FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

4SEG – SEGURANÇA DE REDES
AULA 3
Antimalwares, Firewall, Proxy, DMZ, IDS/IPS

Profa. Maria Cláudia Roenick Guimarães
E-mail: maria.roenick@faeterj-rio.edu.br

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Cenário

- Como vimos anteriormente estamos cercados por ameaças que exploram as vulnerabilidades de nosso ambiente para obter dados e informações que possam ser úteis;
- Existem várias soluções no mercado que permitem proteger nossa infraestrutura e nossos dados desses ataques;
- Estaremos estudando algumas delas ao longo da aula.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Antimalware

- São aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador;
- Muitas vezes é difícil delimitar a área de atuação de cada uma delas, pois a definição do tipo de código malicioso depende de cada fabricante e muitos códigos mesclam as características dos demais tipos;

- Exemplos de ferramentas desse tipo: Antivírus, antispyware, antirootkit e antitrojan;

- A ferramenta que engloba a maior quantidade de funcionalidades é o antivírus. Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas;

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Antimalware

- As ferramentas antimalware diferem entre si das seguintes formas:
  - **Método de detecção**: assinatura (uma lista de assinaturas é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características que o código malicioso possui) e comportamento (baseia-se no comportamento apresentado pelo código malicioso quando executado) são alguns dos métodos mais comuns.
  - **Forma de obtenção**: podem ser gratuitos (quando livremente obtidos na Internet e usados por prazo indeterminado), experimentais (trial, usados livremente por um prazo predeterminado) e pagos (exigem que uma licença seja adquirida).
    - Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras, além de poder contar com suporte.

Antimalware

- As ferramentas antimalware diferem entre si das seguintes formas (Cont.):
  - Execução: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.
  - Funcionalidades apresentadas: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e firewall pessoal.
    - Exemplos: Anubis - Analyzing Unknown Binaries (http://anubis.iseclab.org/), ThreatExpert - Automated Threat Analysis (http://www.threatexpert.com/), Norman Sandbox (http://www.norman.com/security_center/security_tools/), VirusTotal - Free Online Virus, Malware and URL Scanner (https://www.virustotal.com/)

Antimalware

- As ferramentas antimalware diferem entre si das seguintes formas (Cont.):
  - Execução: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.
  - Funcionalidades apresentadas: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e firewall pessoal.
    - Exemplos: Anubis - Analyzing Unknown Binaries (http://anubis.iseclab.org/), ThreatExpert - Automated Threat Analysis (http://www.threatexpert.com/), Norman Sandbox (http://www.norman.com/security_center/security_tools/), VirusTotal - Free Online Virus, Malware and URL Scanner (https://www.virustotal.com/)

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Firewall

- É uma solução que isola a rede interna de uma organização da Internet (ou de outras redes), permitindo que alguns pacotes sejam encaminhados e bloqueando outros;
- Ele permite a um administrador de rede controlar o acesso entre o mundo externo e os recursos da rede que ele administra, gerenciando o fluxo de tráfego de e para esses recursos;
- Pode ser implementado em uma combinação de hardware e software (normalmente chamados de UTM) ou via software. O primeiro garante um melhor desempenho e deve ser utilizado em locais com grande fluxo de dados;
- Os firewalls podem ser classificados em três categorias: (1) filtros de pacotes tradicionais, (2) filtros de estado e (3) gateways de aplicação ou proxys.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Firewall

- O firewall de filtro de pacotes surgiu na década de 80, também conhecido como filtragem estática.
  - Aqui se analisa as informações do cabeçalho dos datagramas IP (pacotes), como endereço IP de origem, destino, tamanho, tipo de serviço etc;
  - Dificuldade em filtrar protocolos que utilizam portas dinâmicas;
  - PERMITE explorar vulnerabilidades de protocolos e serviços da camada de aplicação;

- Como evolução desse modelo, surge o stateless packet filter que permitia análise de mais detalhes no filtro de pacotes, como flags TCP (no Linux, IPCHAINS);

- Uma nova evolução é o stateful packet filter, também conhecido como filtro dinâmico, utilizando um conjunto de regras de filtragem e informações de estado das conexões (no Linux, IPTABLES).

Firewall

- Dentre as arquiteturas mais conhecidas, temos:
  - Dual-Homed Host:
    - Fica entre uma rede interna e a rede externa - normalmente, a Internet;
    - Todo o tráfego passa por este firewall, não havendo acesso da rede interna para a rede externa (e vice-versa) diretamente;
    - Vantagem: Grande controle do tráfego;
    - Desvantagem: Qualquer problema com o dual-homed pode pôr em risco a segurança da rede ou mesmo paralisar o tráfego.

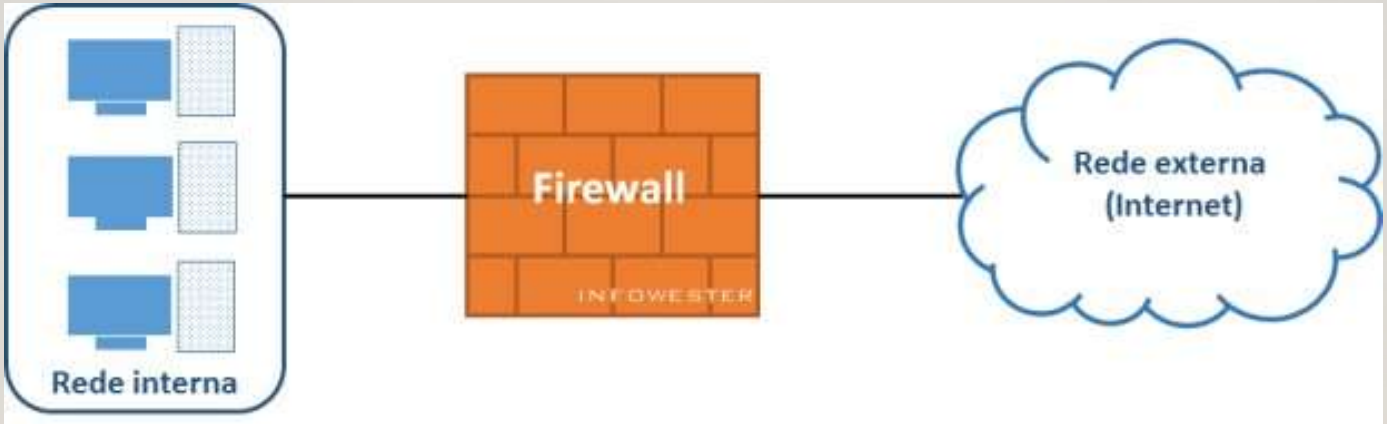


Figura: Arquitetura Dual Homed Host - Fonte: https://www.infowester.com/firewall.php

Firewall

- Dentre as arquiteturas mais conhecidas, temos:
  - Screened Host:
    - Há dois dispositivos intermediadores: um que faz o papel de roteador (screening router) e outro chamado de bastion host;
    - O bastion host atua entre o roteador e a rede interna, não permitindo comunicação direta entre ambos os lados. As decisões tomadas pelo filtro de pacotes no roteador são revisadas pelo bastion host;
    - Ponto crítico da estrutura: o bastion host precisa ser bem protegido.

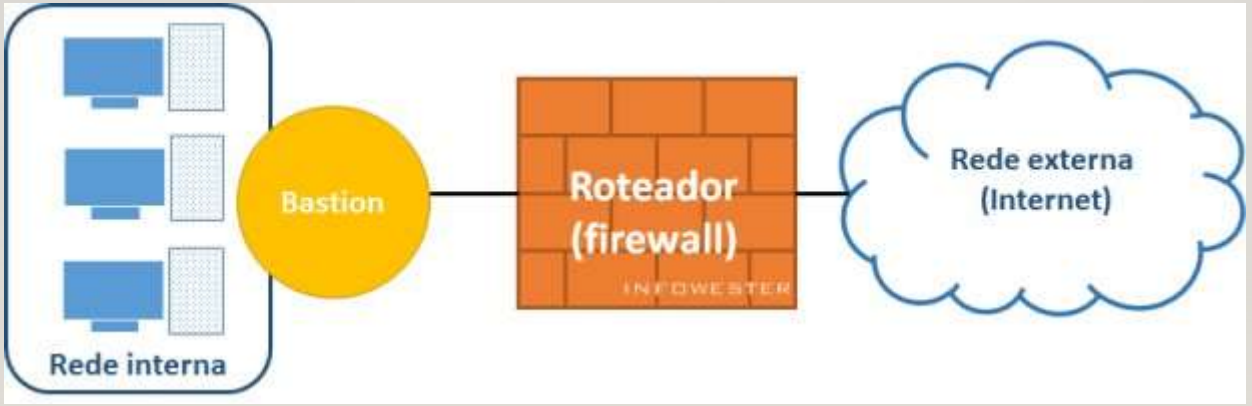


Figura: Arquitetura Screened Host - Fonte: https://www.infowester.com/firewall.php

Firewall

- Dentre as arquiteturas mais conhecidas, temos:
  - Screened Subnet:
    - O bastion host fica dentro de uma área isolada de nome interessante: a DMZ, sigla para Demilitarized Zone;
    - Caso o invasor passe pela primeiro roteador, terá ainda que lidar com a zona desmilitarizada – Maior segurança;
    - Na DMZ, normalmente, ficam os serviços acessíveis pela Internet;
    - O nível segurança e a flexibilidade de configuração fazem da Screened Subnet uma arquitetura normalmente mais complexa e, consequentemente, mais cara.

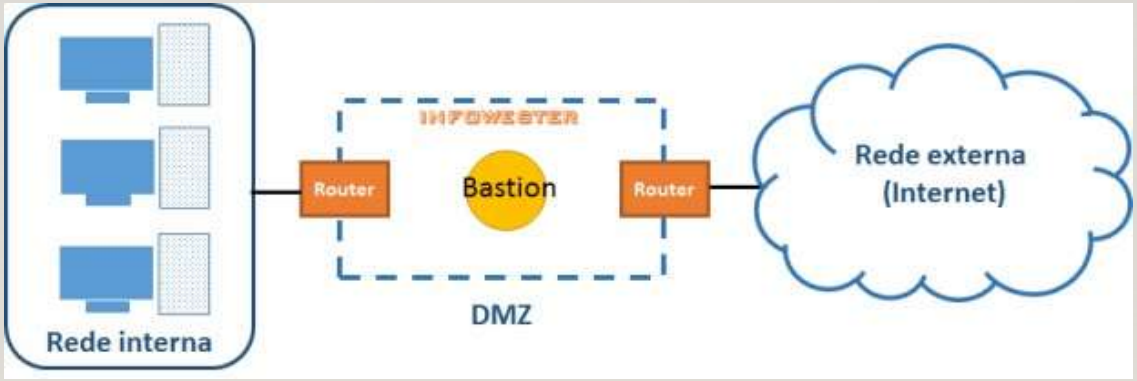


Figura: Arquitetura Screened Subnet - Fonte: https://www.infowester.com/firewall.php

- Gateway de Aplicações ou Proxy:
  - A filtragem de pacotes permite que uma organização faça uma filtragem grosseira de conteúdos de cabeçalhos IP e TCP/UDP, incluindo endereços IP, números de porta e bits de reconhecimento;
  - Gateways de aplicação fazem mais do que examinar cabeçalhos IP/TCP/UDP e tomam decisões com base em dados da aplicação. Um gateway de aplicação é um servidor específico de aplicação, através do qual todos os dados da aplicação (que entram e que saem) devem passar;
  - Necessita de 2 conexões: (1) Cliente – Proxy e (2) Proxy – Servidor;
  - Pode ser implementado:
    - Conexão direta - configurando o navegador;
    - Proxy de Autenticação – usuário se identifica e autentica;
    - Proxy Transparente – NÃO configura o navegador, o usuário não tem o conhecimento da existência do proxy ou que o utiliza.

Firewall

- Vantagens de uso de Gateway de Aplicações ou Proxy:
  - Impor restrições com base em: horários, login, endereço IP, etc;
  - Implementar Cache de páginas e arquivos;
  - Registrar todos os acesso (LOGs).

- Desvantagens de uso de Gateway de Aplicações ou Proxy:
  - Pode utilizar servidores diferentes para cada aplicação (serviço);
  - Aumenta o atraso ao acessar um serviço.

- Laboratório de Firewall e Proxy: https://www.udemy.com/firewall-linux-com-iptables/

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

IDS / IPS

- Para detectar muitos tipos de ataque, precisamos executar uma inspeção profunda de pacote, ou seja, precisamos olhar através dos campos de cabeçalho e dentro dos dados da aplicação que o pacote carrega;
- Um dispositivo que gera alertas quando observa tráfegos potencialmente mal-intencionados é chamado de sistema de detecção de invasão (IDS - Intrusion Detection System);
- Um dispositivo que filtra o tráfego suspeito é chamado de sistema de prevenção de invasão (IPS - Intrusion Prevention System);
- Um IDS / IPS pode ser usado para detectar uma série de tipos de ataques, incluindo mapeamento de rede (provindo, por exemplo, de nmap), varreduras de porta, varreduras de pilha TCP, ataques de DoS, ataques de inundação de largura de banda, worms e vírus, ataques de vulnerabilidade de OS e ataques de vulnerabilidade de aplicações.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

IDS / IPS

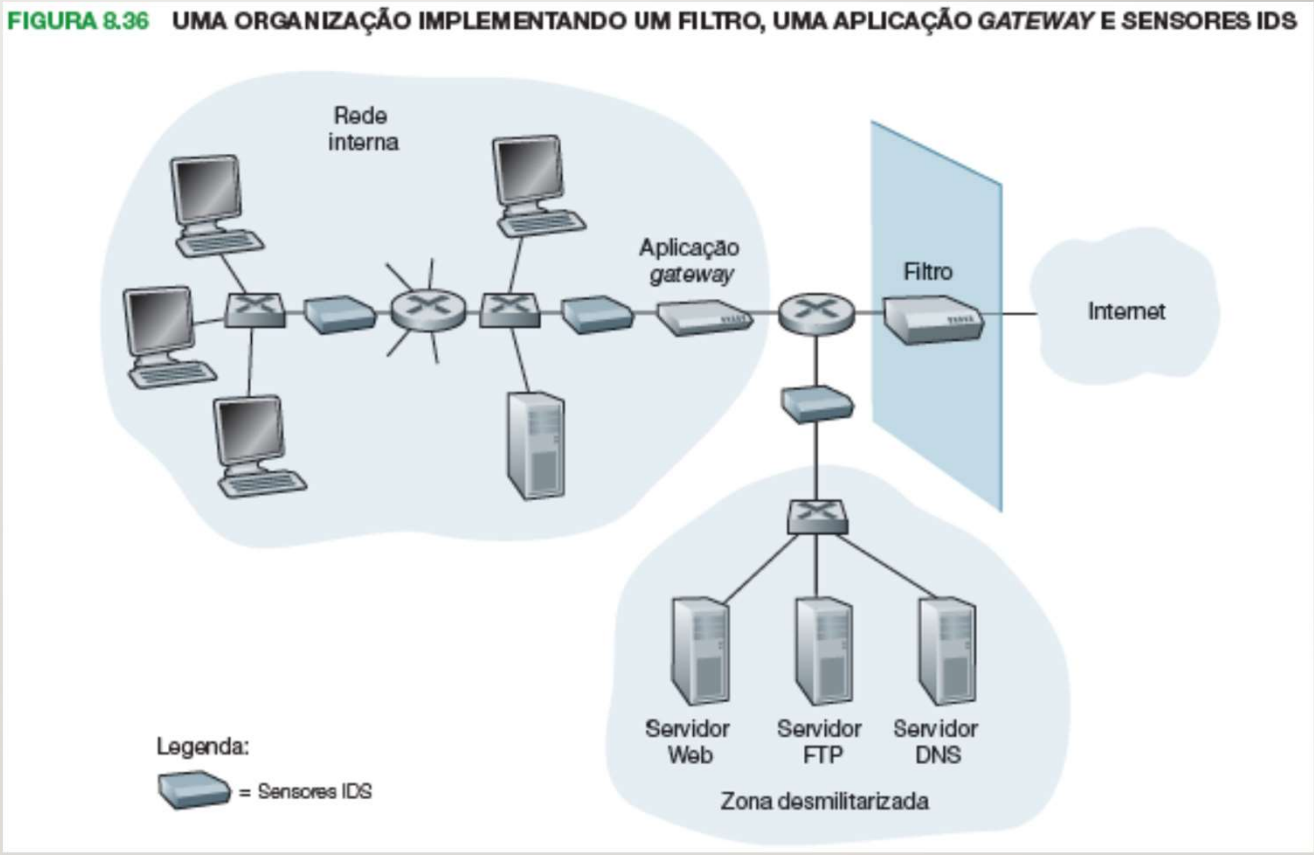
- O conceito IDS/IPS surgiu no início dos anos 80;
- 1ª Geração:
  - Registros de auditoria eram processados off-line;
  - Surgimento dos principais métodos de detecção;
- 2ª Geração:
  - Processamento estatisticamente mais sofisticado;
  - Mais medidas de comportamento monitoradas;
  - Alertas online tornaram-se possíveis;
- 3ª Geração:
  - Uso dos conceitos anteriores para sistemas em rede/sistemas distribuídos;
  - Uso de novas técnicas para detecção (sistemas especialistas, redes neurais, data mining etc);
  - Surgimento dos primeiros IDSs comerciais.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

IDS / IPS

- Pode-se utilizar um ou mais sensores IDS/IPS na organização. Quando múltiplos sistemas são executados, eles costumam trabalhar em harmonia, enviando informações sobre atividades de tráfegos suspeitos ao processador IDS/IPS central, que as coleta e integra e envia alarmes aos administradores da rede quando acharem apropriado;

FIGURA 8.36 UMA ORGANIZAÇÃO IMPLEMENTANDO UM FILTRO, UMA APLICAÇÃO *GATEWAY* E SENSORES IDS

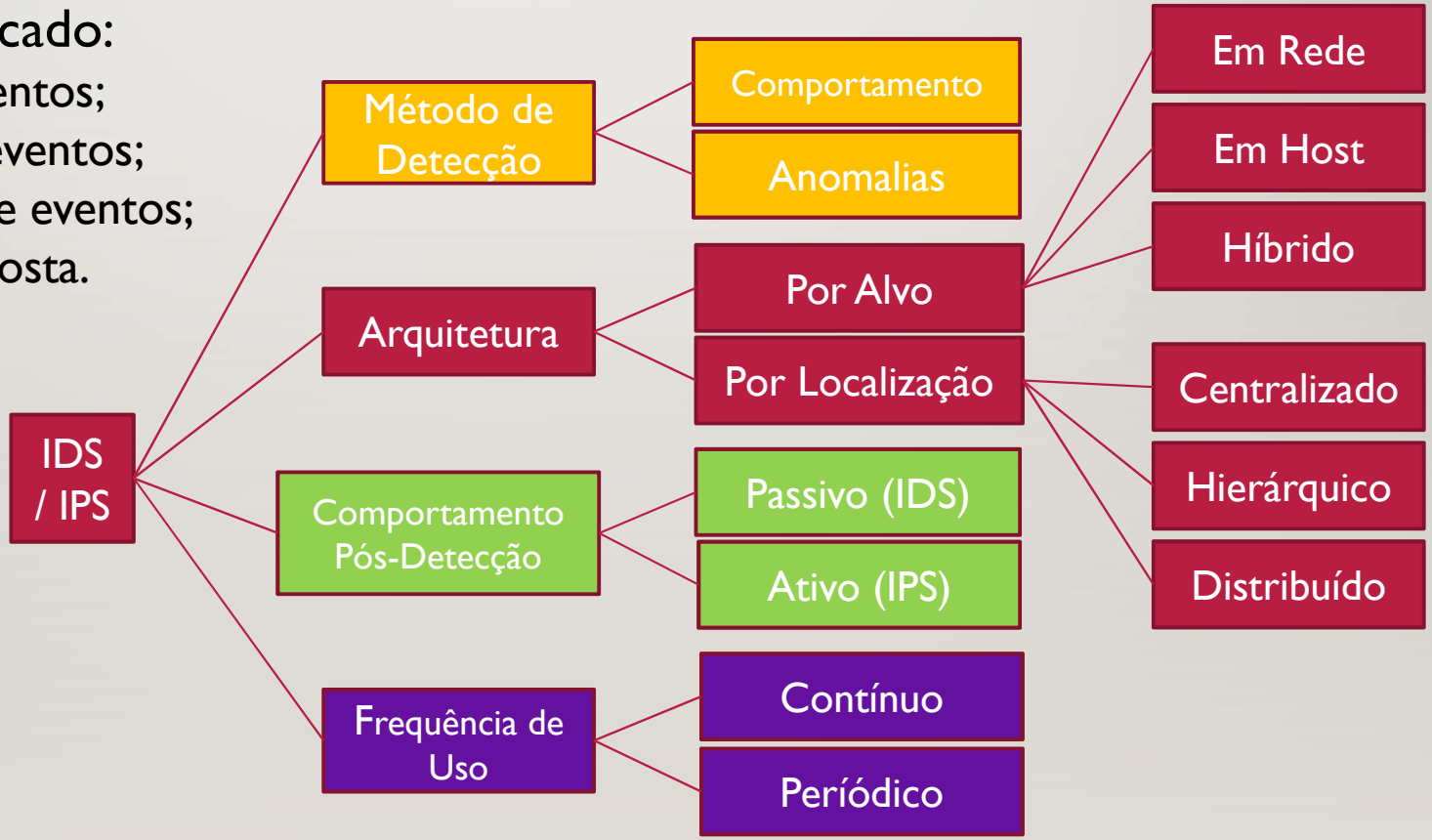


Fonte: KUROSE, J. Redes de computadores e a Internet: uma abordagem top-down/ James F. Kurose, Keith W. Ross ; tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi. – 6. ed. – São Paulo: Pearson Education do Brasil, 2013.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

IDS / IPS

- Os componentes em comum nas soluções de mercado:
  - Geradores de eventos;
  - Analisadores de eventos;
  - Bases de dados de eventos;
  - Unidades de resposta.
- Classificações:



FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

IDS / IPS

- Sistemas IDS/IPS são classificados de modo geral tanto como sistemas baseados em assinatura, ou sistemas baseados em anomalia;
- Um IDS/IPS baseado em assinatura mantém um banco de dados extenso de ataques de assinaturas. Cada assinatura é um conjunto de regras relacionadas a uma atividade de invasão. Uma assinatura pode ser uma lista de características sobre um único pacote (por exemplo, números de portas de origem e destino, tipo de protocolo, e uma sequência de bits em uma carga útil de um pacote), ou estar relacionada a uma série de pacotes;
- Operacionalmente, uma IDS/IPS baseada em assinatura analisa cada pacote que passa, comparando cada um com as assinaturas no banco de dados. Se um pacote (ou uma série deles) corresponder a uma assinatura no banco de dados, o IDS/IPS gera um alerta. O alerta pode ser enviado ao administrador da rede por uma mensagem de correio eletrônico, pode ser enviado ao sistema de gerenciamento da rede, ou pode simplesmente ser registrado para futuras inspeções;

IDS / IPS

- Algumas desvantagens de uso de IDS/IPS baseado em assinaturas:
  - É completamente cego a novos ataques que ainda não foram registrados;
  - Mesmo que uma assinatura combine, isso pode não ser o resultado de um ataque, mas um alarme é gerado (falso positivo);
  - Pelo fato de cada pacote ser comparado com uma extensa coleção de assinaturas, o IDS/IPS fica atarefado com o processamento e deixa de detectar muitos pacotes malignos.

- Um IDS/IPS baseado em anomalias cria um perfil de tráfego enquanto observa o tráfego em operação normal. Ele procura então por fluxos de pacotes que são estatisticamente incomuns;
- Eles não recorrem a conhecimentos prévios de outros ataques, ou seja, potencialmente, eles conseguem detectar novos ataques, que não foram documentados;
- É um problema extremamente desafiador distinguir o tráfego normal de tráfegos estatisticamente incomuns.

IDS / IPS

- O sistema IDS/IPS baseado em host possui as seguintes características:
  - Também conhecidos por HIDS;
  - Dados obtidos na própria máquina;
  - Detecção de ataques relacionados a ações locais;
    - Exemplos: trilhas de auditoria, cópias de arquivos.

- O sistema baseado em rede:
  - Também são conhecidos por NIDS;
  - Analisa dos dados que são retirados da rede;
  - Permite tratar ataques à própria rede;
  - Permite determinar as operações desencadeadas através da rede;
  - Lida com informações como:
    - pacotes de rede (cabeçalhos e dados);
    - estatísticas de tráfego;
    - SNMP.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

IDS / IPS

- Um exemplo de NIDS de código aberto é o SNORT (https://www.snort.org/);
- Baseado em regras que são processadas na análise dos pacotes;
- Modos de operação: (1) Sniffer; (2) Registrador de pacotes; (3) Detecção de intrusos; e (4) Snort Inline, que é um IPS.

- Comparativo:

	HIDS	NIPS
Vantagens	* É específico do host; * Protege host após descriptografia; * Fornece proteção de criptografia em nível de aplicativo.	* É a melhor relação custo-efetividade; * Não é visível na rede; *Independe do Sistema Operacional; *Eventos inferiores ao nível de rede serão vistos.
Desvantagens	*Dependente do Sistema Operacional; * Eventos inferiores ao nível de rede NÃO serão vistos; * O Host é visível para atacantes.	* Não pode examinar o tráfego criptografado; *Não sabe se um ataque foi bem-sucedido.