WHITE PAPER

# QUICK GUIDE: IXIA'S FOUR-STEP DDoS MITIGATION PROCESS

## FIRST STEP: PICK YOUR WEAPON

Here's what you should look at when choosing your distributed denial of service (DDoS) mitigation technology:

- **On premises/in the cloud** – With attacks growing larger and becoming more complex, the dilemma facing many organizations is whether to deploy on-premises DDoS protection or subscribe to a cloud-based provider. Purpose-built defense solutions are deployed on premises, between the Internet and your network core. Deployed at the edge of your network, these tools offer real-time defense with complete and sophisticated visibility into DDoS security events. Cloud-based DDoS mitigation service, on the other hand, is most often utilized as an on-demand option for large-scale attacks. A recent report by SANS Institute stated: "DDoS mitigation solutions integrating on-premises equipment and ISP and/or mitigation architectures are nearly four times more prevalent than on-premises or services-only solutions."

LOOK INTO CLOUD-BASED TOOLS THAT OPERATE AT LARGE SCALE, SO THEY CAN ROUTE EVEN A MASSIVE AMOUNT OF DDoS TRAFFIC TO A NETWORK OF CLOUD-BASED MACHINES.

- **Attack volume** – What scale of attack is the tool or service capable of stopping? These days, the measure is in tens or hundreds of gigabytes per second of malicious traffic. The group calling itself New World Hacking recently claimed responsibility for taking down British Broadcasting Corporation's (BBC's) global website with a DDoS attack of allegedly reaching 602 Gbps. If the attack size is proven true, it would vastly surpass the largest DDoS attack record of 334 Gbps, recorded by Arbor Networks in 2015.
- **Impact on legitimate transactions** – While the DDoS attack is going on, what will happen to your site's visitors? The best result is for users to continue working as usual without even noticing that an attack is going on. For larger-scale attacks this will not be possible—users will be affected. But knowing what level of service you will be able to provide to your users and to how many users while under attack is critical.
- **Cost model** – Many DDoS services are priced based on bandwidth protected. If you are paying for 100 Gbps protection, and the attack scales up to 300 Gbps, you must decide if and how much you are willing to pay for the extra coverage. Try to anticipate your cost structure based on realistic assumptions of attack size.
- **False positives** – One of the most significant issues related to DDoS mitigation is the false positive. This is something every DDoS protection cloud service and vendor has to pay close attention to. A false positive is when a legitimate user triggers the protection system, and in response, that user is flagged as an attacker. False positives appear during DDoS mitigation and are often a consequence of complex Layer 7 application DDoS attacks. Detecting and eliminating false positives through continuous testing, behavior analysis, and rate limiting techniques is highly important in implementing a successful DDoS mitigation practice.

JUST LIKE AN ELITE SQUAD TRAINING FOR A MISSION, YOU NEED A CLEAR IDEA WHAT YOU ARE UP AGAINST.

## SECOND STEP: KNOW YOUR ENEMY

Just like an elite squad training for a mission, you need a clear idea what you're up against. "DDoS attack" is a general term that includes several different types of attacks.

### Volumetric attacks—network level 3/4

- **ACK attack/SYN flood** – Attackers send large volumes of SYN packets to servers, using spoofed source IP addresses. The SYN flood creates embryonic connections which

consumes all of the server resources and shuts down legitimate services running on it.

- **DNS reflection attack** – Attackers contact a large number of open DNS servers, requesting a large DNS zone file and providing the source IP address of the attack target. The DNS servers respond by sending the large DNS zone answer to the attacked server. The server is effectively taken offline, because it is unable to respond to new DNS requests from real visitors.
- **SMURF/ping attack** – Attackers send ICMP ping requests to a network's broadcast address, which is known to relay ICMP to all devices behind the router. The attacker spoofs the source IP to be the same as the router. So, devices behind the router respond with a ping, overwhelming the router with ping traffic and making it unable to respond to real requests.

## Application-based attacks—network level 7

An application-level attack is tough to detect, because it looks just like ordinary user traffic. Hackers plan their attacks by visiting a target system just like an ordinary user, and identifying operations that have high latency on the server—for example, a search that returns millions of rows. They then create a scripted form of the same operation and hit the server with massive amounts of "slow operations" that create a bottleneck and bring down the system. Well-known examples are Apache Killer and Slowloris.

The big challenge of Level 7 attacks is distinguishing between attackers and "civilian bystanders." It is easy for a network operator to take down the entire affected server. But of the thousands of malicious sessions hitting that server, some are legitimate user requests, possibly customers trying to make a purchase. It is crucial but very difficult to distinguish those legitimate requests from attack traffic. Minimizing these false positives is critical to avoiding not preventing legitimate users from using that service.

## Smokescreen attacks

Smokescreen attacks are becoming the real danger inherent behind DDoS. In this type of attack, DDoS is only used to deflect attention from what is really going on. As it becomes obvious that web properties are under attack, internal and external resources focus on shutting the attack down, scrubbing traffic, and staying

up. These intensive efforts afford ample opportunity for additional attack troops to sneak in the back door and inject Structure Query Language (SQL) tools. These injections typically involve large numbers of odd requests, which would ordinarily stand out, but may be lost in the chaos of a seemingly routine DDoS attack. Attackers can infiltrate the network unnoticed, steal valuable data, and wreak havoc.

PERFORM SIMULATIONS OF ATTACKS ON A REGULAR BASIS, INCLUDING CONSTANT UPDATES THAT REPRESENT THE MOST CURRENT TYPES OF ATTACKS.

### Combo and multi-focal attacks

Many of today's advanced DDoS attacks combine some or all of the approaches described above into multifaceted initiatives requiring multifaceted defenses. DDoS attacks have changed from scenarios where one attacker launches a one-dimensional attack from a single commanding control point to highly distributed, phased attacks involving multiple domains and encrypted communications. Coordinated efforts are frequently launched by multiple groups acting in tandem from multiple locations—either deliberately or by virtue of hijacking and botnets.

Today's DDoS attacks are run like military campaigns with extensive up-front planning, a high degree of coordination, and contingency plans that perpetrate or adjust attacks based on the success of the initial response effort. Extensive research done prior to attacks identifies multiple targets and their unique weaknesses. Feedback loops are used to monitor when a site goes down, indicating when a second round or next phase of attack should begin, and to chart progress until sites become unavailable or the ultimate goal is achieved.

## THIRD STEP: PUT IT INTO PRACTICE

Our "secret ingredient" is combat training. Without practicing an actual DDoS attack, you are not really prepared. Here are three options for carrying out a real military exercise in your organization.

### Simulating a simple DDoS attack yourself with basic tools

It is possible to simulate low-scale DDoS in your own lab and get a basic idea what it is like to be under attack. You can do this by grabbing a few lab machines, or a few machine instances on Elastic Compute Cloud (EC2), and running a tool like Kali Linux to generate large amounts of traffic aimed at your server. Of course,

you should do this with extreme discretion and aimed at a **staging system only**.

While the simulated attack is going on, you can use a load testing tool like Load Impact to simulate legitimate user traffic and measure how many legitimate users you are able to serve and what service level they experience while the attack is going on.

However, this test is limited in scale and the types of attack traffic used and only gives you a taste of how to prepare for a real Internet-scale attack.

IXIA'S CYBER RANGE HELPS ORGANIZATIONS RECREATE INTERNET-SCALE CYBER WARFARE SCENARIOS IN A CONTROLLED ENVIRONMENT.

## Simulating a realistic full-scale attack with Ixia's Cyber Range service

IIxia provides a realistic combat training service called Cyber Range to help organizations recreate Internet-scale cyber warfare scenarios in a controlled environment.

Employing the same conditions as the world's largest cyber ranges, including the Defense Advanced Research Projects Agency's (DARPA's) National Cyber Range, Ixia helps you harden your defenses and train your IT professionals as cyber warriors.

As part of the Cyber Range service, Ixia experts arrive on site at your organization with specialized equipment that can perform a sophisticated simulation of real-world cyber conditions. The Cyber Range attack simulations are based on Ixia BreakingPoint®, a security test solution that is able to simulate DDoS traffic at a scale of up to 900 Gbps, three times larger than the biggest attack in recorded history.

The tool can also be used to simulate a multi-faceted attack composed of different attack vectors. At the same time, it runs realistic legitimate traffic similar to your network's real users to measure the impact on users.

## Simulating DDoS on a regular basis with your own equipment

Getting your own Ixia BreakingPoint solution enables you to perform simulations of attacks on a regular basis, including constant updates that represent the most current types of attacks. Ixia provides an Application and Threat Intelligence (ATI) subscription, which gives you regular, bi-weekly updates and recordings of thousands of attack variations.

Ixia's BreakingPoint comes in two flavors. The first one is a virtual edition (VE) that allows you to run a simulated attack from your

own hardware (with limited scale suitable for small to medium enterprises, but with realistic attack characteristics).


The second is a full-scale solution with Ixia's PerfectStorm hardware, an "Internet in a box," which simulates millions of connections hitting your server just like in a real, Internet-scale attack.

Organizations that have their own test software and equipment have the highest level of reassurance that their DDoS mitigation technology, people, and processes are aligned to prevent even the most nefarious attack.

## An example of why testing is critical

Ixia carried out an exercise at a large financial exchange during a maintenance window to validate its DDoS mitigation service provider. Two carrier-class routers were brought down during the exercise, and it turned out the root cause was a configuration issue. Had this happened during business hours, it would have prohibited trades from being executed, costing millions of dollars. With this exercise, the organization was able to validate the DDoS mitigation service provider, practice and refine its incident handling process, reduce mitigation time, significantly reduce false positives, and improve cyber attack readiness.

## FOURTH STEP: BUILD YOUR DDoS MITIGATION "TEST SCENARIOS"

Once you have been through the motions of a realistic attack simulation, you can draft your own "ultimate pass/fail test," a procedure for security teams to follow in case of a real attack. The following table outlines what you should include in your ultimate pass/fail test and the potential impact in case of a real attack.

| What to Include in Your Ultimate Pass/Fail Test | Impact in a Real Attack |
|---|---|
| **An accurate view of your network's structure and traffic profile**<br>Typical load, application profile, regions from which you typically receive traffic | By documenting your network's typical behavior, you will be able to spot anomalies like traffic spikes, network slowness, and unusual traffic to more easily detect if you are under attack. |
| **An incident handling process**<br>Documentation of what should happen in case of an attack, which stakeholders need to be informed, who to turn to for decisions affecting user traffic and critical systems, and contact details of DDoS mitigation service providers and managed security partners | Having a blueprint can dramatically reduce the initial response time in the critical first minutes of an attack, and increase the effectiveness of the team in its response to the attack. |
| **Lessons learned from your practice sessions**<br>What went right, what went wrong, nuances of the tools and processes you are using, things to take note of and problems to avoid—all of this should be documented as part of your ongoing process. | Avoid repeating the obvious mistakes, take the correct actions, and surprise attackers by taking immediate command of the situation. |
| **Contingency plan for DDoS mitigation tools and services**<br>What will you do in case the DDoS mitigation tool or your DDoS cloud services provider are not functioning as needed? It may be necessary to drop all but the most critical traffic. Map out the most critical systems and create a white list of the IP addresses of your most valuable customers. Make a plan to keep them live no matter what, even if your defenses fail. You can do this by gaining visibility of the ports, protocols, and repeat users on your network. | A good plan ensures that even in a worst-case scenario, 20% of your systems and traffic representing 80% of your business value can remain alive. This can stop the vast majority of the damages incurred by a DDoS attack, even if all defenses fail. |

| What to Include in Your Ultimate Pass/Fail Test | Impact in a Real Attack |
|---|---|
| **Plan how to watch out for other attacks**<br>DDoS is often a smokescreen for more sinister activities, such as data exfiltration. Prepare in advance to keep security resources and staff available to guard against attacks happening behind the smokescreen of the main DoS attack. | This awareness prevents irreparable financial and reputation damage caused by theft of internal or client information. |
| **Decide what "good" looks like**<br>You should know how to define and measure successful defense against an attack. For example, you may want to enable failover to a backup site within 30 seconds or ensure that all purchases started before the attack are completed. | Setting your benchmark can help control the spend. With a definition of "good," you know what level of DDoS mitigation services you need to purchase to achieve that measurable result, and the financial value of the result equated with the cost of the services. Also, a definition of "good" helps set expectations with stakeholders—knowing that in most attacks, even with successful defense, some damage to business will happen. |

## Want to experience the power of the Cyber Range or Ixia BreakingPoint?

[Schedule a demo]

**IXIA WORLDWIDE HEADQUARTERS**
26601 AGOURA ROAD,
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 EUROPEAN HEADQUARTERS**
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

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

SALES +65.6332.0125
(FAX) +65.6332.0127