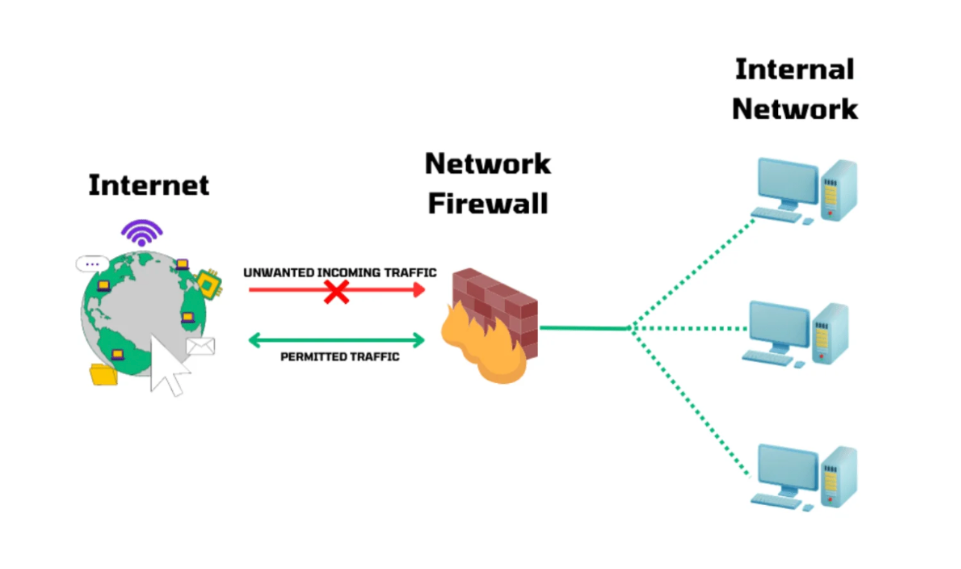


<https://www.msdata.com.br/prevencao-a-fraudes/>



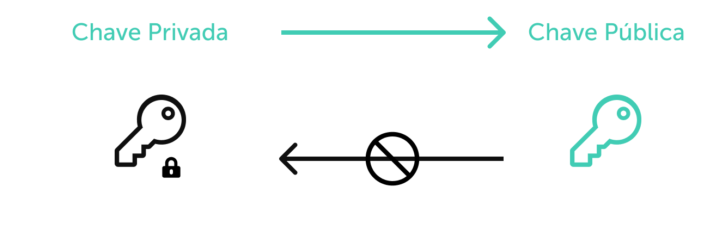
<https://www.enterprisenetworkingplanet.com/security/network-firewall/>



<https://www.itandgeneral.com/snort-official-integrator/>



<https://kinsta.com/pt/base-de-conhecimento/o-que-e-criptografia-de-dados/>



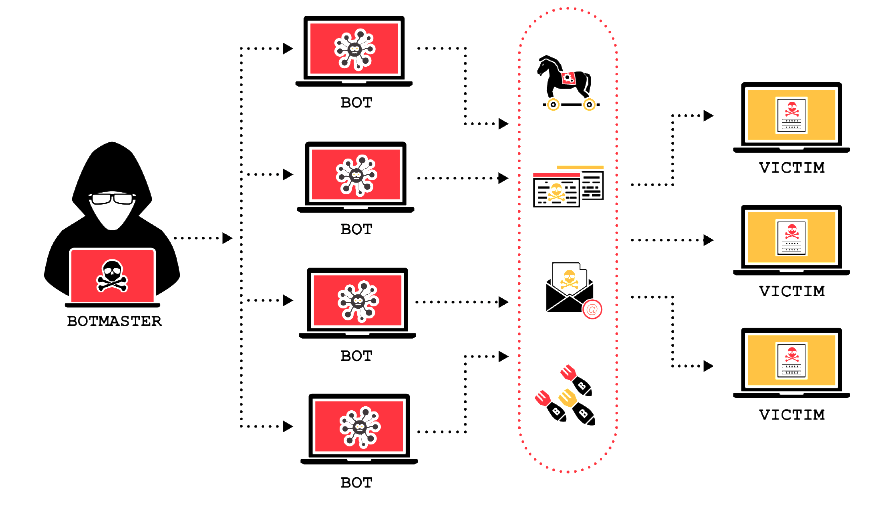
<https://www.ledger.com/pt-br/academy/seguranca/o-que-sao-chaves-publicas-e-chaves-privadas>



<https://dir.indiamart.com/noida/testing-services.html>



<https://tisec.com.br/o-que-e-phishing/>



<https://blog.guardsi.com.br/o-que-e-ataque-ddos/>

# Fontes de infos: Firewalls

## ****Ativos de Rede Focados em Segurança****

Com o aumento das ameaças digitais, entender quais dispositivos usar na defesa da sua rede é essencial.

Ativos de rede focados em segurança são ferramentas críticas como firewalls, IDS/IPS e gateways UTM. Eles ajudam a monitorar, filtrar e proteger sua infraestrutura digital.

### Top 3 Dispositivos Pagos

1. **Firewall Next-Generation – Palo Alto Networks (PA-Series)**
   * **Vantagens:** DPI, App-ID, integração com Threat Intelligence.
   * **Desvantagens:** Alto custo e curva de aprendizado elevada.
   * **Fonte:** Documentação técnica da Palo Alto Networks.
2. **Fortinet FortiGate (UTM)**
   * **Vantagens:** Pacote completo de segurança com boa interface de gestão.
   * **Desvantagens:** Licenciamento complexo e atualizações exigem atenção.
   * **Fonte:** Especificações oficiais da Fortinet.
3. **Cisco Firepower com Snort (IDS/IPS)**
   * **Vantagens:** Detecção/prevenção em tempo real, integração Cisco, regras Snort.
   * **Desvantagens:** Configuração complexa e dependência de conhecimento técnico.
   * **Fonte:** Documentação e guias de produto da Cisco.

### Alternativas Gratuitas

1. **pfSense**
   * **Vantagens:** Gratuito, gerenciável via web, roda em hardware modesto.
   * **Desvantagens:** Interface antiga e dependente de plugins.
   * **Fonte:** Projeto e comunidade pfSense.
2. **Snort (IDS/IPS)**
   * **Vantagens:** Configurável, gratuito, com atualizações da comunidade.
   * **Desvantagens:** Requer uso de CLI e monitoramento ativo.
   * **Fonte:** Projeto e comunidade Snort.

### Conclusão

Com soluções pagas e gratuitas, é possível montar uma defesa eficiente conforme seu orçamento e necessidade. Avalie o cenário e lembre-se: proteger sua rede é um investimento, não um custo.

# ****Fontes de infos: Criptografia****

## O Poder da Criptografia na Segurança Digital

Criptografia é a base da segurança moderna na internet. Desde proteger mensagens privadas até garantir transações bancárias, ela está em praticamente todos os aspectos da nossa vida digital. Seus princípios são **fundamentais na ciência da computação**.

### Como a Criptografia Funciona?

A criptografia transforma dados legíveis em um formato ilegível para qualquer um que não possua a chave correta. Existem dois principais tipos:

* **Criptografia Simétrica:** A mesma chave é usada para criptografar e descriptografar.
  + **Fonte:** Conceito fundamental em criptografia.
* **Criptografia Assimétrica:** Usa um par de chaves: uma pública e outra privada.
  + **Fonte:** Desenvolvida por Diffie e Hellman, popularizada por RSA.

### Aplicações Reais da Criptografia

Você já usou criptografia sem saber! Exemplos:

* **Sites com** https://**:** Utilizam criptografia TLS/SSL.
  + **Fonte:** Padrão IETF (Internet Engineering Task Force).
* **Mensageiros como WhatsApp:** Usam criptografia ponta-a-ponta.
  + **Fonte:** Implementações baseadas em protocolos de segurança como o Signal Protocol.
* **Autenticação de usuários (login):** Muitas vezes envolve criptografia de senhas.
  + **Fonte:** Boas práticas de segurança de dados (NIST).

### Algoritmos Mais Utilizados

* **AES:** Criptografia simétrica de alta performance e segurança.
  + **Fonte:** Padrão NIST FIPS PUB 197.
* **RSA:** Muito utilizado em transmissões seguras de dados.
  + **Fonte:** Algoritmo nomeado em homenagem a Rivest, Shamir e Adleman.
* **SHA:** Embora seja um algoritmo de hash, é vital para integridade de dados.
  + **Fonte:** Família de algoritmos de hash criptográfico publicada pelo NIST.

# Fontes: Pentest

## Pentest: Testando a Segurança Antes que Alguém o Faça

O teste de penetração, conhecido como pentest, é uma simulação controlada de um ataque cibernético. Seu objetivo é identificar vulnerabilidades antes que elas sejam exploradas por criminosos.

### Por Que Fazer um Pentest?

Empresas de todos os tamanhos devem realizar testes de intrusão regularmente para garantir a segurança de seus ativos digitais. Os benefícios incluem:

* Identificação proativa de falhas de segurança;
* Melhoria da postura de segurança da organização;
* Atendimento a requisitos de conformidade (LGPD, ISO, PCI-DSS);
* Redução de riscos e prejuízos com ataques reais.
  + **Fonte:** Boas práticas de segurança cibernética e requisitos de conformidade regulatória (e.g., ISO/IEC 27001, PCI DSS).

### Tipos de Pentest

Existem várias abordagens para realizar um teste de penetração:

* **Caixa Preta (Black Box):** O testador não tem informações internas do sistema. Simula um ataque externo sem conhecimento prévio.
* **Caixa Branca (White Box):** Total conhecimento da infraestrutura e código-fonte. Simula um ataque interno ou realizado por alguém com informações privilegiadas.
* **Caixa Cinza (Gray Box):** Acesso parcial às informações, como credenciais de usuário padrão. É uma abordagem mista.
  + **Fonte:** Metodologias padrão de testes de segurança, como OSSTMM (Open Source Security Testing Methodology Manual) e OWASP Testing Guide.

### Etapas do Processo de Pentest

* **Planejamento:** Definição de escopo, objetivos e regras de engajamento.
* **Reconhecimento:** Coleta de informações públicas sobre o alvo (OSINT).
* **Varredura:** Identificação de portas e serviços ativos, bem como possíveis vulnerabilidades.
* **Exploração:** Uso de técnicas para tentar explorar as vulnerabilidades encontradas e obter acesso.
* **Relatório:** Documentação detalhada das descobertas, incluindo vulnerabilidades, impactos e recomendações para mitigação.
  + **Fonte:** Padrões de teste de penetração (e.g., PTES - Penetration Testing Execution Standard, OWASP Testing Guide).

### Ferramentas Populares para Pentest

* **Burp Suite:** Ferramenta líder para testes de segurança em aplicações web.
  + **Fonte:** Documentação oficial PortSwigger.
* **Metasploit:** Framework open-source para desenvolvimento e execução de exploits.
  + **Fonte:** Projeto Rapid7 Metasploit.
* **Nmap:** Scanner de redes e portas amplamente utilizado para descoberta e auditoria.
  + **Fonte:** Projeto Nmap.
* **OWASP ZAP (Zed Attack Proxy):** Alternativa gratuita e open-source ao Burp Suite para testes de segurança web.
  + **Fonte:** Projeto OWASP.

# Fontes: Ataques

## Segurança na Rede: Conheça os Principais Ataques Cibernéticos

A segurança na rede é essencial para proteger dados pessoais, financeiros e empresariais. Conhecer os principais tipos de ataques é o primeiro passo para se defender eficazmente.

### 1. Phishing

O **phishing** é um ataque em que o invasor se passa por uma entidade confiável, geralmente via e-mail, para enganar o usuário e obter informações sensíveis como senhas ou dados bancários.

* **Exemplo:** E-mails falsos do banco pedindo atualização de dados.
* **Como evitar:** Sempre verifique remetentes e não clique em links suspeitos.
* **Fonte:** OWASP (Open Web Application Security Project) e CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

### 2. Vishing

Semelhante ao phishing, mas feito via **chamadas telefônicas**. O atacante tenta enganar a vítima para revelar informações confidenciais.

* **Exemplo:** Ligações que simulam atendimento bancário.
* **Dica:** Nunca forneça dados pessoais por telefone.
* **Fonte:** Glossários e guias de segurança cibernética (e.g., NIST - National Institute of Standards and Technology).

### 3. Malware

**Malware** é um termo genérico para qualquer software malicioso, como vírus, worms ou trojans, projetado para danificar ou acessar indevidamente sistemas.

* **Forma de infecção:** Downloads, anexos de e-mail, sites comprometidos.
* **Prevenção:** Manter antivírus atualizado e evitar instalações de fontes não confiáveis.
* **Fonte:** Classificações de ameaças cibernéticas (e.g., MITRE ATT&CK, ESET).

### 4. Spyware

Um tipo de **malware** que espiona as atividades do usuário sem seu consentimento, coletando informações como histórico de navegação, senhas e dados bancários.

* **Consequências:** Roubo de identidade, espionagem corporativa.
* **Dica:** Utilize ferramentas de anti-spyware e monitoramento de sistema.
* **Fonte:** Definições de software malicioso e ferramentas de segurança (e.g., Malwarebytes).

### 5. Ataque DDoS

**Distributed Denial of Service (DDoS)** é um ataque que visa sobrecarregar um servidor ou rede, tornando um serviço indisponível para usuários legítimos.

* **Alvo comum:** Sites de empresas, serviços financeiros, plataformas de jogos.
* **Defesa:** Uso de firewalls, balanceamento de carga e soluções anti-DDoS.
* **Fonte:** Cloudflare e Akamai (empresas especializadas em mitigação de DDoS).