IDS - SISTEMA DE DETECCIÓN DE INTRUSIONES

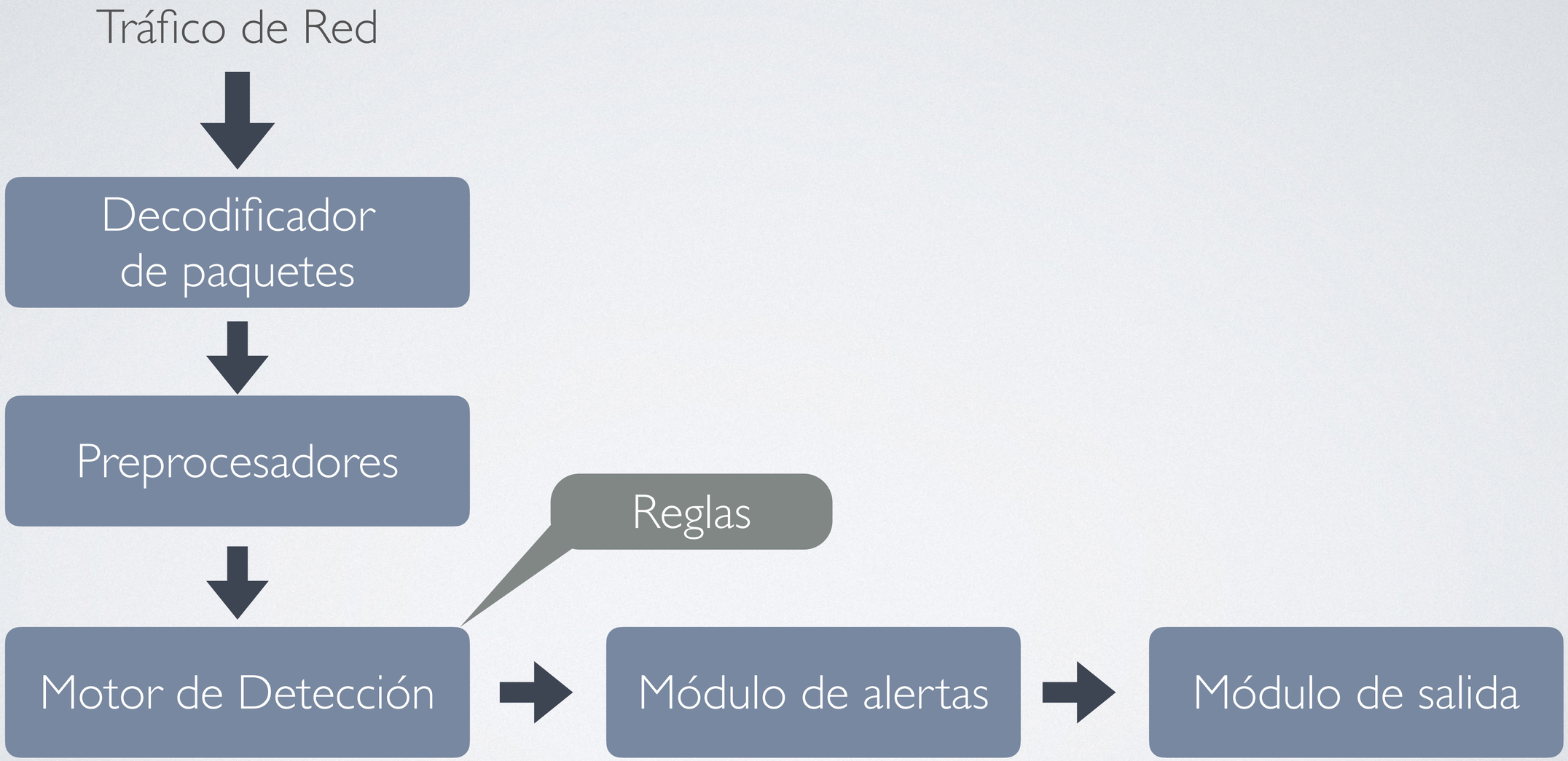
TIPOS SEGÚN SU COMPORTAMIENTO:

- Basados en anomalías: necesitan "aprender" cuál es el comportamiento normal
- Basados en reglas: avisan cuando se produce una situación previamente definida

TIPOS SEGÚN SU APLICACIÓN:

- De host (HIDS): controlan la actividad en un equipo (procesos, conexiones, ficheros..)
- De red (NIDS): monitorizan el tráfico de red

COMPONENTES DE SNORT



REGLAS

```
SINTAXIS: acción protocolo origen puerto_origen -> destino puerto_destino (opciones)

Ejemplo: alert ip 8.8.8.8 53 -> 192.168.0.0/24 53 (msg:"DNS";sid:1000001;)
```

Acción: alert, log, pass, dynamic, drop, reject

Protocolo: TCP, UDP, ICMP e IP (que incluye los tres anteriores).

Para indicar cualquier ip o puerto se usa la palabra **any**

Opciones:

- **msg**: mensaje de la alerta
- **sid**: identificador de la regla. Las propias deben ser mayor a 1.000.000

REGLAS

Opciones:

- **content**: contenido del paquete, se puede indicar en texto o hexadecimal (entre |)
  - **offset**: dónde empezar a buscar el contenido
  - **depth**: dónde parar de buscar el contenido
  - **nocase**: para que la búsqueda de los datos no sea sensible a las mayúsculas

```
alert tcp any any -> 192.168.1.10 21 (content:"USER root"; msg:"Acceso root por FTP";sid:1000002;)
```

```
alert tcp $EXTERNAL_NET any -> 192.168.1.0/24 143 (content: "|90C8 C0FF FFFF|"; msg: "IMAP overflow";)
```

```
alert tcp any any -> 192.168.1.0/24 80 (content: "cgi-bin/phf"; offset: 3; depth: 22; msg: "CGI-PHF access";)
```