# AULA 10 – Sistemas de Detecção de Intrusão

## Intrusão

Uma intrusão pode ser qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou sistema. As intrusões são divididas em duas classes principais:

- **Intrusões devido a mau uso do sistema**: são os ataques realizados a pontos fracos (conhecidos) do sistema. Podem ser descobertas através de comparações com padrões já estabelecidos. Por exemplo, pode-se detectar a tentativa de criar um arquivo através da análise de *logs*;

- **Intrusões devido à mudança de padrão**: são detectadas com observação de mudanças de uso em relação ao padrão de perfil de uso normal do sistema montado anteriormente. Os padrões podem ser de utilização da CPU, número de conexões por minuto, número de processos por usuário, número de conexões, volume de dados trafegando no segmento de rede, entre outros. Uma variação significativa nesses padrões pode indicar uma invasão.

## IDS

A RFC 2828 (*Request for Coments* nº 2828) define o termo IDS – Intrusion Detection System – Sistema de Detecção de Intrusos como sendo um serviço que monitora e analisa eventos de uma rede com o propósito de encontrar e providenciar alertas em tempo real a acessos aos recursos da rede de maneira não autorizada. Ou seja, pode ser definido como um programa ou sistema, que está constantemente, em segundo plano, de maneira imperceptível para o usuário comum, monitorando o tráfego de uma rede de computadores a procura de indícios de invasões. Se encontrá-las, aciona as rotinas pré-definidas pela empresa a fim de inibir tal acesso.

## Características do IDS

Um sistema IDS deve possuir as seguintes características:

- Deve funcionar continuamente sem intervenção humana e ser seguro o suficiente para permitir a sua operação em segundo plano;

- Deve ser tolerante à falhas, ou seja, a sua base de conhecimento não deve ser perdida em caso de falha do sistema operacional;

- Deve monitorar a si próprio evitando qualquer mudança na sua base de dados;

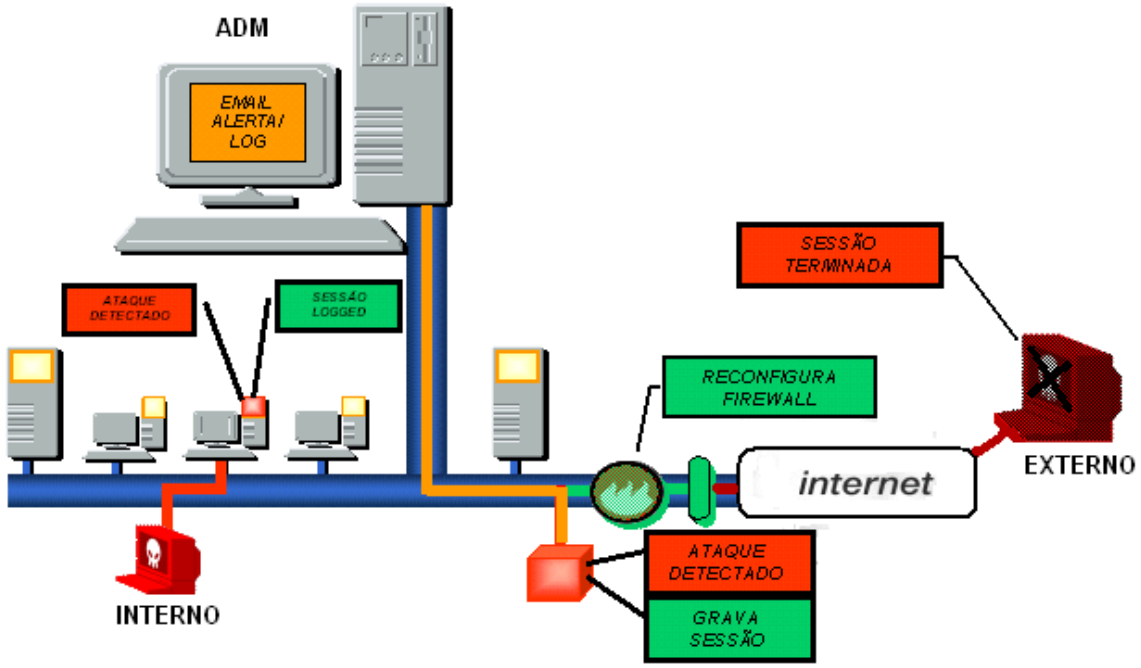
- Deve causar o mínimo de impacto no funcionamento do sistema;

- Deve detectar mudanças no funcionamento normal do sistema;

- Deve detectar o menor número possível de Falsos Positivos, classificando uma ação legal como uma possível intrusão;

- Não deve permitir Falso Negativo (ocorre quando uma intrusão real acontece, mas o sistema a classifica como legítima);

- Não deve permitir a Subversão (ocorre quanto o intruso modifica a operação da ferramenta de IDS para forçar a ocorrência de falso negativo).




Um sistema contra intrusão pode ser utilizado com vários propósitos. Dentre os principais podem ser destacados:

- Indicar ao administrador de rede ou do sistema, em tempo real, sobre uma possível invasão, disparando automaticamente mecanismos de segurança;

- Reconfigurar automaticamente o firewall, a fim de impedir a tentativa de ataque;

- Colher informações de tentativas de intrusão;

- Diagnosticar e corrigir eventuais falhas de segurança.