Sistemas de Detecção de Intrusão

Características

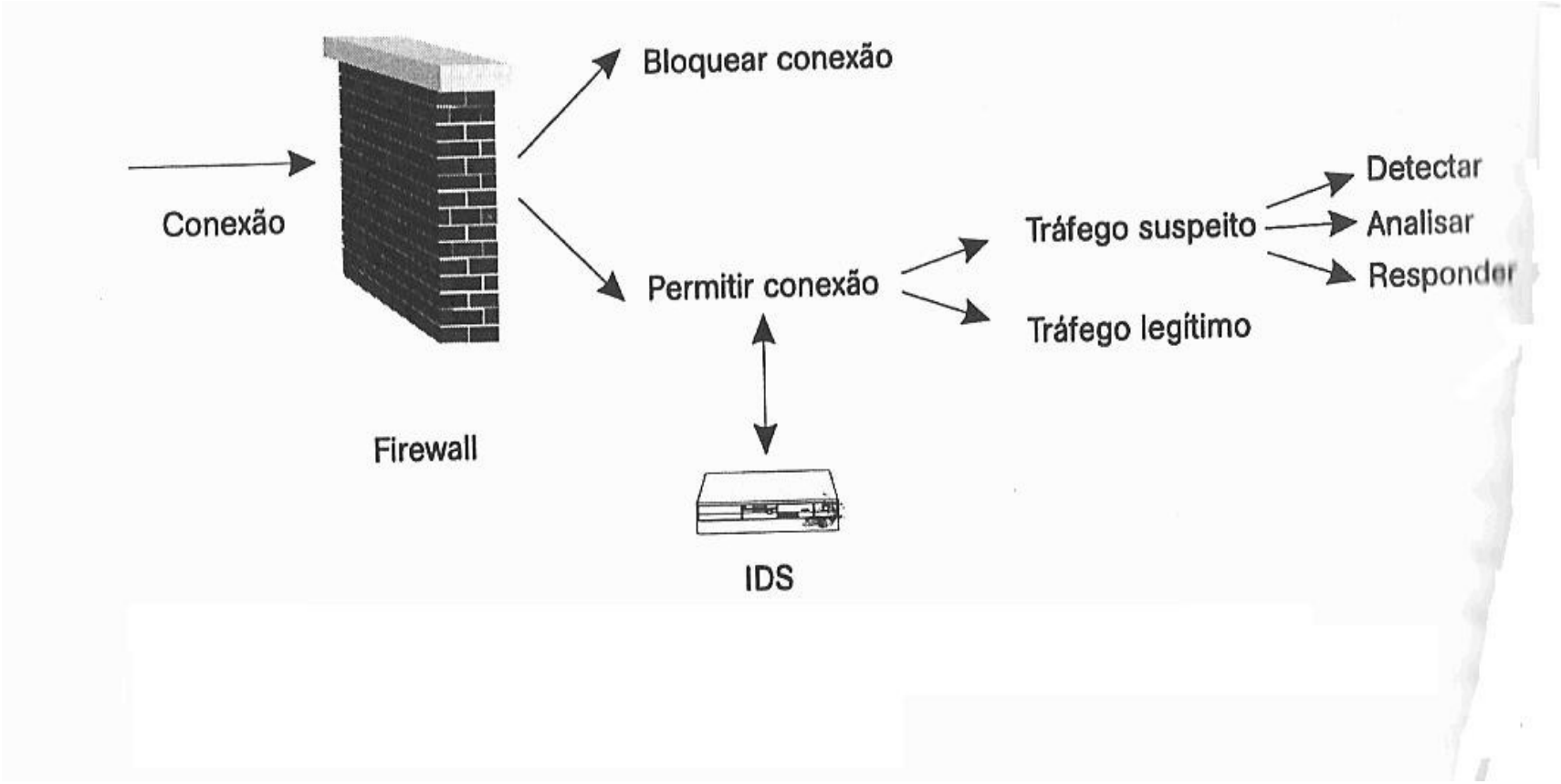
- Funciona como um alarme.
- Detecção com base em algum tipo de conhecimento:
  - Assinaturas de ataques.
  - Aprendizado de uma rede neural.
- Detecção com base em comportamento anômalo.
- IPS: Intrusion Prevention System

Características

- A detecção é realizada com a captura de pacotes, analisando os cabeçalhos e o campo de carga útil dos pacotes, que são comparados com padrões ou assinaturas conhecidas.

- Um IPS tem o objetivo de prevenir os ataques e diminuir a quantidade de alarmes falsos.

Firewall libera conexão e IDS detecta.



Funções do IDS

- Coleta de informações
- Análise de informações
- Armazena informações
- Responde às atividades suspeitas

Tipos

- Tipos de IDS
  - IDS baseado em Host.
  - IDS baseado em Rede.
  - IDS híbrido.
- Tipos de IPS
  - IDS baseado em Host.
  - IDS baseado em Rede.
- Honeypots

HIDS - IDS baseado em Host

- Monitoramento de sistemas (máquinas).
- Tomam as informações nos arquivos de *logs* ou de agentes de auditoria.
- Monitoram acessos e alterações em arquivos do sistema, modificações em privilégios dos usuários, processos do sistema e programas em execução.
- Arquivos corrompidos podem ser *backdoors*.

Exemplos de HIDS

- Tripware
- Swatch
- Portsentry (pode usar o TCP Wrapper)
- Outros

- Obs: TCP Wrapper is a host-based network ACL system, used to filter network access to Internet protocol services run on (Unix-like) operating systems such as Linux or BSD.

Características fortes dos HIDS

- Verificar o sucesso ou falha de um ataque.
- Ataques que ocorrem fisicamente num servidor podem ser detectados.
- Ataques que utilizam criptografia podem não ser notados pelos NIDS, mas descobertos pelos HIDS, pois o SO primeiro decifra os pacotes.
- Independem da topologia da rede.
- Geram poucos “falsos positivos”, que são alarmes falsos de ataques.
- Não necessita de hardware adicional.

Características fracas dos HIDS

- Fica difícil de configurar e gerenciar em todos os hosts de uma rede.
- É dependente do SO. HIDS para Linux é diferente de um HIDS windows.
- Não é capaz de detectar atqques de rede como Smurf.

Obs: The **smurf attack**, named after its exploit program, is a denial-of-service attack that uses spoofed broadcast ping messages to flood a target system.

Características fracas dos HIDS

- Necessita de espaço de armazenamento adicional para os registros do sistema.
- Não têm bom desempenho em sistemas operacionais que geram poucas informações de auditoria.
- Apresenta diminuição do desempenho do host monitorado.

HIDS - IDS baseado em Host

- Acesso a arquivos.
- Integridade de arquivos.
- Varredura de portas
- Modificação e privilégios de usuários.
- Processos do sistema.
- Execução de programas.
- Uso de CPU.
- Conexões.

IDS baseado em Rede

- Monitora o tráfego no segmento de rede.
- Interface de rede atuando no modo prosmícuo.
- Detecção realizada com a captura de pacotes e análise dos cabeçalhos e conteúdos.

Exemplos de NIDS:

- RealSecure,
- NFR,
- Snort

Componentes dos NIDS

- Os sensores que cuidam dos segmentos de redes, fazem a captura, formatação de dados e análise de tráfego.
- Gerenciador: fazem com que os sensores sejam administrados de modo integrado, com a definição dos tipos de resposta para cada tipo de comportamento suspeito detectado.
- A comunicação entre sensores e gerenciador é criptografada.

Características Positivas dos NIDS

- Monitoramento pode ser fornecido por múltiplas plataformas.
- Ataques como: *port scanning*, *IP spoofing*, *SYN flooding* e *Teardrop* podem ser detectados.
- Pode monitorar portas conhecidas como a porta TCP 80 do HTTP.

Características Positivas dos NIDS

- Pode detectar tentativas de ataques (ataques que não tiveram resultados).
- Fica mais difícil um cracker apagar seu rastro.
- Impõe dificuldades para o cracker saber se existe ou não um NIDS.
- Não causa impacto no desempenho da rede.

Características negativas dos NIDS

- Não são capazes de monitorar tráfego cifrado.
- Perda de pacotes em redes saturadas.

Hybrid IDS

- Desvantagens dos HIDS.
- Desvantagens dos NIDS.
- No mundo real, pode-se verificar que a melhor estratégia é utilizar ambos os tipos para a proteção dos recursos da organização.
- Em servidores Web, NIDS são capazes de detectar SYN Flooding, IP spoofing, Teardrop e port scanning, mas somente um HIDS é capaz de detectar um Web defacement (pixação do site).

Honeypots

- Funcionam como armadilhas para os crackers.
- Não contém dados ou informações importantes para a organização.
- Seu único propósito é passar-se por um equipamento legítimo da organização.
- É configurado para interagir como o atacante.
- Detalhes de ataques podem ser capturados e estudados.

Tipos de Honeypots

- Sacrificial Lambs

  Sistemas disponibilizados com sua configuração padrão. Perigo: ser usado como ponto de origem para novos ataques.

Tipos de Honeypots

- Facades

  Emulam serviços, ao invés de diponibilizarem servidores reais.

  Não podem ser usados como pontos de origem para novos ataques.

  Não existem vulnerabilidades nos serviços emulados. Pouca informação sobre ataques.

Tipos de Honeypots

- Instrumental Systems:

  Previne que o sistema seja usado para novos ataques, mas provêem muitas informações sobre eles, mantendo os atacantes interessados no sistema.

Posicionamento dos Honeypots

- **Minefield**
  - Inserido juntamente com os servidores reais de uma DMZ.
  - Parte do princípio que quando um sistema é atacado, ele é usado para descobrir outros
  - Caso o Honeypot seja atacado, as informações sobre o ataque já passam a estar disponíveis.
  - Quando um sistema real é atacado, o honeypot identifica o ataque, assim que o sistema atacado inicie o *scannimg* da rede, para descobrir outros pontos de ataque.

Posicionamento dos Honeypots

- **Shield**
  - Inserido juntamente com os servidores reais de uma DMZ.
  - O Honeypot recebe o tráfego considerado suspeito, baseado nos serviços.
  - O Firewall ou o roteador direciona todo o tráfego não condizente com cada sistema, para o Honeypot, que passa a receber as informações do atacante.
  - Para um servidor Web, recebe todo tráfego HTTP, mas outros tráfegos para esse servidor é direcionado para o Honeypot.

Posicionamento dos Honeypots

- **Honeynet**
  - Inserido juntamente com os servidores reais de DMZs.
  - É uma rede de honeypots.
  - Pode misturar **sacrificial lambs**, **facades** e **instrumental systems**.

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.