NimbusDDOS

ARTICLE :

# Why DDoS Testing is Critical to DDoS Protection

Enterprises face a myriad of cyber threats daily. Today, one of the most damaging cyberattacks is the distributed denial of service (DDoS) attack. Cybercriminals execute DDoS attacks by making your server, network, website, or cloud service unusable by bombarding it with a massive volume of requests with the intention of overwhelming the target. In doing so, they block legitimate traffic and effectively deny people access to your service. The motive of DDoS attacks is often extortion - pushing companies to pay a ransom to withdraw the attack. But sometimes they are driven by revenge or hacktivism. That's why DDoS protection is increasingly becoming a necessity for every organization.

**Why Test Your DDoS Protection?**

Although DDoS attacks on larger organizations, like banks, are the ones that attract widespread attention, any business that relies on connected resources and the cloud is a potential target. DDoS protection is something that every business must take seriously to avoid financial losses and reputation damages that accompany successful attacks. Testing your DDoS mitigation makes a lot of sense when your business relies heavily on e-commerce, websites, and other online applications. If you must maintain a 24/7 online presence, DDoS testing is essential. Here are the reasons you should periodically test your DDoS protection solution:

**1. To Ensure Your Mitigation Solution is Working Properly**

DDoS hardware solutions work well when configured properly, but they can be susceptible to misconfiguration. Similarly, cloud mitigation works if the alerting is timely and filters have been properly configured by the vendor. A DDoS test will help you understand how well your mitigation solution can handle various DDoS attacks. The test involves simulations of real-world DDoS attacks on your IT systems in a controlled and pre-scheduled manner. DDoS testing gives you an insight into your infrastructure capabilities and whether your DDoS protection is functioning as expected. You also get mitigation advice and remedies on how to strengthen your DDoS mitigation solution.

**2. To Help You Recognize Attacks**

Not all DDoS attacks are easy to spot. Although volumetric DDoS attacks (for example stuffing 2 Gbps on a 1 Gbps internet circuit) are easy to identify, a significant portion of DDoS techniques don't involve massive amounts of data. These low and slow attacks (such as protocol and application layer attacks) can slip through common defenses since they are designed to mimic normal user or application behavior. DDoS testing helps you identify areas in which the mitigation solution may be deficient, and improve configurations for low and slow DDoS attacks.

**3. To Optimize Processes and Procedure**

Another critical importance of DDoS testing is to make sure your mitigation procedures are working instead of discovering deficiencies in the procedure during a real-world attack. DDoS testing is an integral part of "security as a process". When investing in mitigation processes, it's critical to ensure they are working; otherwise, you'll be spending money on something that does not fulfill your business requirements.

NimbusDDOS

**4. To Provide a Training Opportunity for Incident Response Teams**
The best technology and processes often fail due to inadequate training of incident response team members. A real-world DDoS attack will often identify gaps in training that might not be apparent during synthetic "table-top" exercises or classroom training.

**5. To Ensure That Your Cloud Mitigation Provider Meets SLAs**
Without formal DDoS testing, the only way to ensure that a cloud mitigation vendor is achieving their SLA is to wait for a real-world DDoS attack and measure their performance. This is a significant problem for enterprises as it makes DDoS defenses reactive rather than proactive. Formal DDoS testing allows enterprises to periodically assess the SLA performance of their vendor on a schedule that is in-line with regulatory requirements and business best practices.

**6. To Know How Much Traffic Your Website and Cloud Applications Can Handle**
Cloud applications and web servers have a finite capacity. You want to know how much traffic your network can handle before it breaks down. DDoS testing, specifically application layer DDoS tests, can function in much the same way as a traditional load test. Unlike a typical load test, that tests normal behavior, a DDoS test looks at less common traffic patterns and is more effective at identifying architectural bottlenecks.

**7. To Identify What Part of Your Network is Vulnerable to DDoS attacks**
DDoS attacks may target any area of the infrastructure including application servers, DNS servers, firewalls, routers, and internet bandwidth. DDoS testing professionals employ a coordinated group of botnet nodes to send traffic to the target in a bid to bring the system to its knees. The test will help you pinpoint your network's vulnerable components and allow intelligent investment in the right DDoS protection tools.

**Summary**
DDoS testing isn't just about testing your network infrastructure for vulnerabilities. It also serves as a drill to ensure that you have the right personnel and processes in place in case of a DDoS attack. Our DDoS Testing Service will help you identify deficiencies in your mitigation programs and recommend effective solutions. If you are looking to test your company's ability to withstand DDoS attacks, contact us today and speak with one of our DDoS engineers.