ixia
A Keysight Business

WHITE PAPER

QUICK GUIDE: SIMULATING A DDoS ATTACK IN YOUR OWN LAB

DDoS attacks are a big risk to any business with an online presence. Even a basic test of a DDoS attack can help you discover critical data, including how many packets are dropped by your DDoS mitigation solution, how your mitigation solution actually functions in a real attack, what level of service you are able to provide while under attack, and how your people and process react to and withstand an attack.

In this guide we present three options for simulating a DDoS attack in your own lab:

- **Tier 1**—Simulating a basic attack using open-source software and readily available computing resources
- **Tier 2**—Simulating a more complex single-link attack using professional network testing software—Ixia BreakingPoint Virtual Edition
- **Tier 3**—Simulating a high-speed, multi-site attack between 10 Gbps and 960 Gbps using Ixia's PerfectStorm hardware, which can simulate traffic from up to millions of attacking computers

DDoS ATTACKS ARE A BIG RISK TO ANY BUSINESS WITH AN ONLINE PRESENCE.

ixia
A Keysight Business

TIER 1—SIMULATING A BASIC DDoS ATTACK WITH OFF-THE-SHELF TOOLS

As we will show in this section, it is possible, with some effort, to simulate a basic DDoS attack on your network and see how your defenses hold up. However, this test will be very limited in scale and the types of attack traffic used. It will only give you a taste of how to prepare for a real Internet-scale attack.

Warning: In this section we will use an open source tool called Kali Linux to create a simplified simulation of a DDoS attack. This tool is sometimes used by hackers to carry out real DDoS attacks. Our intention in presenting this information is to help IT personnel safeguard their companies from attack. Please use it responsibly and at your own risk, and be sure to direct your simulated attack at test equipment or networks only.

Attack Configuration

We will use the open source Kali Linux tool to simulate a simple attack—a SYN Flood. This involves hitting your target server with a large number of SYN packets and seeing how it affects your user experience. We will be limited to a low-volume attack because you probably have only a few computers available in your lab to carry out the test. If you have access to a public cloud like Amazon EC2, you could spin up a few more virtual machines to increase the effect of the simulated attack.

We recommend you target the attack against a realistic staging environment that is as similar as possible to your production system.

Attack volume: Five computers, starting from 50,000 SYN Packets per second, and increasing gradually.

How to Simulate the Attack—SYN Flood

1. Before you start the DDoS attack, simulate some “good” users. You can use a load testing tool such as Load Impact. Emulate some basic user behavior with a similar number of users to what you would expect in your production environment.

2. If you have a DDoS mitigation solution, set it up for your staging environment so you can test responses when the attack occurs.

THIS TEST WILL BE VERY LIMITED IN SCALE AND THE TYPES OF ATTACK TRAFFIC USED. IT WILL ONLY GIVE YOU A TASTE OF HOW TO PREPARE FOR A REAL INTERNET-SCALE ATTACK.

3. Install the open source Kali Linux on five machines in your lab. You will need to use Linux machines and have root permission on the current user.

4. On each of the computers, run the following command:

```
$ sudo hping3 -i u20 -S -p 80 -c 50000 192.x.x.x
```

`-S` specifies sending SYN packets

`-p 80` targets port 80

`-i u20` waits 20 microseconds between packets = 50,000 packets per second

You should see output similar to this:

```
HPING 192.x.x.x (eth0 192.168.1.1): S set, 40 headers
+ 0 data bytes
```

```
--- 192.x.x.x hping statistic ---

50000 packets transmitted, 0 packets received, 100%
packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms
```

5. Every few minutes, move between the five computers, use Control-Z to unbind the port and step up the rate of packets by modifying the -i ux flag, decreasing x each time by 2. This will increase packets by a bit more than 5,000 packets per second in each iteration.

6. While the simulated attack is going on, monitor your regular user experience metrics. These might be page load time, latency of transactions, number of transactions completed, etc. Of course the metric tested should be in sync with the user behavior you are simulating in your load test.

What Can You Learn?

After running an attack like the above and measuring your operational metrics, you will know what to expect in a low-volume DDoS attack. This is a “lower threshold” test of how your defenses hold up to a basic attack.

ixia
A Keysight Business

LIMITATIONS OF THE BASIC IN-HOUSE TEST

1. Your load test is not a realistic test of user traffic, which includes external users of different types, internal users and more—you cannot know for sure how real users will be affected.

2. It is complex to simulate multi-faceted attacks like in the full-fledged battle exercise we presented in our DDoS simulation page.

3. Most importantly—in your lab you cannot simulate a large scale attack. Real attacks can involve thousands or even millions of infected machines hitting your network with traffic.

To really test your setup and the claims of DDoS mitigation services, you need to simulate a high volume attack—this might require thousands or millions of PCs—and a realistic mix of attack and user traffic.

BREAKINGPOINT CAN SIMULATE DDoS ATTACKS, AND HAS MUCH MORE POWERFUL CAPABILITIES THAN OPEN SOURCE TOOLS.

TIER 2—REALISTIC ATTACK SIMULATION WITH PROFESSIONAL NETWORK TESTING SOFTWARE: BREAKINGPOINT VIRTUAL EDITION

Ixia's BreakingPoint Virtual Edition is an award-winning software product deployed at some of the world's largest enterprises. It provides scalable real-world application and threat simulation, using virtualized computing resources in your own lab. BreakingPoint can simulate DDoS attacks, and has much more powerful capabilities than open source tools:

- Virtualizes your lab hardware to create a unified resource for launching test attacks.
- Simulates real-world applications for testing "positive" traffic—all popular application protocols, social media, P2P, gaming, enterprise applications, and more.
- Simulates real attack patterns - 36,000+ security strikes, 6,000+ recorded security attacks, and 100+ evasion techniques commonly used by hackers.

How it Works: Simulating DDoS with BreakingPoint

BreakingPoint includes an easy-to-use software lab that can generate many different types of DDoS traffic.

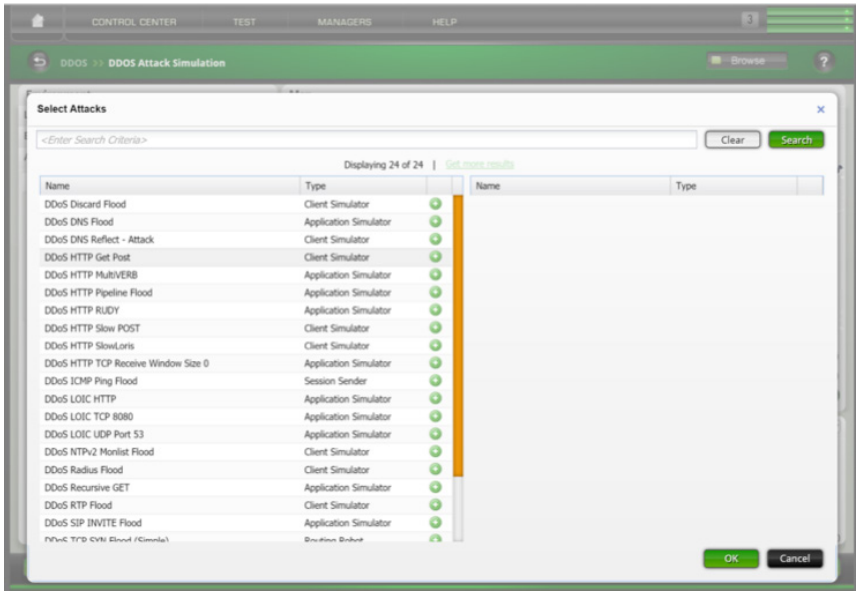
The lab interface shows a **Lab Topology** for your network, and a map to simulate where the attacks are coming from and going to.

This is supported by Ixia's Application Threat Intelligence (ATI) subscription, which provides the geography of every IPv4 address—allowing you to simulate user traffic and attack traffic from different countries and territories. ATI also provides the ability to simulate traffic from the latest applications (such as Facebook, Instagram, and NetFlix).

At the bottom is a timeline. The green bar represents your valid traffic and the red represents simulated DDoS traffic.

You can change the **Background Traffic** (simulated valid user traffic) to any mix of applications you desire. ATI supports an unlimited number of traffic combinations to match any existing network.

You can then set up your **Attack Traffic**. With the ATI subscription, you gain access to over 36,000 different attacks, including a large variety of DDoS attacks. It is also possible to combine DDoS with other types of attacks, as is often the case in real life.



While BreakingPoint VE will probably suit the needs of most small to medium enterprises, organizations with network bandwidth greater than 10GB will want to leverage Ixia's PerfectStorm hardware, which can simulate attacks at Internet scale.

Want to experience the power of BreakingPoint?

Schedule a demo

ixia
A Keysight Business

TIER 3—SIMULATING A FULL SCALE DDoS ATTACK WITH BREAKINGPOINT + PERFECTSTORM HARDWARE

PerfectStorm is the hardware companion to BreakingPoint, able to generate large volumes of traffic, starting from 10Gbps and going up incrementally to the full power of 960Gbps. That is more than twice as much bandwidth as the biggest DDoS attack in recorded history (as of March 2016).

ONE BOX THAT CAN SIMULATE THE POWER OF THE ENTIRE INTERNET.

At its largest scale, PerfectStorm can generate up to 720 million concurrent connections, new TCP connection rates of up to 24 million, and massive encryption with up to 240Gbps of SSL traffic and 480Gbps of IPsec traffic per system. It is one box that can simulate the power of the entire Internet.

With BreakingPoint, as described in Tier 2 above, running on top of PerfectStorm hardware, you can not only realistically simulate an attack, but do so at realistic scale (between 10-960Gbps, depending on how far you choose to scale the hardware). This can be a true test of how your systems and defenses will hold up to a DDoS attack.

Testing Your Breaking Point

With this full setup, you can test how far your system can go under attack, and ensure you are really prepared for an attack no matter how large.

Even with an effective mitigation strategy in place, it is highly likely users will be affected by a DDoS attack. The question is, by

how much and can you continue to do business while an attack is going on? Or, if not, what is the expected damage?

By carrying out realistic tests with Ixia's hardware-software combination, you can see under what scale of attack your infrastructure completely shuts down, and what is the maximum attack you can withstand. You can also identify a minimum threshold of user experience which allows you to continue operating—and test which scale of attack takes you below that minimum threshold.

This kind of exercise can provide invaluable information for security teams, IT management, and business management, helping them understand what to expect in case of an attack—and to what extent the mitigation strategy can protect the business.

Learn about full-scale DDoS testing with BreakingPoint and PerfectStorm.

Schedule a demo

IXIA WORLDWIDE
26601 W. AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 1.818.871.1805

WWW.IXIACOM.COM

IXIA EUROPE
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127