SEGURANÇA DA INFORMAÇÃO

IDS e Honeypot

ROTEIRO

- O que é intrusão

- Detecção de Intrusão
  - Componentes de um IDS
  - Tipos de IDS

- Honeypots
  - Motivação
  - O que são honeypots

O QUE É INSTRUSÃO

Ação destinada a comprometer a segurança do alvo

- Confidencialidade
- Integridade
- Disponibilidade de recursos de computação/rede

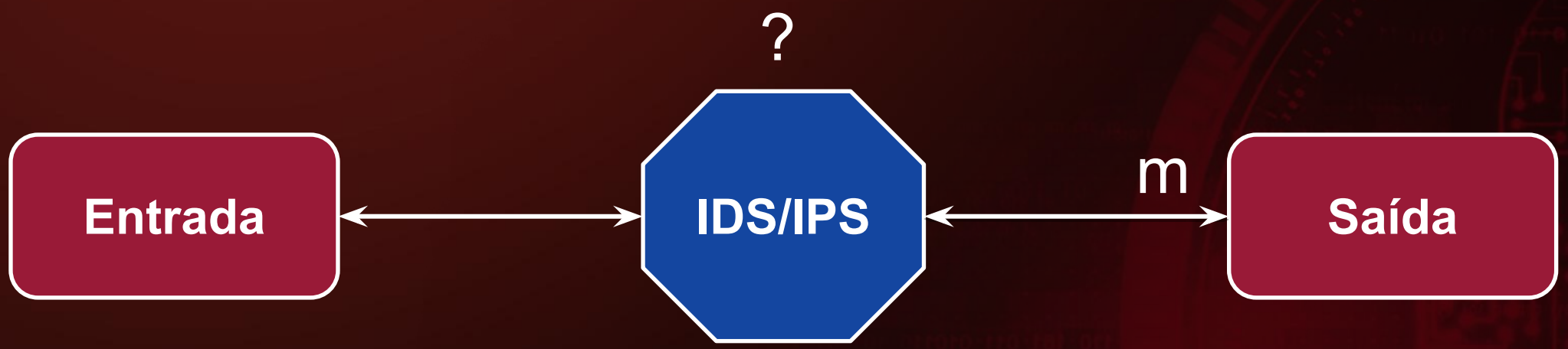
DETECÇÃO DE INTRUSÃO

A identificação através de assinaturas de intrusão e relatório de atividades de intrusão

Prevenção de Intrusão

O processo de detectar atividades de intrusão e gerenciar ações responsivas automáticas em toda a rede

DETECÇÃO DE INTRUSÃO



Para cada mensage m, ou:

- Reporta *m* (IPS: bloqueia ou registra)
- Permite *m*
- Enfileira

DETECÇÃO DE INTRUSÃO

Abordagem

Política x Anomalia

Localização

Rede ou Host

Ação

Detecta ou Previne

DETECÇÃO DE INTRUSÃO

Abordagem

Política

Utiliza regras pré-definidas para detectar ataques

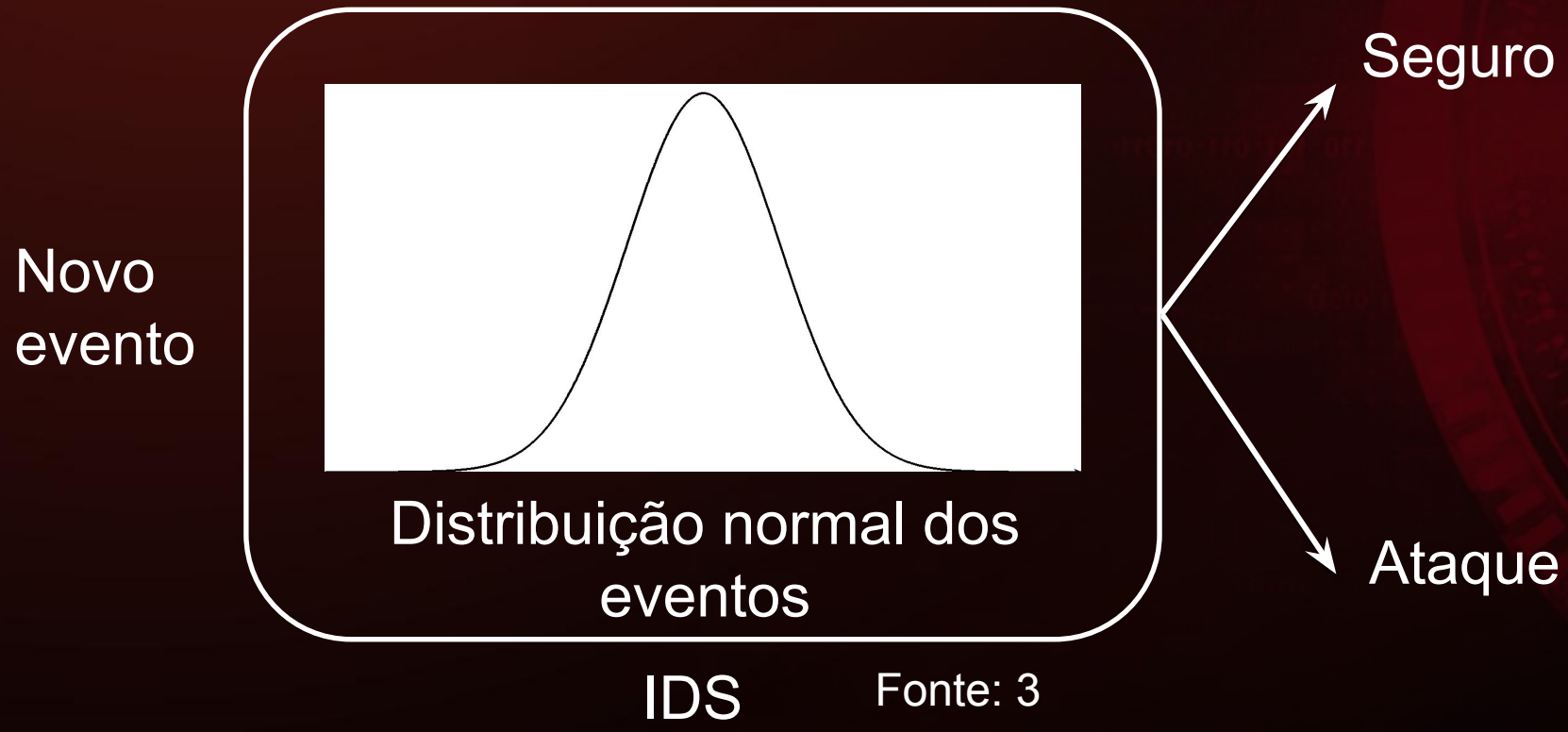
Exemplos:

- Expressões regulares
- Hashes criptografados

DETECÇÃO DE INTRUSÃO

Abordagem

Detecção de Anomalia



Fonte: 3

DETECÇÃO DE INTRUSÃO

ABORDAGEM

Detecção de anomalias

Vantagens

Não requer política pré-determinada (uma ameaça “desconhecida”)

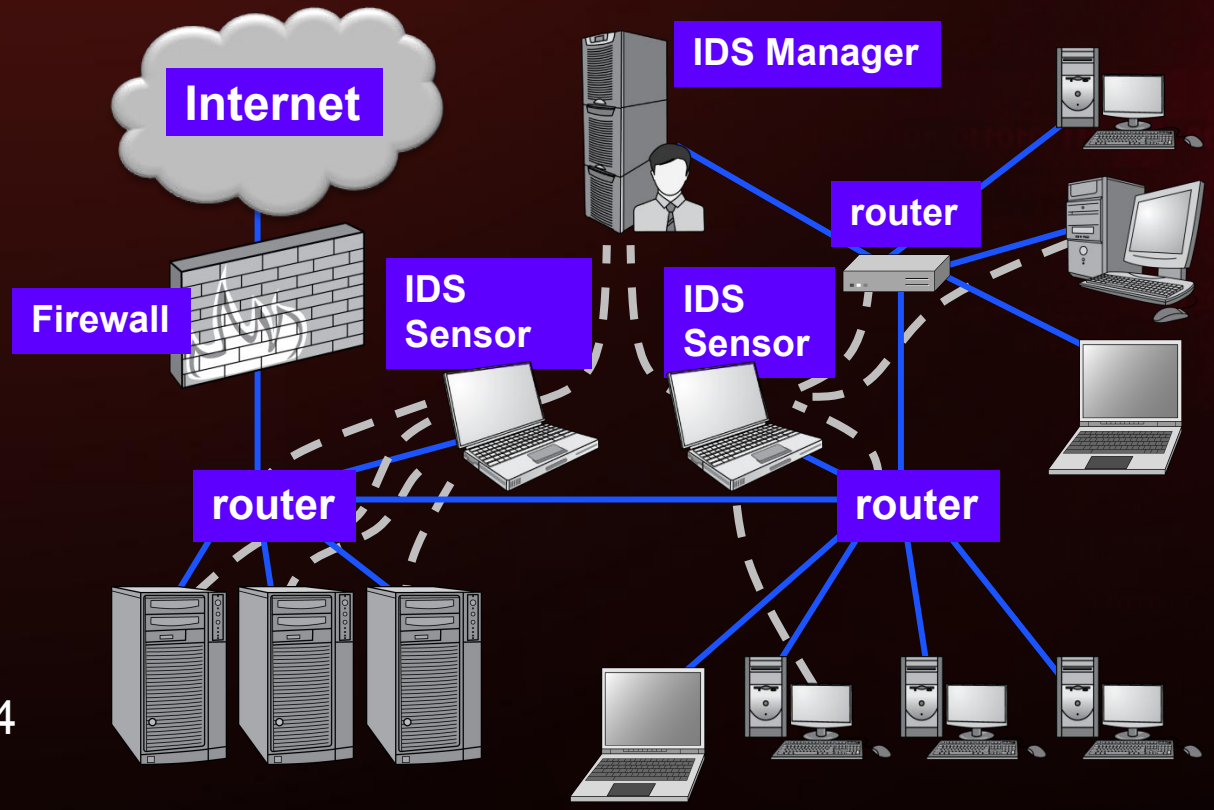
Desvantagens

Alguns ataques não estão fortemente relacionados ao tráfego conhecido
Aprender distribuições é difícil

COMPONENTES DE UM IDS

O gerenciador de IDS compila dados dos sensores IDS para determinar se ocorreu uma intrusão.

Se um gerenciador de IDS detectar uma intrusão, soará um alarme



Fonte: 4

RESULTADOS DE UM ALARME (POSSÍVEL)

Ruim
Ataque Rejeitado

Ruim
Ataque perdido

Fonte: 4

TIPOS DE IDS

BASEADO EM REGRAS

Regras e assinaturas identificam os tipos de ações que correspondem a determinados perfis conhecidos para um ataque de intrusão

Alarme disparado pode indicar qual ataque aciona o alarme

Problema: Não é possível lidar com ataques desconhecidos

TIPOS DE IDS

BASEADO EM ESTATÍSTICA

Representação estatística (perfil) das formas típicas que um usuário age ou um host é usado

Determina quando um usuário ou host está agindo de maneira altamente incomum e anômala.

Alarme quando um usuário ou host se desvia significativamente do perfil armazenado para um usuário ou host

Problema: alta taxa de falsos positivos, não é possível dizer qual ataque aciona o alarme

HONEYPOTS

Motivação

- Segurança é um problema sério
  - Métodos para detecção/proteção/defesa:
    - Firewall (F): O policial de trânsito
    - IDS (I): detecção e alerta

Problemas:

- Ameaças internas (F)
- Programas carregados de vírus (F)
- Falsos positivos e falsos negativos (I)

HoneyNet

- É uma camada adicional de segurança

HONEYPOTS

O QUE SÃO?

Problemas de Segurança

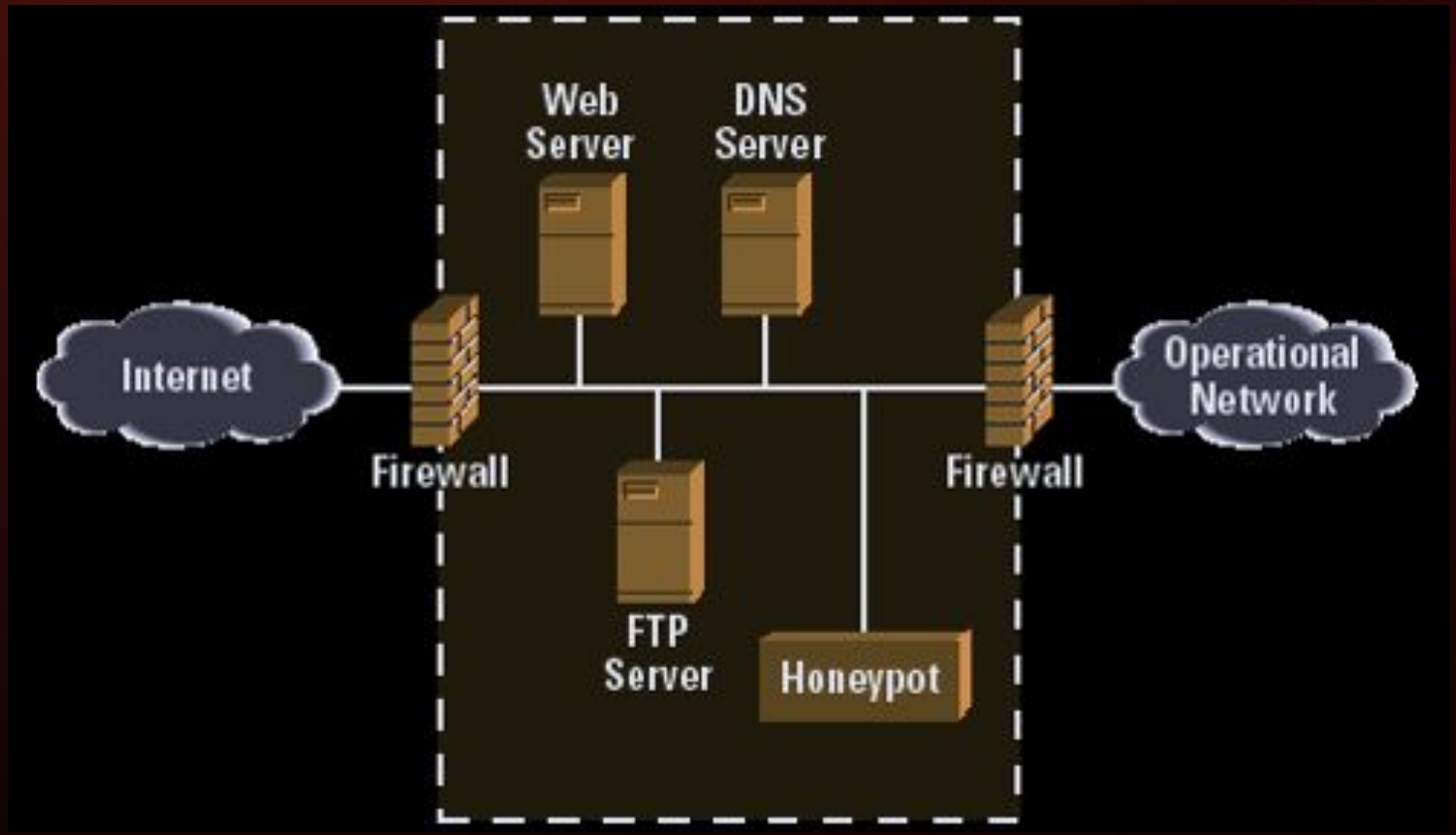
Firewall

IDS

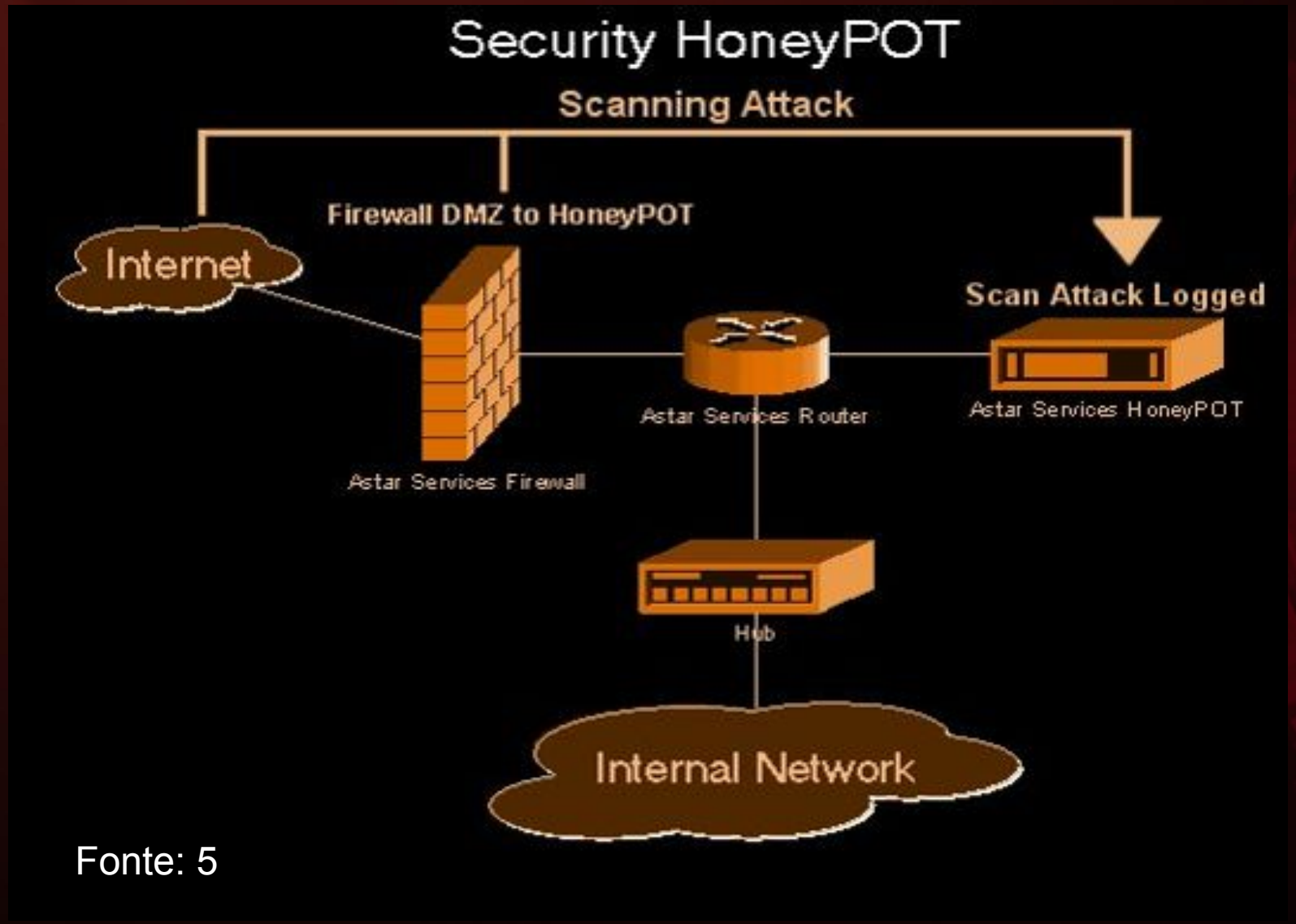
HoneyNets

HONEYPOTS

Um Honeypot é uma técnica de detecção de intrusão usada para estudar os movimentos de hackers



HONEYPOTS



Fonte: 5

HONEYPOTS

Propriedades:

- Captura todos os dados de entrada/saída
- Destinado a ser comprometido
- Sistemas de produção padrão
- Apresenta 3 componentes:

Captura de dados
- Captura furtiva
- Local de armazenamento - longe da honeypot

Controle de dados
- Proteja a rede de honeynets

Análise de Dados

REFERÊNCIAS

1) Honeypots e Honeynets: Definições e Aplicações
2) http://www.honeyd.org/
3) https://users.ece.cmu.edu/~dbrumley/courses/18487-f14/www/
4) http://www.cs.ucf.edu/courses/cis3360/
5) https://en.wikipedia.org/wiki/Honeypot_%28computing%29