How to Build a DDoS Response Plan in 7 Steps

IMPERVA INCAPSULA

IMPERVA®

INTRODUCTION

You've probably heard about distributed denial of service (DDoS) attacks, or maybe you've even been hit by one. If you're like most organizations, you've already been DDoSed. Perhaps the attack was minor, a wakeup call, but then the attack subsided without causing damage and you just left DDoS protection on your "to-do list."

If you don't have a DDoS attack plan, it's probably time to bump it up to the top of your list. That's because DDoS attacks are getting bigger, persistent, and more harmful. They inflict serious cost in terms of lost revenue, damaged systems and lost consumer trust. DDoS is no longer just a web server problem; infrastructure is now a target. The attacker's ambition is clear: Take down your online existence and harm your organization.

The attackers have a stash of attack methods from which to choose. Simple, low-cost DDoS toolkits and botnet-for-hire services that cost as little as $50 for an attack leave no online network, application, service, or website immune to danger. First and foremost is the volumetric or network level attack that tries to clog your pipeline to the Internet. Protocol attacks can succeed at consuming the resources of servers, routers, firewalls and even load balancers. Attackers can also launch application attacks that try to overload web servers by mimicking real users. These attacks can cripple a mid-sized website with as few as 50-100 requests per second.

So the question is: What can you do before an inevitable attack to ensure you have adequate defenses in place? Two things–develop a plan and adopt a DDoS mitigation solution.

7 STEPS TO BUILDING A DDOS RESPONSE PLAN

Every organization should have a DDoS response plan in place so that when the inevitable attack occurs, response is swift, damage is minimal and your good reputation remains intact. Here are seven steps to building a DDoS response plan.

1. Build a DDoS Response Team

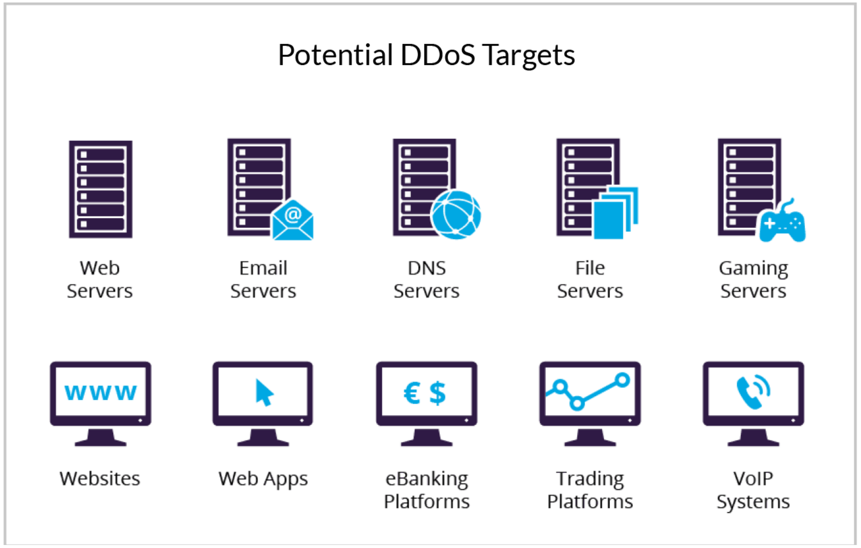
The first step is to identify the various people and departments within your organization who will be in charge of both planning and execution. Your team must fulfill a range of tasks–from identifying and mitigating an attack to coordinating with ISPs, notifying customers, communicating with the press, and minimizing potential reputation and liability issues.

2. Create a Response Plan

The purpose of your response plan is to define various resources, tools, and procedures required to minimize the risk and costs of a DDoS incident before it happens. It should include topics such as risk assessment, organizational roles and responsibilities, and more.

3. Assess Your Risk of an Attack

In preparing your organization to deal with a DDoS incident, it's imperative to understand the scope of your risk. Which infrastructure assets need protection? What is the cost of a given asset becoming unavailable?



The cost of an extended outage can be measured in terms of lost revenue and resources required to recover an asset. This risk of an outage needs to be evaluated against the cost of implementing DDoS protection for the particular assets.

4. Identify Single Points of Failure

Another important part of risk assessment is the identification of single points of failure, such as your DNS server or routers, and how to minimize potential issues related to them. For example, today many DDoS attacks are targeted against DNS servers–often an Achilles' heel of network security. Even if your online systems are protected, a successful attack against your DNS server can render it unavailable.

5. Strategize with Your ISP

It's important to clearly communicate with your Internet service provider (ISP) as part of your DDoS response preparation. In large attacks that can completely strangle your bandwidth, your ISP has no choice but to intervene.

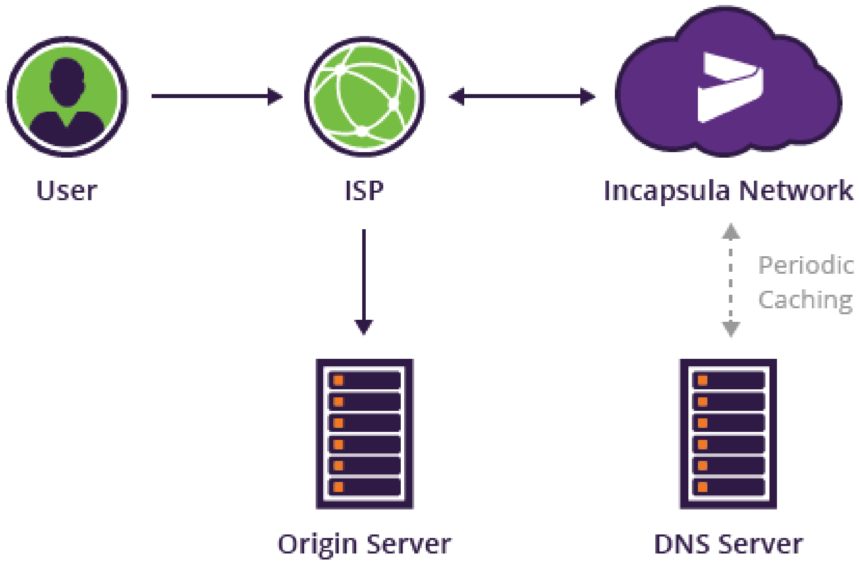
Massive DDoS attacks targeting one ISP customer can result in service degradation for all its other customers and may even result in service-level agreement (SLA) violations with respect to availability. In extreme cases, the ISP can pull the plug on your connectivity altogether.

6. Check Your DNS TTLs

Time to live (TTL) is the value determining how long a piece of data is valid. In the DNS world, TTL limits how long your current DNS settings are cached with ISPs. This means that if your website's TTL is set at three hours, other DNS servers won't bother checking for a DNS update for your domain over that duration. If you're using an on-demand, DNS-based DDoS mitigation solution, your TTL needs to be lowered prior to experiencing a DDoS attack. A lower TTL equates to a faster reaction; this is the time it takes to get traffic routed through your DDoS solution.

7. Test and Maintain

If you're using an on-demand DDoS mitigation solution, you don't want to wait for an actual attack to discover whether everything is in working order. As time goes by, you introduce new websites and applications, and your DDoS protection provider periodically updates its systems. It's important to check the impact of these changes on your readiness. For testing purposes, you should turn on your DDoS mitigation measures for a two-hour period every three to four months or once a year at an absolute minimum. Test to certify your systems and applications continue to function properly, traffic continues to arrive, and there is no negative impact on your users.



ADOPTING THE RIGHT DDOS PROTECTION SOLUTION – QUESTIONS TO ASK

When it comes to selecting a DDoS protection solution, the good news is that there are many technologies, products, and services available. The bad news is there are a lot of options to choose from, each representing a different approach. These include homegrown solutions, cloud-based services, and appliances deployed within the data center. There is not one right answer for everyone; each type of IT setup requires a different DDoS solution.

Here are some key questions to ask as you think about your own requirements and evaluate a DDoS mitigation solution.

Attack Detection

- Does the solution support automatic attack detection or does it require manual intervention?
- Does the solution scale on-demand to mitigate large attacks?
- In addition to network attacks, will the solution mitigate application attacks?

Time to Mitigation

- Does the solution's time to mitigation match my business and operational needs?

User Classification

- Can the solution distinguish between legitimate users and bots?
- How does it handle legitimate users when a DDoS attack occurs?

Web Application Firewall

- Does the solution include a web application firewall to protect web applications?

Always-On or On-Demand

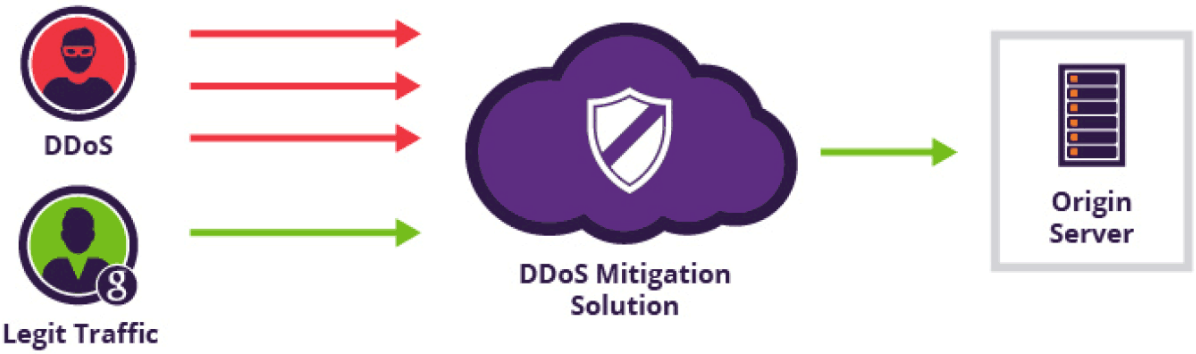
- Will I always be protected by the solution?

- Do I need to manually engage protection each time an attack occurs?

Deployment Mode

- Does the solution deployment model make sense for my architecture?
    - DNS redirection for web applications
    - Individual IP address protection
    - BGP routing for Class C infrastructure protection
    - DNS proxy for DNS-targeted attacks

Malicious DDoS attacks have become a fact of life for almost all organizations, but a well organized plan and a DDoS mitigation solution will keep the attackers from causing you significant harm.



PREPARATION CHECKLIST

STEP	ACTIVITY	DETAILS/TIMETABLE
1	Build DDoS response team	• Identify people and departments that need to be involved • Define roles and responsibilities
2	Create DDoS response plan	• Define resources, tools, and procedures required to minimize the risk and costs of a DDoS incident • Plan should cover the steps below
3	Identify single points of failure and bottlenecks	• DNS Server • Bandwidth • Router and switches • Firewalls and other network equipment • Redundancy and disaster recovery options
4	Coordinate with your ISP	• What type of DDoS protection does it offer? • What type of DDoS attacks can it protect against (e.g. network layer, application layer)? • What type of assets can it protect: DNS servers? Infrastructure? Websites? • How much protection does it provide? • What is its SLA in terms of time to mitigation?
5	Optimize DNS Time-to-Live (TTL)	• Optimize your DNS TTLs for the type of DDoS solution you choose to deploy
6	Test DDoS readiness	• Once every 3 – 4 months

Find out how you can optimize website performance with a free 14-day trial

- It's easy.
- No software to download or equipment to install
- On-boarding requires only a DNS change
- Includes load balancing and web application acceleration

Get Started Today

Questions? Contact us

IMPERVA INCAPSULA

IMPERVA