IMPLANTACION Y PAP SISTEMAS IDS/IPS

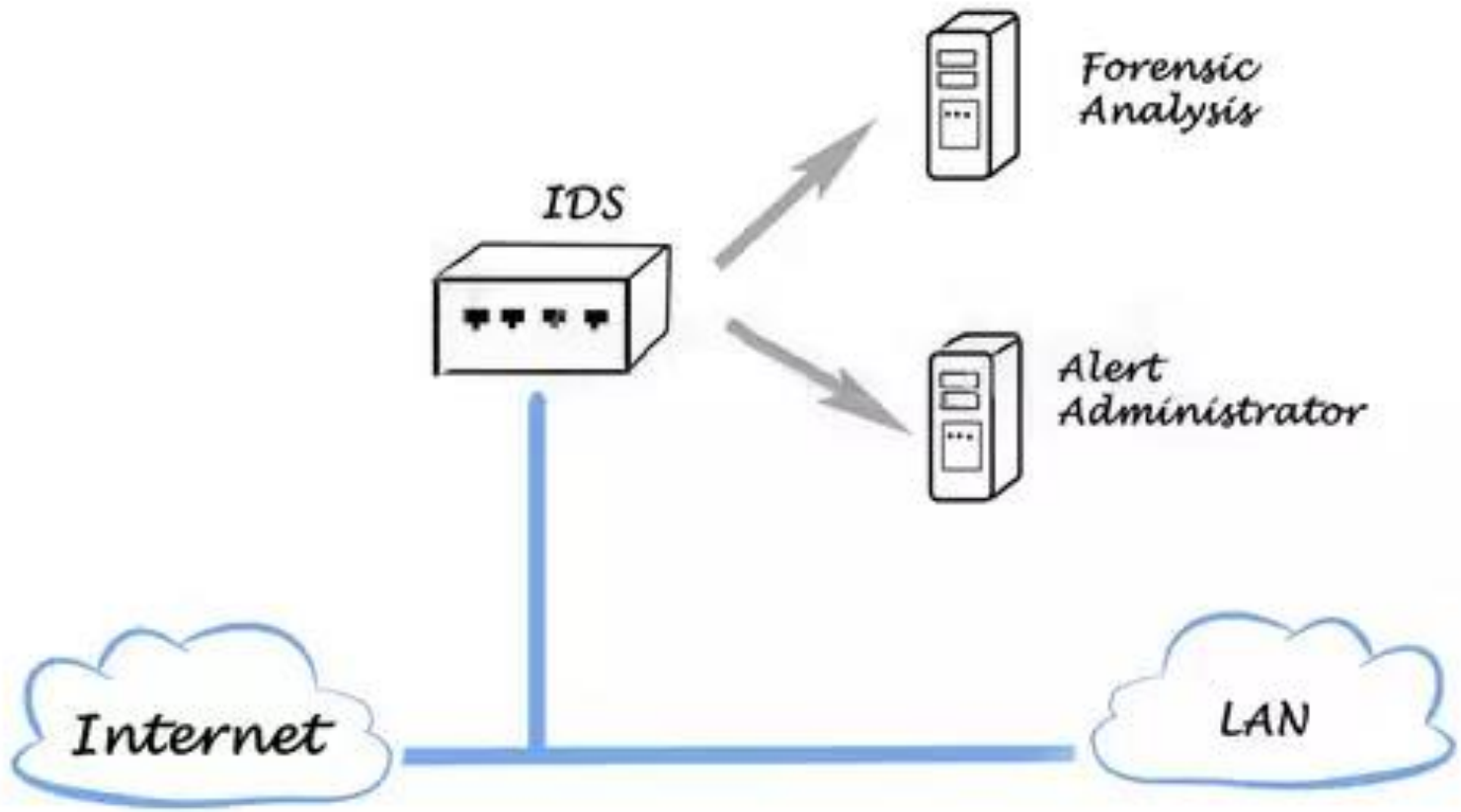
Implantación

- Uno de los lugares más comunes para implementar un IDS es cerca del firewall.
- Dependiendo del tráfico a monitorizar, se coloca por delante o por detrás del firewall para monitorizar el tráfico sospechoso, originado desde dentro o desde fuera de la red.
- Cuando se coloca en el interior, el IDS debe estar cerca de la DMZ. Sin embargo, la mejor práctica es utilizar una defensa en capas mediante la implementación de un IDS delante del firewall y otro detrás del firewall en la red.

Implantación

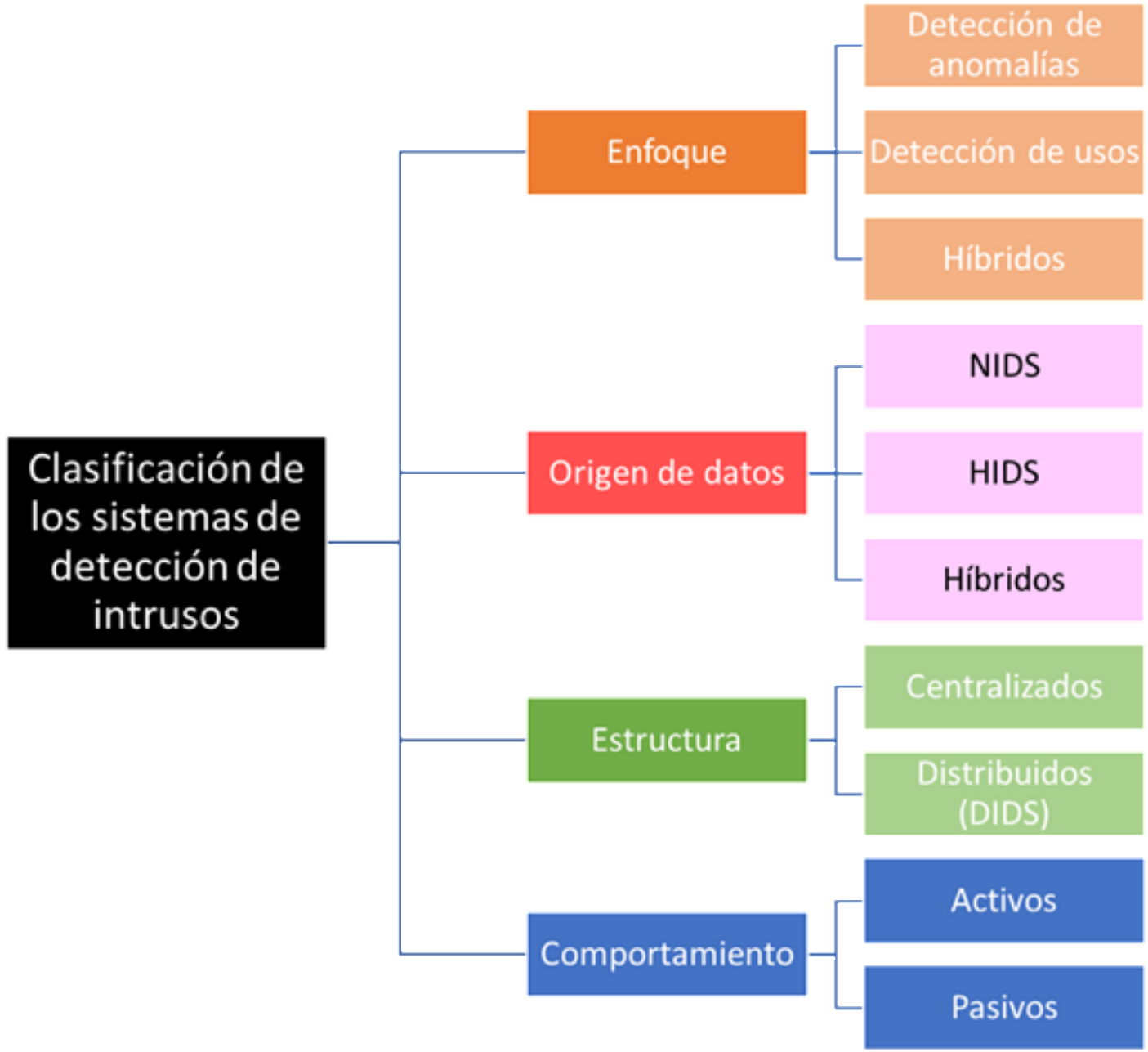
- Antes de implementar el IDS, es esencial analizar la topología de la red, comprender cómo fluye el tráfico hacia y desde los recursos que un atacante puede usar para obtener acceso a la red e identificar los componentes críticos que serán posibles objetivos de ataques contra la red. Una vez que se determina la posición del IDS en la red, el IDS debe configurarse para maximizar su efecto de protección de red.

Intrusion Detection System



Metodos deteccion

- a. Utilice firmas: el fabricante puede proporcionar más de 2.000 firmas, e IDS puede usar estas firmas para emparejar el tráfico de red. Cuando un nuevo paquete de datos ingresa a nuestra red, puede analizar su similitud en función de los datos de la firma en la base de datos. Si se detecta una coincidencia, se emitirá una alarma.
- b) Anormalidad de búsqueda: establezca una línea base para la operación del usuario. Por ejemplo, si treinta personas abren una conexión al mismo tiempo (considere el número de conexiones x 5), si una solicitud anormal establece 30 × 5 = 150 conexiones al mismo tiempo, se emitirá una alarma.
- c. Anomalía de protocolo: detecta información anormal basada en el protocolo. Por ejemplo, el protocolo utilizado por el sistema es HTTP, pero cuando el sistema detecta que algunas solicitudes usan otros protocolos o comandos desconocidos, el sistema pensará que viola el protocolo convencional y luego emitirá una alarma.


Clasificación de los sistemas de detección de intrusos
Enfoque
Detección de anomalías
Detección de usos
Híbridos
Origen de datos
NIDS
HIDS
Híbridos
Estructura
Centralizados
Distribuidos (DIDS)
Comportamiento
Activos
Pasivos

Funcionamiento

- Los IDS tienen sensores para detectar firmas maliciosas en paquetes de datos, y algunos IDS avanzados incluyen detección de actividad de comportamiento del tráfico malicioso. Incluso si las firmas de los paquetes no coinciden perfectamente con las firmas en la base de datos de firmas de IDS, el sistema de detección de actividad puede alertar a los administradores sobre posibles ataques.

- Si la firma coincide, el IDS realiza acciones predefinidas como terminar la conexión, bloquear la dirección IP, descartar el paquete y/o generar una alarma para notificar al administrador. Cuando el paquete pasa todas las pruebas, el IDS lo reenviará a la red.

¿Cómo detecta una intrusión?

- Un IDS **utiliza tres métodos** para detectar intrusiones en la red:

Reconocimiento de firmas

- El **reconocimiento de firmas**, también conocido como detección de uso indebido, intenta identificar eventos que indican un intento de acceso a un sistema o red.
- Esta técnica implica primero crear modelos de posibles intrusiones y luego comparar estos modelos con eventos entrantes para tomar una decisión de detección.
- Las firmas para IDS se crearon bajo el supuesto de que el modelo debe detectar un ataque sin perturbar el tráfico normal del sistema. Solo los ataques deben coincidir con el modelo, de lo contrario, podrían producirse falsas alarmas

detección de anomalías

- **La detección de anomalías difiere del reconocimiento de firmas.**
- La detección de anomalías implica una base de datos de anomalías. Se detecta una anomalía cuando se produce un evento fuera del umbral de tolerancia del tráfico normal.
- Por lo tanto, cualquier desviación del uso regular es un ataque. La detección de anomalías detecta intrusiones en función de las características de comportamiento fijas de los usuarios y los componentes de un sistema informático.

detección de anomalías de protocolo

- **La detección de anomalías de protocolo depende de las anomalías específicas de un protocolo**.
- Identifica fallos particulares en la implementación del protocolo TCP/IP por parte de los proveedores.
- Los protocolos están diseñados de acuerdo con las especificaciones RFC, que dictan negociaciones estándar para permitir la comunicación. El detector de anomalías de protocolo puede identificar estos ataques.
-

Tipos de sistemas de detección de intrusos

- Hay **dos tipos de sistemas de detección de intrusos**, sistemas de detección de intrusiones **basados en red y** sistemas de detección de intrusiones **basados en host.**
-

sistemas de detección de intrusos basados en la red (NIDS)

- **Los** verifican cada paquete que entra en la red para detectar la presencia de anomalías y datos incorrectos. Un NIDS captura e inspecciona todo el tráfico. Genera alertas a nivel de IP o aplicación en función del contenido.

- Los NIDS están más distribuidos que los IDS basados en host.
- El NIDS identifica las anomalías en los niveles de **routing y host**.
- Audita la información contenida en los paquetes de datos y registra la información de los paquetes maliciosos.
- Además, asigna un nivel de amenaza a cada riesgo después de recibir los paquetes de datos.
- El nivel de amenaza permite que el equipo de seguridad permanezca alerta. Estos mecanismos generalmente consisten en una caja negra colocada en la red en un modo promiscuo, escuchando patrones indicativos de una intrusión. Detecta actividad maliciosa, como ataques DoS, escaneos de puertos o incluso intentos de acceso a servidores.

IDS basado en host (HIDS)

- **Un IDS basado en host (HIDS)** analiza el comportamiento de cada **sistema**. El HIDS se puede instalar en cualquier sistema, desde un simple PC de escritorio hasta en un servidor. Es más **versátil** que el NIDS. Además de detectar actividades internas no autorizadas, los sistemas basados en host también son eficaces para detectar modificaciones de archivos no autorizados.

IDS basado en host (HIDS)

- El HIDS se centra en los aspectos cambiantes de los sistemas locales. También está más centrado en la plataforma, con un mayor enfoque en el sistema operativo Windows, sin embargo, hay otros HIDS disponibles para plataformas UNIX. No son muy comunes debido a la sobrecarga en la que incurren al tener que monitorizar cada evento del sistema.

- Es importante que nuestro IDS actualice la información de forma habitual, para así tener actualizadas siempre sus técnicas de análisis así como de las bases de datos de firmas.

- Existen una serie de organizaciones, asociaciones y empresas que nos permisos estar al corriente de las evoluciones en materia de técnicas de intrusión y ataques. Las principales son:

- Bugtraq: Es una lista de difusión dedicada a la publicación de vulnerabilidades, su uso y corrección. (https://www.securityfocus.com/)
- CERT: Computer Emergency Response Team. Se trata de una organización que estudia las vulnerabilidades, investiga las evolucaciones en términos de redes y seguridad y ofrece servicios relacionados con la seguridad. (Entrada de Wikipedia al respecto)
- CIAC: Computer Incident Advisory Capability. Una organización de alerta e investigación gestionado por el departament de energía de Estados Unidos. (https://www.energy.gov/cio/about-our-services/integrated-joint-cybersecurity-coordination-center)

Consideraciones de diseño

- a. IDS generalmente se implementa detrás del firewall.
- b) En el diagrama de diseño anterior, el IDS implementado en la ubicación 1 se usa para proteger el servidor web.
- c. El IDS implementado por Location 2 se usa para proteger los componentes de red restantes del software malicioso.
- d. Este es un IDS basado en la red, no un IDS basado en el host, por lo que no puede detectar malware generado entre dos hosts en la red.

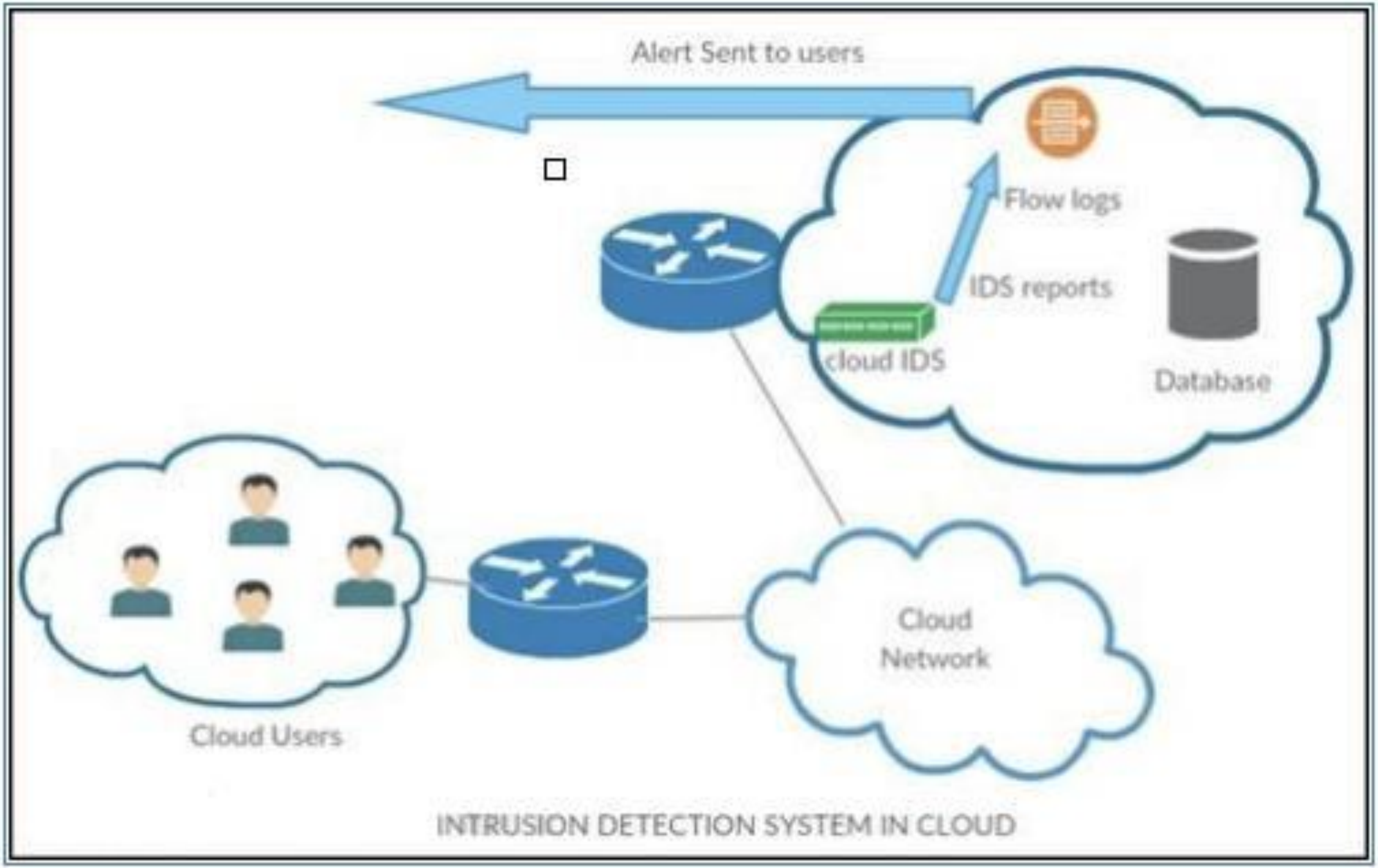
Tipos

- **IDS / IPS basado en host**
- El IDS basado en host solo puede monitorear un sistema. Se ejecuta en el host que necesita proteger. Puede leer el registro del host y buscar anomalías. Pero debe tenerse en cuenta que después de que ocurre el ataque, el IDS basado en el host puede detectar anomalías. El IPS basado en la red puede detectar paquetes de datos en el segmento de la red. Si el IPS basado en la red está diseñado correctamente, puede reemplazar el IPS basado en el host. Otra desventaja de los IDS basados en host es que cada host en la red necesita implementar un sistema IDS basado en host. Puede imaginar que si tiene 5000 hosts en su entorno, sus costos de implementación serán muy altos.
-

- **IDS / IPS basado en dispositivo**
- Puede instalar IDS en un servidor físico o virtual, pero debe abrir dos interfaces para manejar el tráfico de red entrante y saliente. Además, también puede instalar el software IDS como Snort en el servidor Ubuntu (máquina virtual).
- **IDS / IPS basado en enrutador**
- En una red, casi todo el tráfico pasa a través de enrutadores. Como puerta de enlace de un sistema de red, el enrutador es un puente entre el host en el sistema y la red externa. Por lo tanto, en la arquitectura de diseño de seguridad de red, los enrutadores también son lugares donde se pueden considerar los sistemas IDS e IPS para su implementación. Hay muchos software de terceros que se pueden integrar en los enrutadores, y pueden formar la primera línea de los sistemas de red contra amenazas externas.
- I**DS / IPS basado en firewall**
- La diferencia entre un cortafuegos e IDS es que el cortafuegos parece evitar que ingresen amenazas externas a nuestra red, pero no puede monitorear los ataques que ocurren dentro

Implementación de IDS / IPS basado en entorno de nube

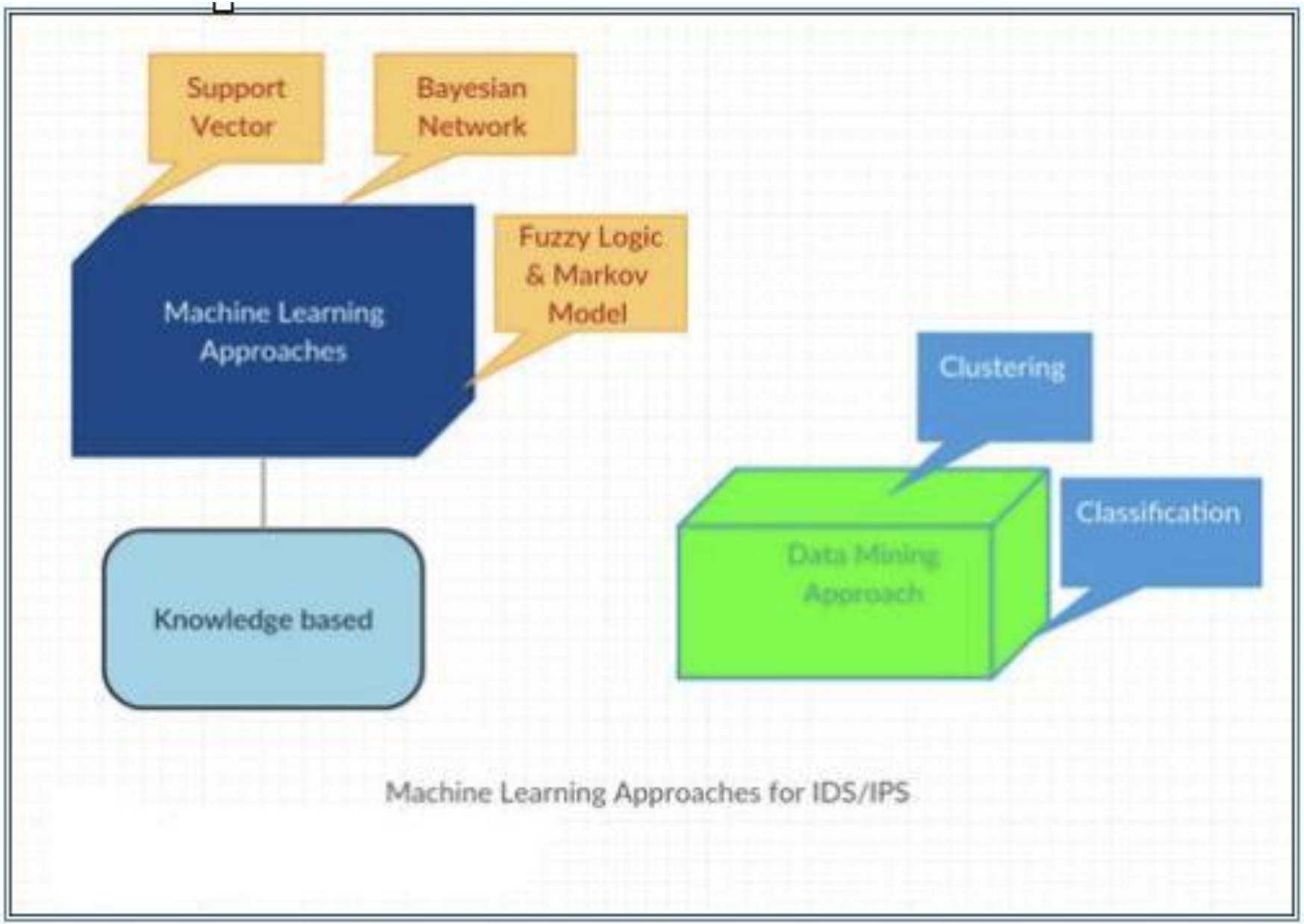
- Para los usuarios que alojan sus archivos y aplicaciones en la nube, si el proveedor de servicios en la nube ha implementado IDS puede convertirse en uno de los factores que los clientes consideran. Además, los usuarios también pueden implementar Snort IDS (Community Edition) para monitorear y detectar amenazas.



INTRUSION DETECTION SYSTEM IN CLOUD

Mejoras

- **Utilice algoritmos de aprendizaje automático para la detección de intrusos.**
- Existen muchos algoritmos de aprendizaje automático que pueden detectar anomalías y generar advertencias. El algoritmo de aprendizaje automático puede aprender los patrones de comportamiento malicioso, e incluso si el comportamiento malicioso cambia, puede generar alertas rápidamente.
-



Machine Learning Approaches for IDS/IPS

Gestionando las alertas

- cuando detecta tráfico perjudicial, dejará una traza en el archivo de registro, a través de syslog y enviará una copia del paquete en un archivo con formato tcpdump, que es compatible con Wireshark, al utilizar el formato lippcap.

- Aunque también se puede enviar a información a una base de datos, como MySQL/MariaDB

Falsos positivos

- Se denomina falso positivo a la instancia en la que el IDS identifica una actividad como un ataque, pero la actividad es un comportamiento aceptable.

- Por este motivo, muchas tecnologías IPS también tienen la capacidad de capturar secuencias de paquetes del evento de ataque.

- Dichas secuencias se pueden luego analizar para determinar si hubo una amenaza real y para mejorar aún más la protección IPS