# Sinais e Ações em Caso de Ataque DDoS

⚠️ Sinais comuns de um ataque DDoS  
  
1. Alta carga repentina da CPU  
Exemplo: CPU / 95% com system: 70% ou iowait alto.  
Comportamento: Muitos processos ou pacotes inundam a máquina, forçando o kernel a responder sem parar.  
  
2. Aumento do load average  
Em uma máquina com 4 núcleos:  
LOAD 1 min: 8.5 = muito acima do limite saudável.  
Isso pode indicar que há mais processos aguardando CPU do que o sistema consegue atender.  
  
3. Uso de memória anormal  
MEM - 90%, mesmo com poucos processos ativos.  
Pode ser causado por processos criados em massa (fork bomb ou ataque de aplicação).  
  
4. Alto número de conexões de rede (especialmente SYN ou UDP)  
Ver com:  
netstat -an | grep :80 | wc -l  
ss -s  
Ou:  
sudo netstat -anp | grep SYN\_RECV  
  
5. Picos no tráfego de rede  
Monitorar com ferramentas como:  
- iftop (visualização em tempo real)  
- vnstat (histórico de tráfego)  
- nload  
Exemplo de pico: Entrada de 100 Mbps em uma máquina que normalmente recebe 2 Mbps.  
  
6. Muitos context switches (ctx\_sw) ou interrupções (inter)  
Se ctx\_sw: 50K ou inter: 20000+, é um sinal de que o sistema está lidando com muitos eventos — comum durante DDoS.  
  
7. Serviços lentos ou indisponíveis  
Acesso a páginas da web, API, SSH, etc. fica lento ou para completamente.  
  
🔧 Ferramentas para detectar DDoS em tempo real  
  
Ferramenta Comando O que faz  
iftop sudo iftop Mostra conexões de rede em tempo real  
nethogs sudo nethogs Mostra uso de banda por processo  
ss ss -ant Verifica conexões TCP abertas  
netstat netstat -an | grep :80 Mostra conexões à porta 80  
top / htop htop Ver uso de CPU/memória por processo  
tcpdump sudo tcpdump -n port 80 Analisa tráfego específico  
  
🛡️ Como agir se estiver sofrendo DDoS  
  
Bloqueie IPs suspeitos  
Exemplo:  
sudo iptables -A INPUT -s 123.45.67.89 -j DROP  
  
Limite o número de conexões  
Com iptables:  
sudo iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 30 -j DROP  
  
Use firewall e rate limiting  
Configure fail2ban, ufw, ou regras no nginx/apache para bloquear IPs com muitos acessos.  
  
Mitigação em camada superior  
Se estiver na web: use serviços como Cloudflare, Imperva, AWS Shield, etc., para filtrar o tráfego antes de chegar no seu servidor.