IDS/IPS

Hasta ahora se han desplegado redes que implementan mecanismos de control de tráfico entre redes en diferentes puntos. Ahora necesitamos herramientas que ayuden a catalogar amenazas no definidas previamente, definidas por aplicaciones maliciosas o APT (Advanced Persistent Threat).

Los sistemas de detección de intrusiones analizan el tráfico en una red o el comportamiento de un equipo y determinan si están ocurriendo sucesos anómalos que puedan ser asociados a acciones maliciosas o ataques. En la actualidad, para detectar ataques, tenemos 2 enfoques:

- Monitorizar el tráfico de red para localizar ataques conocidos
- Disponer de sistemas de detección de instrucciones que modeliza el comportamiento de una red para detectar si se producen anomalías.