NimbusDDOS

ARTICLE :

Features of the NimbusDDOS Platform

How does NimbusDDOS help protect businesses from DDoS attacks? One critical component of the strategy we build for our clients is using simulated DDoS attacks. These attacks allow the NimbusDDOS team to identify risk areas in the client's system so we can craft a DDoS attack prevention strategy.

The way NimbusDDOS launches these attacks is through our proprietary DDoS attack platform. This platform has been specially designed to simulate real-world DDoS attacks. In fact, our simulated attacks are real - although strategic and highly controlled.

Let's explore the components of the NimbusDDOS attack platform and how it can help identify DDoS attack risk areas in your company's infrastructure.

Accurate Traffic Sources
DDoS attacks are all about traffic. Generating an accurate amount of traffic at the correct rate is essential to simulating an authentic attack.

- Infinite scaling. A DDoS attack often involves an excessive number of requests to your environment which overwhelms it. As modern DDoS attacks can reach 2+ Tbps, a powerful scaling method is required. NimbusDDOS uses public cloud resources to achieve a scale capable of properly testing any size environment.

- Globally distributed. DDoS attacks can originate from anywhere in the world. By leveraging public cloud resources, traffic can be sourced from numerous continents, including North America, South America, Europe and Asia. Clients that operate in a BGP anycast or multi-datacenter active-active configuration are especially in need of this type of international testing.

- Consistency in traffic delivery. Traffic needs to be delivered in a consistent manner to allow for accurate data analysis and avoid testing side effects. In order to do this, the NimbusDDOS attack simulation platform uses an active feedback control system. The active feedback helps the system to know how much traffic is being delivered, and how to adjust delivery based on the needs of the simulated attack.

NimbusDDOS

Safety Mechanisms

Because the simulated attacks created by the NimbusDDOS platform are real, and often performed in the client's production environment, the need for the failsafe of an emergency shutdown is critical. NimbusDDOS uses both in-band and out-of-band mechanisms for the shutdown.

Both methods allow an attack of any size to be halted within one minute. As a result, both NimbusDDOS experts and clients can have peace of mind that the simulation is completely under control.

Metrics Visualization

NimbusDDOS created our own user portal to view real-time data collected during a simulated DDoS attack. This data is critical for conducting the simulation in real time, as NimbusDDOS experts can observe the data and suggest alterations to a client's defenses while the test is ongoing.

Further, the data is available for review after the simulation. This data can then be used to help craft a DDoS attack strategy that is personalized to the client's specific environment and IT response team.

Try the NimbusDDOS Platform Yourself

Would you like to see how NimbusDDOS can identify ways to better protect your system from DDoS attacks? To learn more or schedule a consultation, contact NimbusDDOS or call (800) 674-DDOS.