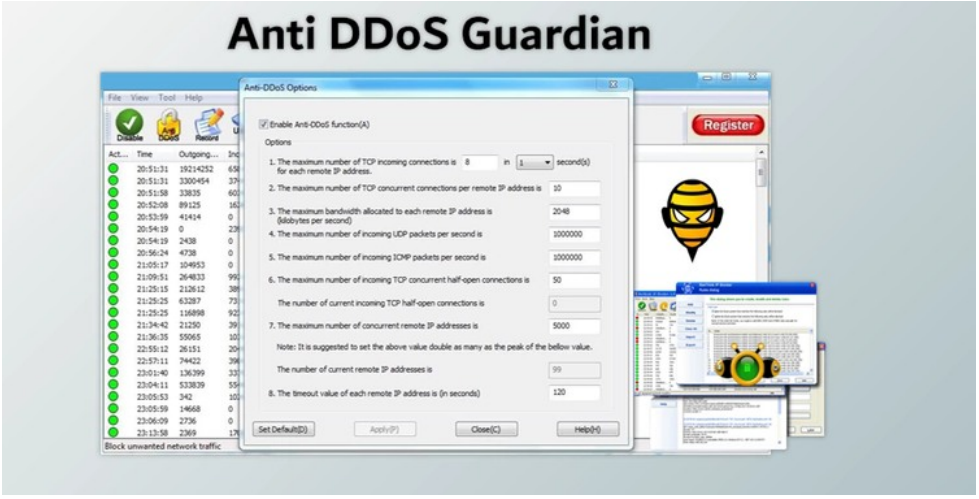
Anti DDoS Guardian v6.1 (12 Mar 2023) for Win

2025-01-22 01:54:20



Secure the security of your Windows server from advanced DDoS attacks. Eliminate applications layer (L7) DDoS attacks, UDP floods, TCP SYN flooding, RDP Password brute force attacks, slow HTTP Attacks on Get&Post, and much more—reputation by thousands of network professionals as well as security experts.

Anti-DDoS Guardian is DDoS mitigation software installed on Windows servers. It is part of the TCP/IP stack and offers comprehensive DDoS security on Internet servers. The Anti-DDoS Guardian monitors and blocks any suspicious activity on the network in real-time. The new version includes support for Windows 11 and Windows Server 2022.

A DDoS attack indicates that many illegal computer systems are connecting to servers on the internet at the same simultaneously, and the massive volume of traffic that is incoming causes servers not to be able to handle legitimate users.

Anti-DDoS software is installed on Internet servers to prevent DDoS attacks. Anti-DoS software works on different network layers to detect illegal traffic and mitigate attacks. Since it is software, it is flexible and configurable. Please click here to learn more about Anti DDoS software.

Internet servers need to provide additional protection on top of CDN DDoS protection. CDNs are very effective against large-scale attacks targeting the physical layer. However, when DDoS attacks involve the application layer, Anti DDoS software performs better. You can easily manage network traffic and control TCP connections with Anti DDoS software. On top of that, Anti DDoS software often saves money.

Application layer DDoS attacks are launched by multiple clients attacking the TCP/IP application layer of the server. The intention is to consume the server's resources for TCP/IP at a low cost by having excessive TCP connections. There is a limit on simultaneous TCP connections that can be made per Internet server Users may send numerous TCP connection requests to surpass the server's TCP connection limit without even a single connection being completed. It's as if too many fake customers arrive at the restaurant without making a reservation, and they sit in the restaurant and stand around waiting. So, it's impossible to service real customers. A criminal's goals are achievable in a small quantity using a tiny amount of computers. This is why application layer DDoS attacks are highly effective, cost-effective, and challenging to spot. The application layer DDoS attacks may also be described as"layer 7" (L7) attacks.

Anti-DDoS Guardian thwarts applications layer (L7) DDoS attacks by restricting how many concurrent TCP connections per user. If a client attempts to connect to a server with more than TCP connections, the client will be denied access. Learn more about how Anti-DDoS Guardian stops layer seven and application layer DDoS attacks.

The most effective application-level DDoS mitigation tool available.Block Layer 7 (L7) DDoS attacks, low and slow attacks, slow Loris attacks, a slow HTTP test POST and GET floods, Windows Remote Desktop brute force password attacks, and much more.

Monitor traffic on the network as well as TCP connections in real time. Advanced rate limits are available for client simultaneous TCP connection, TCP connectivity rate, UDP rate, and bandwidth.

There is no lag, and the system is robust and robust and. It runs smoothly for months without losing performance. It's lighter than ever before, with only 2 MB.

- Network flow and TCP connection management.
- Real-time DDoS/DoS monitor
- Support white list
- Support programming interface to import IP blocking list from third-party applications
- TCP half-open connection control.
- UDP flow control.

所有软件资源 100%安全 已检测 无病毒 无篡改
去预览

标签

Tools Applications

- Block unwanted country IP addresses.

版本列表

Anti DDoS Guardian v6.1 (12 Mar 2023) for Win

苏ICP备19032038号 Powered by getShopSys