- IDS(Intrusion Detection Systems)
- IPS(Intrusion Prevention Systems)

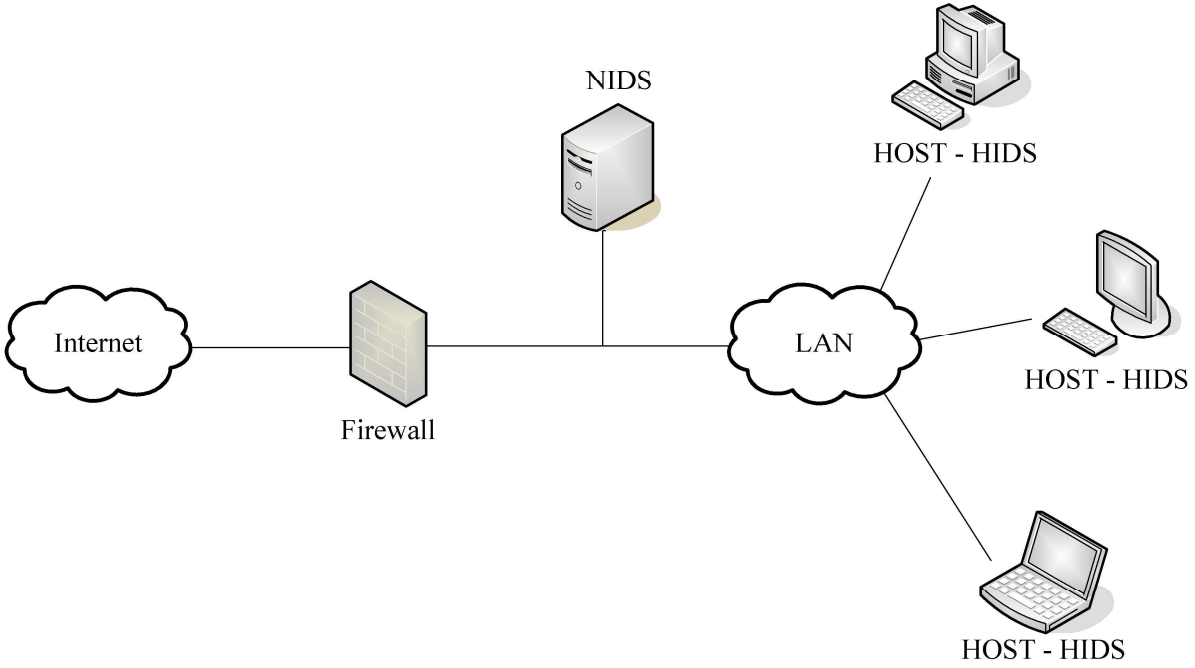
Características

- Funciona como um alarme.
- Detecção com base em algum tipo de conhecimento:
  - Assinaturas de ataques.
  - Aprendizado de uma rede neural.
- Detecção com base em comportamento anômalo.
- IPS (Intrusion Prevention System).

- Existem basicamente dois tipos de IDS.
  - NIDS (*Network-Based Intrusion Detection System*)
  - HIDS (*Host-Based Intrusion Detection System*)

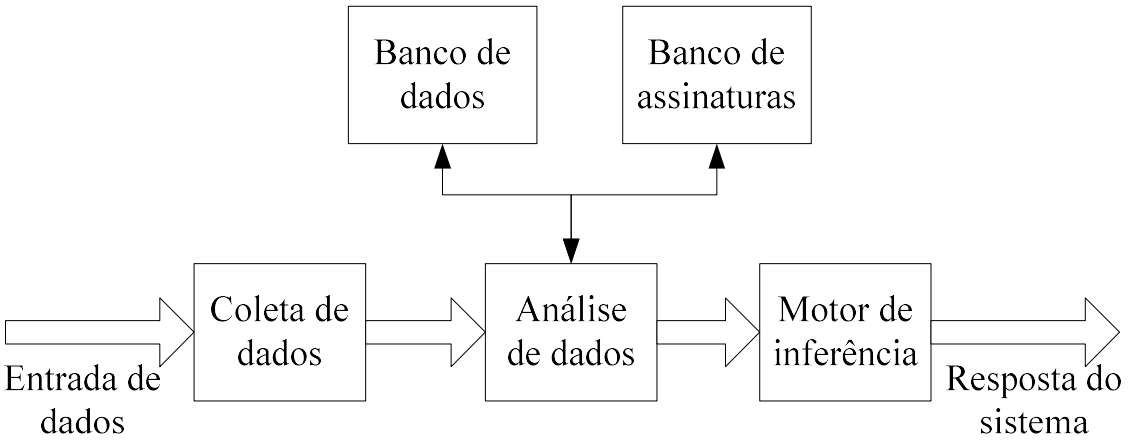
Localização de um IDS na rede.

- IDS é o processo de monitoramento de eventos e análise dos sinais/anomalias, de intrusões que ocorrem em um ambiente computacional



Funções do IDS

- O IDS possui as seguintes funções.
  - Coleta de informações
  - Análise de informações
  - Armazena informações
  - Responde às atividades suspeitas



Resultados possíveis de uma análise

- Tráfego **suspeito detectado** (comportamento normal).
- Tráfego **suspeito não detectado** (falso negativo).
- Tráfego **legítimo** que o IDS **analisa como sendo suspeito** (falso positivo).
- Tráfego **legítimo** que o IDS **analisa como sendo normal** (comportamento normal).

Metodologia de detecção

- **Baseado no conhecimento.**
  - Base de assinaturas de ataques conhecidos
  - Rede neural.

- **Baseado no comportamento.**
  - Desvios dos usuários ou dos sistemas, quanto a um padrão de normalidade.
  - Análise estatística afim de encontrar possíveis mudanças de comportamento: por exemplo, aumento súbito de tráfego.
  - Problemas: falsos negativos e muitos falsos positivos.

Análises estatísticas para IDS e IPS.

- A detecção estatística de anomalia envolve a coleta de dados relacionados ao comportamento dos usuários legítimo por um período de tempo.

- Depois, testes estatísticos são aplicados ao comportamento observado para determinar com alto nível de confiabilidade se esse comportamento não é um comportamento legítimo do usuário.

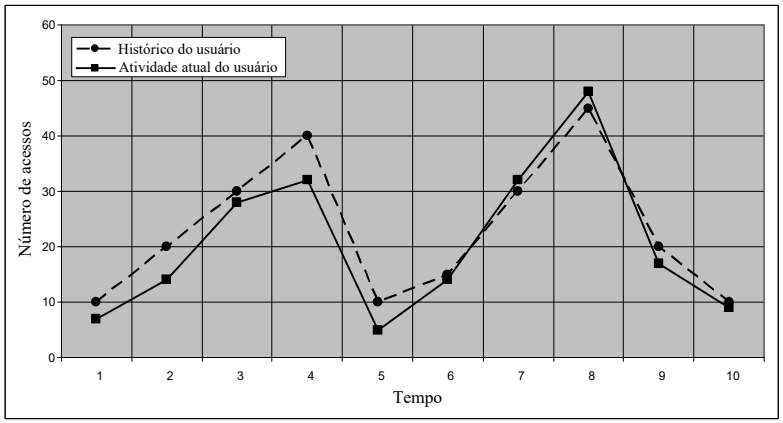
- O método de análise estatística mantém um histórico de perfis estatísticos de cada usuário ou do sistema que se controla.

Inatel
Instituto Nacional de Telecomunicações

www.inatel.br

Análises estatísticas para IDS e IPS.

- Atividade de um usuário legítimo.



- Atividade de uma **possível** anomalia na rede.