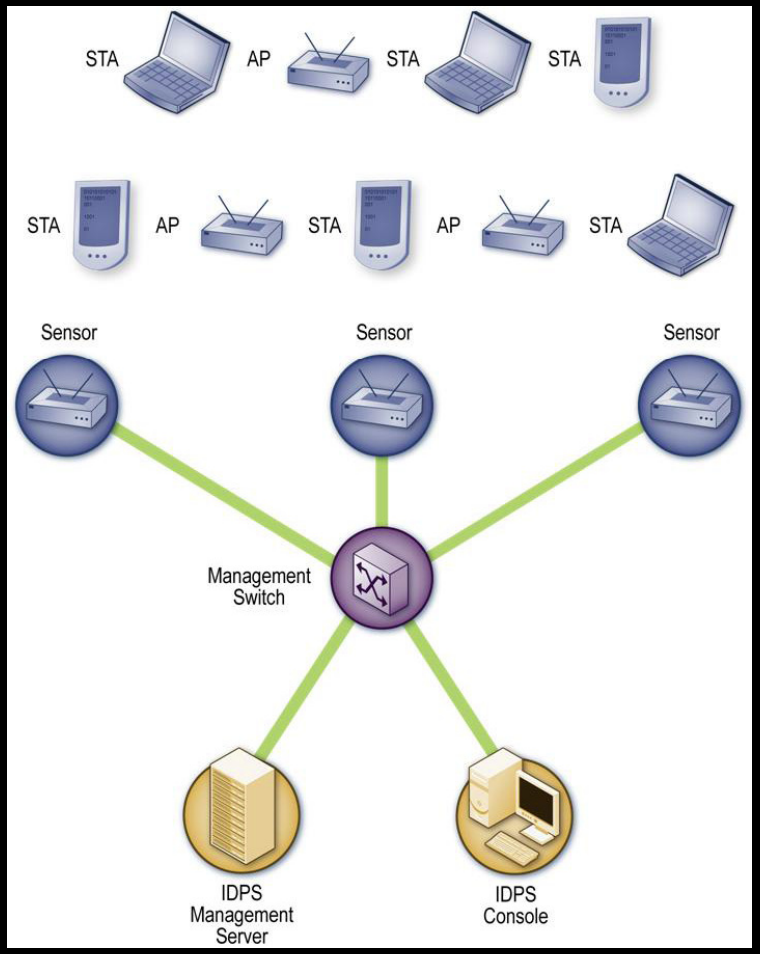
- Bajar costo en equipamiento y mantenimiento obteniendo mayor capacidad de procesamiento y reduciendo el espacio físico.



Wireless IDPS

WIDPS – Detección y Prevención de Intrusos en las redes Wireless

- Los IDPS en las Wireless LAN analizan los protocolos inalámbricos en busca de actividades sospechosas
- Funcionan del mismo modo que los IDPS de la red, con su servidor, base de datos y consola para administración
- Se pueden presentar en dos modalidades:
  - Equipos dedicados
  - APs con funcionalidad de IDPS
- Los análisis se dan solo de a un canal por vez lo cual aun tiene su contra.



Resumiendo - Problemáticas de hoy en día

- Tenemos un mundo cada vez mas instrumentado, interconectado e inteligente. Nuevas posibilidades, complejidades y por lo tanto nuevos riesgos para los cuales tenemos que estar preparados
- La gravedad de los fallos de seguridad aumentan año a año. Muchas empresas deben cerrar por los costos asociados a este tipo de infracciones. Multas, postura en el mercado, perdidas de datos de clientes, etc.
- La seguridad tradicional ya no es suficiente, Firewalls y Routers tradicionales son fáciles de eludir al día de hoy, los antivirus tradicionales son lentos a la hora de detectar un nuevo ataque.
- La mayoría de las empresas tienen miles de dispositivos conectados a Internet, cientos de aplicaciones instaladas en la red y gigabits de tráfico que fluye por la red cada día.

Resumiendo - como contrarrestamos

- Sistemas para detección y prevención de intrusos
- Prevención de intrusos
- Detección de intrusos
- Host
- Network
- Wireless
- Maquinas Virtuales
- Aumento de los requisitos de Seguridad frente a normas como la ISO 27001, PCI DSS, etc.

PREGUNTAS???

MUCHAS GRACIAS!!!

Charles Ware

cware@uy.ibm.com

Agradecimienos:

Joaquin Louzao

Juan Paulo Cabezas

Andres Aitcin

Mario Falcao

Dario Lessa

Gerardo Geis

Mauricio campiglia