DDoS Response Playbook

Why You Should Read This Guide?

Distributed denial of service (DDoS) attacks have become a fact of life for any business with a web presence. Whether you're an enterprise, e-commerce business, local organization, or government office – it's merely a matter of time before you're going to have to deal with the inevitable DDoS attack. The question is what you can do before an attack in order to have adequate defenses already in place.

Like any business initiative, good preparation and planning can go a long way toward making the DDoS response process as manageable, painless, and inexpensive as possible. Organizations that engage in advance DDoS response planning are far more likely to limit potential damage and act in an effective manner than those that try to improvise their way through a DDoS-induced crisis.

This handbook provides you with a practical guide for planning and executing a DDoS response plan. It outlines pragmatic steps and best practices for choosing and setting up the right mitigation solution for your organization, how to authoritatively respond to an attack, and conduct a thorough post-attack analysis for developing follow-up defense strategies.

What's inside

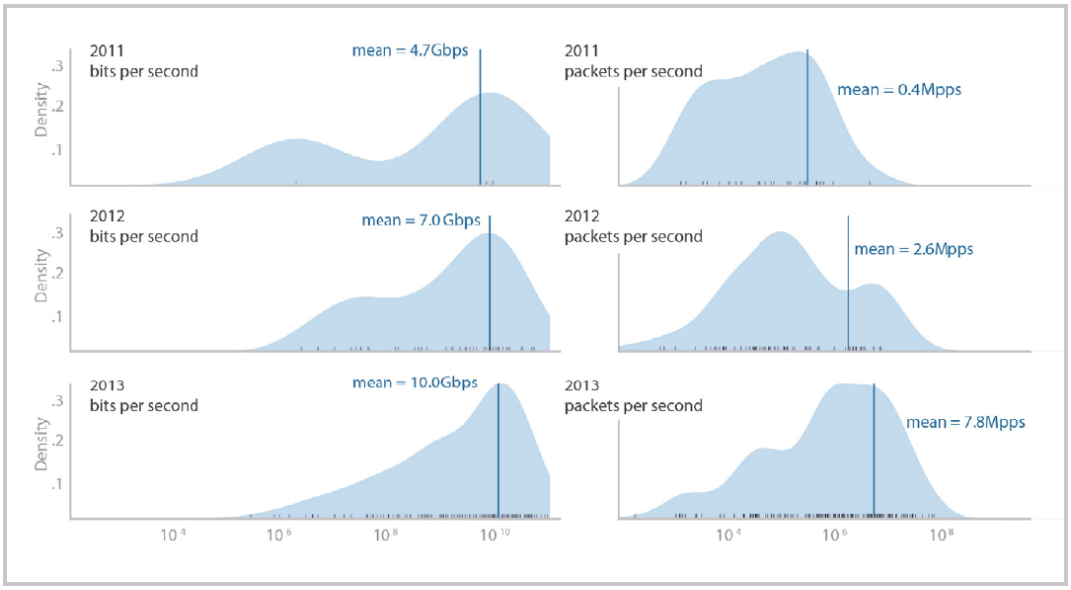
DDoS 101 – The Basics

Before preparing a DDoS response plan, let's set the groundwork by answering a few key questions regarding the nature of the threat and how these attacks impact your organization.

How often do DDoS attacks occur?

Based on industry reports and current trends, the prevalence of DDoS assaults is increasing at a rapid pace. According to digital security firm NSFocus, there is an average of 28 such attacks every hour.

Over the last year, Incapsula's 2013-2014 DDoS Threat Landscape report points to a 240% increase in botnet (i.e., network of zombie computers used by offenders to launch DDoS attacks) attack activity. In Q4 2013, the number of such assaults rose by 42%, according to Verizon's 2014 Data Breach Investigations Report.



2014 Verizon Data Breach Investigations Report (DBIR)

Given the relative simplicity and low cost of instigating a DDoS attack, as well as the relative impunity perpetrators enjoy, these trends are hardly surprising. Simple, low-cost DDoS toolkits and botnet-for-hire services – costing as little as $50 for an attack – leave no online network, application, service, or website immune from danger.

Who launches DDoS attacks and why?

Hacktivists

As the name implies, this type of hacker is typically motivated by a political cause. Hacktivists use DDoS attacks as a means to express their criticism of everything from governments and politicians, to "big business" and current events – such as the World Cup. Since September 2012, nearly 50 U.S. financial institutions have been targeted in over 200 DDoS attacks by the Qassam Cyber Fighters hacktivist group (allegedly backed by Iran).

Extortionists

Another common motivation for DDoS attacks is extortion, whereby a miscreant sends a ransom note to victims before or after an attack. A recent wave of extortion-styled attacks targeted several prominent online software companies – including MeetUp, Bitly, Vimeo, and Basecamp, among others. Once a site has been targeted, money (usually in the $300 – $400 range) is demanded in exchange for stopping or not carrying out the attack.

Competitors

DDoS attacks are increasingly being used as a competitive business tool. Some are designed to keep a competitor from doing online business or participating in a significant event such as Cyber Monday (the cyber equivalent of blocking the entrance to your competitor's store). If your site is down, your services are disrupted and consumers may flock to your competitor. Even a very small amount of downtime can end up costing a company many thousands of dollars.

Vandals

And then there are "black hat" hackers – innately nasty people who get a kick out of bringing down a company's website. In the words of Batman's faithful butler, Alfred Pennyworth, "Some men just want to watch the world burn." DDoS vandals are the equivalent of the first generation of computer virus writers, looking for their fifteen minutes of fame.

What are the different DDoS attack methods and how do they affect your website?

DDoS assaults are intended to do just what the name implies – prevent a server or network resource from performing actions it is charged with providing. Such attacks are generally divided into three types:

- **Network (OSI model layers 3 & 4) attacks** clog the "pipelines" connecting your network, website, or online service to the Internet. They send huge amounts of traffic, overwhelming connection capacity until your systems become unavailable. The largest of these assaults, such as SYN floods and DNS amplification, already exceed 200Gbps. These volumetric penetrations continue to grow in size, fueled in part by the growing availability of cloud infrastructure. Verizon's 2014 Data Breach Investigations Report confirms this trend, showing an increase in average attack size from 4.7 Gbps in 2011 to 10.1 Gbps in 2013.
- **Protocol attacks** consume actual server resources, or those of intermediate communication equipment – such as firewalls and load balancers. They are measured in packets per second (p/s).
- **Application (OSI model layer 7) attacks** seek to overload resources upon which an application is running. The application crashes and takes the site offline. Layer 7 penetrations typically mimic legitimate user traffic so as to evade an organization's common security measures (including network layer anti-DDoS solutions). They do not require high volumes, for even a rate of 50 – 100 requests/second is enough to cripple most mid-sized websites.

Over 80% of DDoS attacks employ multiple methods (according to Incapsula's report) to create smokescreens, bypass protective solutions, and target multiple resources. Such multi-vector assaults wreak havoc within organizations and confound even the most vigilant human operators.

"DDoS attacks have evolved significantly in the last few years and are now a legitimate business concern. They can have a damaging effect on revenues and send an organization into full crisis mode."

Mark Hughes,
BT Security President
TweakTown

What is the financial impact of a DDoS attack on your business?

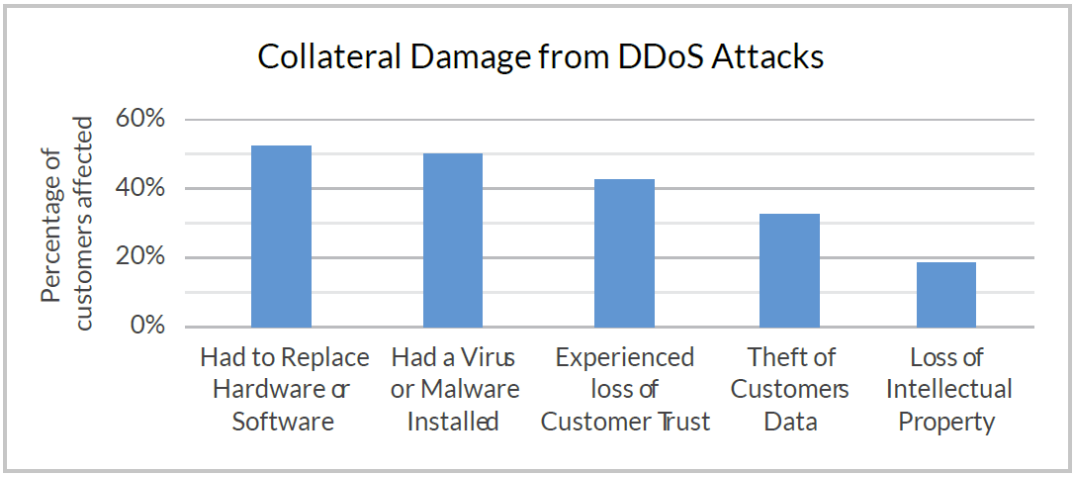
In August 2014, Incapsula surveyed 250 businesses having at least 250 employees to get the facts related to DDoS attack frequency and costs.

Almost half – 45% – of respondents indicated that their company had been hit by a DDoS attack at some point in the past. Of those who had been affected, 91% reported a barrage had occurred in the last 12 months, while 70% were compromised two or more times.

The majority of assaults (86%) lasted less than a day, while 68% persisted less than 13 hours. Although seemingly short-lived, the estimated cost of any such attack is $40,000 per hour – making the approximate cost of each intrusion almost $500,000. These costs are not limited to your IT group; they also have a significant impact on security/risk management, customer service, and customer sales.

The costs of DDoS attacks are not just financial. In this context, 52% of respondents had to replace hardware or software, 50% had a virus or malware installed or activated, and 43% experienced loss of consumer trust. In addition, as a result of DDoS penetration – combined with other hacking techniques – 33% experienced customer data theft, while 19% experienced loss of intellectual property.

Companies of all sizes experience DDoS attacks. They are often worse for larger organizations, however. Findings from our 2014 customer survey show that those having 5,000 or more employees are most likely to experience a DDoS encroachment, incur higher assault costs, and require more employees to combat the problem.



Preparation

Building Your DDoS Response Team

Establishing your DDoS response team is a crucial preparatory step toward reducing the impact of a DDoS attack. 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.

Ideally, your DDoS response team should include representatives from marketing, operations, customer service/support, legal, and IT security. These stakeholders should collaborate in developing your plan and establishing the roles/responsibilities of each team member—both in terms of planning and execution.

Creating a DDoS 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, mitigation strategies, monitoring, attack recovery, communications planning, and more. These are covered in the following sections.

Risk Assessment

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? What are the thresholds for implementing your plan?

Caused by a DDoS incident, the impact of an extended outage can be measured in terms of lost revenue and resources required to recover an asset. This risk needs to be evaluated against the cost of implementing DDoS protection for the asset.

Websites and externally-facing applications (i.e., any application or service accessible from outside your organization), are the crown jewels of the hacker community. The reason is simple –disrupting applications not only impacts online business, but is highly-visible to the world, affecting the user experience of your customers. It's imperative, therefore, that your web applications should be among the first assets to be reviewed for DDoS resiliency.

Other pieces of infrastructure such as email servers, FTP servers, VoIP services and back office platforms, like a CRM or ERP, can also be targeted with a DDoS attack. In addition to assessing risk for core business assets, business owners need to prioritize protection around infrastructure critical to their business. To an online banking or e-commerce site, for example, website downtime due to a DDoS attack means lost revenues and reputation damage. An insurance company, on the other hand, may be less concerned about its corporate website than ensuring that their agents in the field always have access to the back-office systems.

It is reasonable to assume that internal applications and services (i.e., those that can only be accessed via the company network) do not require DDoS protection.

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 router – 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; protecting it is mission-critical. You may want to purchase excess bandwidth or a dedicated link from your ISP in order to absorb additional traffic volumes generated by DDoS attacks. Consider system redundancy and disaster recovery options that can help you get back online quickly in the event of a prolonged barrage.

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. Following attack suppression, it can condition its future service to your organization based upon your adoption of a DDoS mitigation service.

Many ISPs already offer such a service to their customers. In such a case, be sure you understand its options for defending against DDoS attacks. Additionally, confirm your understanding of SLAs regarding response times.

Here are some helpful questions to your ISP:

- What type of DDoS protection does it offer?
- What type of DDoS attacks is it able to 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 relation to mitigation time?
- Can it terminate service to your organization due to a DDoS attack?

Working With Two ISPs

Where your organization's network and the target being assaulted are through the same ISP, a single DDoS attack could take down both. This could severely impact your ability to communicate with the outside world and conduct business as usual. Incapsula recommends you work with two ISPs to deal with a situation such as this. In this scenario, your primary ISP would have a mitigation solution in place to handle the DDoS attack traffic. Meanwhile your second ISP is used for connectivity in support of your Internet phone systems, blog, et al., should the bombardment overpower your primary ISP.

Moreover, in an extreme case where your ISP discontinues service, having a second ISP enables you to retain connectivity until the problem is thwarted.

Setting Optimal 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.

Shorter TTLs can cause heavier loads on name servers because the DNS records must be updated more frequently, however they allow for DNS changes to be propagated more rapidly.

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 low TTL equates to a faster reaction; this is the time it takes to get traffic routed through your solution. For example, if your TTL is set at three hours, then time-to-mitigation is the time it takes you to notice the attack plus three hours for TTL.

Testing

If you're using an on-demand DDoS mitigation solution, 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 vendor periodically updates its systems. It's important to check the impact of these changes on your readiness.

For testing purposes, Incapsula recommends turning on your DDoS mitigation measures for a two-hour period every 3 – 4 months (once a year at an absolute minimum). Certify your systems and applications continue to function properly, traffic continues to arrive, and there is no negative impact on your users.

Some DDoS mitigation providers bill on a per-incident fee. You may want to contact your provider prior to testing to ensure that you won't incur undue fees.

Maintenance Aspects

Five years ago, switching IP addresses was a fairly common, short term method for avoiding DDoS attacks. Today this method is no longer effective, for massive network attacks often target an entire IP range (a.k.a., a subnet). Since the impact on your ISP remains the same, you still run the risk of being kicked off its service.

Moreover, today's DDoS attacks are DNS-aware. Even if your new IP address belongs to a different ISP, the attack is still able to reach its target destination.

Switching ISPs works as long as your secondary ISP is being protected from the attack. This means that its anti-DDoS service is already in place and your new IP address is hidden.

Regarding network components, if you're considering upgrading to more robust equipment to deal with DDoS attacks, think again. Your bandwidth is finite, while DDoS attack size of continues to grow. Even equipped with a 20Gbps anti-DDoS appliance in front of your router/firewall, assaults exceeding that limit will get stopped upstream by the size of your Internet link, creating a problem for both you and your ISP.

Preparation Checklist

STEP 1: Build DDoS response team

❑ Identify people and departments needing to be involved

❑ Define roles and responsibilities

STEP 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

STEP 3: Conduct risk assessment

❑ Internet-facing applications and websites

❑ Infrastructure assets

❑ Third-party services

❑ DNS services

STEP 4: Identify single points of failure

❑ DNS server

❑ Bandwidth (Internet link size)

❑ Router and switches

❑ Firewalls and other network equipment

STEP 5: Strategize 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?

STEP 6: Other ISP-related issues

❑ Working with two ISPs for redundancy

❑ Optimize your DNS TTLs

STEP 7: Test DDoS readiness

❑ Once every 3 – 4 months

Building the Right DDoS Protection Strategy

When it comes to selecting a DDoS protection solution, the good news is that there are highly-effective technologies, products, and services available. The bad news is there are a lot of options to choose from – each representing a different protection 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. Think about your own requirements and choose a fully-compatible solution.

Key Technologies and Capabilities

Regardless of the chosen approach, select technologies that cover these essential DDoS detection and mitigation capabilities:

Attack Detection

Here your choice is between automatic and manual attack detection. Currently, the majority of detection is done manually by operators in the network operations center. DDoS mitigation requires 24 × 7 monitoring, however. This is problematic both in terms of the technology and the fact that humans are fallible. For this reason, many perpetrators attack during major holidays, the middle of the night, or on weekends when IT staff may not be available. How much traffic can your network absorb before systems crash?

When defending websites or applications, attack detection is often not effective without having visibility into the type of traffic and users generating it. If, for example, your operator sees a sudden spike in traffic, how would he/she recognize it as the spearhead of a DDoS attack – rather than a legitimate increase due to a marketing promotion or external event? As for a DDoS botnet, you don't want to wait for hundreds of bots to hit your site before it's determined an attack is in progress. You require a robust technology that can instantly stop the first bot.

Obviously, automatic detection is better – which means finding the right security technology.

Time-To-Mitigation

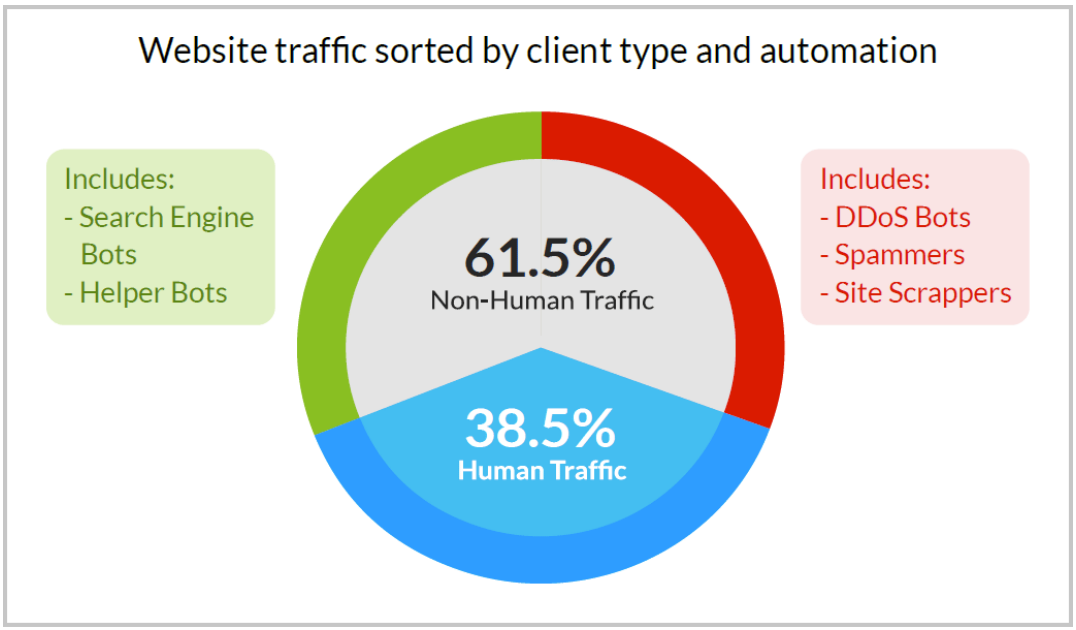
Simply identifying a DDoS penetration is not enough. Once identified, it must be stopped. Time-to-mitigation is the duration required to start blocking a DDoS attack once it has been identified. Different deployment models and defense strategies have differing potential times-to-mitigation; this should be seriously considered when selecting a mitigation solution. Any duration longer than a few seconds is wholly unacceptable.

Client Classification

Not only is it important to differentiate between human and bot traffic, it is also essential to distinguish between "good" and "bad" bots. Good bots, such as search engines and monitoring tools, are critical for website functionality and should not be blocked.

Virtually all DDoS attacks are performed by bots. For this reason, being able to identify them is paramount in dealing with any assault. When assessed by common traffic-monitoring tools, layer 7 DDoS penetrations masquerade as a surge in ordinary human traffic. To correctly identify them, your security solution needs to autonomously determine that the surge is perpetrated by automated malicious agents. Client classification permits granular security rules and mitigation policies so that legitimate clients are never blocked, even when your website is under attack.

One method used for client classification is progressive challenge mechanisms, which differentiate between bots and legitimate application users by validating whether the client browser can execute JavaScript, store cookies and perform other basic browser functions.



The majority of website visitors are automated, non-human users. Of those, roughly 50% are malicious and perform functions such as DDoS attacks, comment spam, and site scraping.
Source: Incapsula Bot Report, 2014

WAF

DDoS is often used by sophisticated perpetrators as a means to an end in multi-vector attacks. Here the DDoS assault serves as a smokescreen, tying up your IT security team and distracting them from the "true" target (e.g., sensitive data theft, network resource compromises). In addition to diverting attention, attackers use DDoS to weaken perimeter defenses or crash security appliances; this increases their chance of success using more traditional vectors (e.g., exploiting known vulnerabilities).

In seeking to protect your websites and applications against well-disguised layer 7 DDoS attacks, you'll require robust web application firewall (WAF) technology. This solution analyzes application traffic, distinguishing potential risks from legitimate usage.

A WAF protects your website or web application against traditional methods used in a multi-vector attack. This includes shielding against any type of application level hack, such as SQL injection, cross site scripting (XSS), illegal resource access, remote file inclusion (RFI), and other vulnerabilities. Make certain your WAF provider has the security expertise required to ensure your protection against new and emerging attack techniques.

Deployment Modes

Your DDoS protection solution can be deployed in various ways (e.g., always on, on-demand) and can be on-boarded using different strategies. Mix and match the following summary of options to meet your organization's specific needs.

- **Always-on**
  Always-on DDoS protection, as it implies, means that your websites and applications are always guarded from the moment it is deployed. This type of implementation offers instant DDoS identification and mitigation, so your systems are protected from the first salvo of any assault. This strategy has the quickest time-to-mitigation and negates the question of "How long before my solution kicks-in?"

By definition, always-on is a more secure option, but you should take into account that not all systems work optimally with DDoS protection continually engaged. The choice is dependent on your systems, applications, and on the service you're considering.

For websites or web applications, services which are not based on a content delivery network (CDN) can introduce such a high degree of latency that the user experience is greatly impeded. On-demand mode may be preferable in these situations.

- **On-demand**
  On-demand services are only engaged when an attack is detected. Typically, it can take up to three hours to activate such a solution due to internal procedures and escalation processes. Activation may also depend on the day and time of detection). Meanwhile, the bombardment continues at full strength – resulting in performance degradation and potential downtime during the critical first stages.

When choosing between always-on and on-demand, evaluate the possible impact on your application performance versus the risk of being exposed to a DDoS attack until your solution is engaged.

DNS Redirection for Web Application Protection

This deployment type of uses DNS redirection to reroute all website traffic (HTTP/HTTPS) through the DDoS protection provider's network. It requires changing your website's DNS setting to point to your provider's network; there incoming traffic is scrubbed prior to being routed back to the IP address origin. DNS redirection offers fast and easy onboarding, since there isn't an additional hardware or software requirement involved. As a bonus, it lets you keep your existing hosting and application infrastructures.

Once traffic enters the provider's network, various inspection layers identify and filter out malicious DDoS traffic. While malicious traffic is weeded out, legitimate traffic continues to flow unhindered to your protected websites.

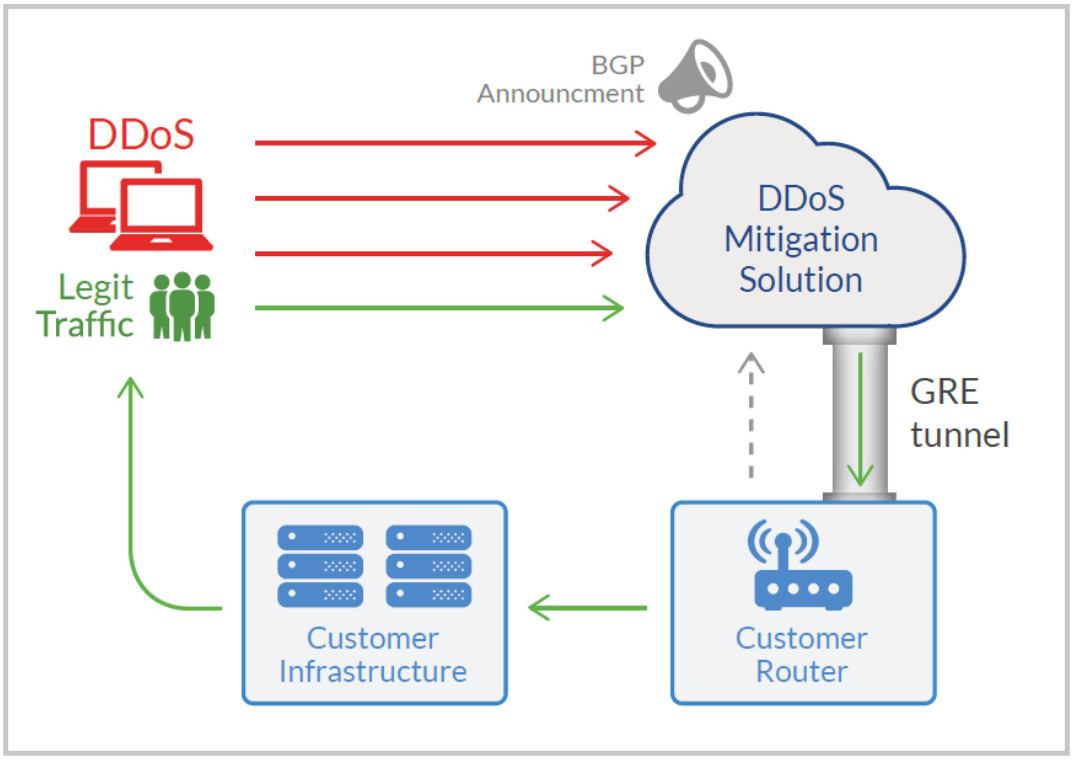
However, in using DNS redirection – particularly with respect to preventing layer 7 attacks – the degree of sophistication depends on the vendor.

It's important to understand the type of network through which DDoS attacks will be redirected. Legacy scrubbing networks – a simple collection of scrubbing servers through which traffic is routed for cleansing – impact website performance, since your data must transit through them en route between a website and its users. A more modern – and therefore preferable – type of scrubbing network is where the DDoS protection solution sits on top of a global CDN. CDNs do not introduce latency and, in many cases, speed up web traffic thereby enhancing the user experience.

While true any type of DDoS mitigation method you employ, provisioning and implementing prior to an attack is especially important. This is because SSL certificates may need to be configured so that HTTPs-based traffic can also be inspected and cleansed.

Border Gateway Protocol (BGP) Routing

For enterprises needing to protect multiple service types and protocols across an entire subnet range of IP addresses (known as a /24 or C-class subnet), BGP routing-based solutions are effective. Typically these are an on-demand solution type. They're good for thwarting large volumetric and advanced DDoS assaults targeting any type of protocol or infrastructure – including HTTP/S, SMTP, FTP, VoIP, et al. This deployment mode also provides origin protection against direct-to-IP attacks (i.e., attacks against network infrastructure/servers that target a specific IP address).



BGP routing most often requires an additional monitoring solution; it may be included as part of the sale or as an add-on to identify attacks. During an attack traffic is redirected through a set of distributed scrubbing centers using BGP announcements. From that point on, the protection provider acts as the ISP, advertising all protected IP range announcements. All incoming traffic is inspected and filtered; only clean traffic is securely forwarded to the application origin via GRE tunneling or a dedicated cross-connect. Outbound traffic is returned asymmetrically via your usual upstream ISP.

A minor drawback to using the BGP routing-based approaches is that latency may increase during attacks. This happens because traffic must first be routed through the scrubbing network for cleansing, without CDN technology in place to counteract the extra travel distance the data incurs.

Dedicated IP

For smaller organizations wishing to protect multiple service types and protocols, but do not have a full C-class IP range, this is similar to IP-based protection. In this deployment mode (and unlike BGP), the protection provider assigns you a "dedicated IP address" from its own IP range. Using this address, all incoming traffic passes through the provider's network where it is inspected and filtered. A redundant, secure two-way GRE tunnel is used to forward clean traffic to the origin IP and to return outbound traffic from the application to the users.

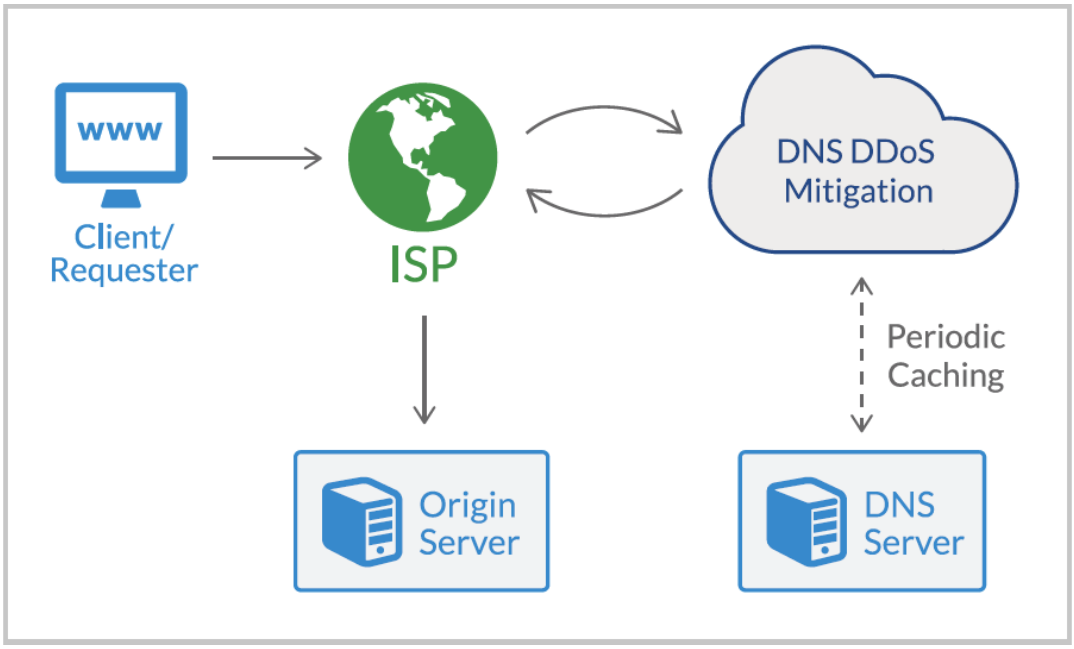
DNS Proxy

Deployed as an always-on service, proxy solutions can be used to safeguard DNS servers from targeted DDoS attacks. To set this up, a proxy is deployed in front of your protected DNS servers, where it inspects all incoming DNS requests. It filters out malicious requests, ensuring that only safe queries reach your origin DNS server. Additionally, it also blocks attempts to use your server as a platform for DNS amplification attacks targeting other servers.

Depending on the TTL settings of your name server, implementing a DNS proxy solution can potentially be accomplished in minutes (but could take as long as 24 hours). Once enabled, the proxy becomes your authoritative DNS server, while you continue to manage your DNS zone files outside of the proxy network.

If you use an external DNS provider, a proxy service can help you avoid huge bills by offloading large volumes of malicious traffic sent to the DNS server. Moreover, it reduces the chances of being blacklisted from their service due to DDoS attacks originating from your site.

DNS proxies offer an added benefit in that they can also function as caching servers. If the proxies are deployed globally, such as on a CDN, they can cache DNS requests and return results locally – thereby accelerating DNS server response times.



Physical Link / Cross-Connect

This mode is identical to the BGP routing model previously described, with one exception. Instead of connecting the protection provider's scrubbing centers to your network via GRE tunneling, a direct physical link – also known as a cross-connect cable – is used. This most often requires that your infrastructure reside in the same data center as your protection provider. By using a direct physical connection, you're always assured predictable latency and maximum throughput.

DDoS Mitigation Requirements Checklist

Attack Detection

❑ Does the solution support automatic detection?

❑ Does the solution scale on demand to mitigate massive network/protocol layer attacks?

❑ Does the solution mitigate application layer attacks?

Time to Mitigation

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

User Classification

❑ What user classification technologies are in place?

❑ Can it distinguish between legitimate users and bots?

WAF

❑ Do the solutions I'm evaluating include a WAF?

❑ If not, how will they protect me from application layer threats?

Always-On

❑ Will I always be protected by the solution?

❑ Do I need to engage it each time an attack occurs?

Deployment Mode

❑ Does the solution deployment model make sense for my architecture?

- DNS redirection for web applications
- BGP routing for infrastructure protection
- DNS proxy for DNS-targeted attacks
- Physical link for infrastructure protection in shared data center

Responding to an Attack

Identifying an Attack

Early detection plays a pivotal role in minimizing the impact of a DDoS assault. Even before bringing down your networks or systems, frontline appliances are affected, attack volume increases, and performance further degrades for every second a penetration goes unnoticed.

Additionally, some DDoS Attacks patterns are specifically designed to exploit slow reaction times. For example, so-called "hit-and-run" bursts rapidly flood a network with requests, slamming it again and again every few minutes – sometimes for days. Slow-to-respond manual safeguards are worthless in such situations.

Many DDoS intrusions are launched over a weekend or on holidays, with the assumption that response teams are not available. Coupling automatic detection with instant triggering of mitigation measures offers a highly-effective 24 × 7 DDoS mitigation while eliminating time-consuming manual procedures.

Establish a War Room

Designate a "war room" to serve as a planning and communications center during an attack. This could be an existing security or network operations center – perhaps even a conference room. Here your response team can review security updates and strategize defense schemes. Assign a lead who will be responsible for all high-level security decisions during the onslaught.

Important: Do not assume your organization email will be available during this time. Verify that your response plan documents, team contact information (and other key personnel), as well as that of your ISP and DNS providers, is kept in a secure location independent of Internet access. A hard copy of all of this information may prove to be essential.

Responding to Ransom Notes

According to a recent Incapsula survey, 46% of DDoS victims received a "ransom note" from their attacker, often prior to the assault. Such messages promise to spare the organization in exchange for money.

Perpetrators often ask for a few hundred dollars. Kept intentionally small, the demand is seen as affordable to a small business – or easy to hide in the expense report of a mid-level manager within a larger company. The offenders are playing arbitrage – they easily rent a botnet for $500 and then send out $500 ransom notes to ten or more companies, calculating that some will pay.

Paying ransom is not recommended. First, there is no guarantee that the attacker will honor their commitment. If a willingness to pay is sensed, the initial requested amount may even be raised. Further, once an organization is known to pay, there is no guarantee the perpetrator won't return – much like organized crime extortion and "protection money" schemes.

If you receive a ransom note, Incapsula recommends the following:

1. Do not reply to the note. There is no negotiating with attackers, so responding is pointless.
2. Do not pay the ransom for the reasons outlined above.
3. Alert your response team and try to weather the attack using an effective DDoS mitigation solution.
4. Inform your legal team of the attack and send them a copy of the ransom note. Depending on its length and impact, public companies may decide to disclose the event.

```
we have a botnet
army ready to take
down your site.

you have 48 hours
to pay us $1200

merry xmas!
```

The Importance of a Communications Plan

Communicating with customers, partners, and the general public soon after a DDoS attack is vital for preserving your organization's reputation.

The public will know that your site, service, or other systems are down – keeping it secret simply fuels fears. Instead, it's better to explain to customers the difference between a DDoS assault and other types of cyber-attacks that place customer data at risk.

If your organization's website has been afflicted by a DDoS attack, it's possible your blog may also be out of commission (if it's hosted on the same server as the attack target). In such casein event, social channels such as Twitter can be an effective communications vehicle, helping to limit damage to your brand. This serves as another reason to invest in a secondary Internet connection, so as to maintain external communication channels while under attack.

A communications plan helps your organization minimize brand damage and reduce the financial impact of a DDoS attack, while also preparing it in advance to answer questions from customers, the press, and shareholders (as applicable).

Dealing With Customers and Partners

Maintaining good faith with customers is paramount. Consumers are generally supportive of a company organization under attack; trying to hide it may shift consumer anger from the perpetrator to your business.

Providers of services to other organizations (B2B), in particular, should decide how transparent you need to be when disclosing the details of a DDoS attack, since this information could also impact your clients' customers. You may want to prepare financial compensation to customers in advance. This includes making plans for potential discounts and service credits, as well as having reinforced call center and customer outreach teams on call following a service outage.

Communicating with Employees

Communicating with employees is essential for several reasons. First of all, you want to be certain that your web ops team, for example, can reach key decision makers or have the authority to make decisions when a site goes down. Non-IT employees may also be seriously impacted by loss of availability to email and other web-based applications. They need to be informed of the situation and provided instructions with respect to backup or offline options until systems are back online.

Dealing with the Media

Nominate a single spokesperson for the DDoS response team in advance and prepare that person to deal with the media. This ensures consistent external messages and avoid confusion.

Also, your PR team should have a blog post already written as part of its crisis communication plan so it can be quickly published in the event of an attack.

Given the sensational nature of cyber attacks, you can anticipate that a DDoS attack could carry unwanted publicity along with it. As part of your planning, have an idea as to how you are going to notify and respond to any media inquiries if the scale of the attack warrants a response.

Legal and Regulatory Disclosures

There are few, if any, government-mandated requirements for DDoS mitigation or incident reporting. This is partly due to the relative newness of such multi-vector assaults. It can also be attributed to the fact that DDoS attacks typically don't fall under established areas of regulation in relation to data breaches.

This could be changing, however. Given the impact of cyber attacks (many of which include DDoS attacks) in recent years on financial institutions and other businesses, regulators and investors are focusing an increasing amount of attention toward cyber security risk disclosures. The U.S. Securities and Exchange Commission (SEC) already requires corporations to disclose to investors the cyber security risks they face, just as they disclose other material operational risk. After the spate of DDoS attacks against leading banks in 2013, the SEC is considering making specific disclosure of DDoS attacks a requirement, with some companies already voluntarily complying.

Post-Attack Steps

Following a DDoS incident, there is more to do than simply cleaning up and returning to business as usual. Take the time to review the lessons learned and make adjustments where necessary.

Process Analysis

By analyzing gaps in your DDoS response plan execution from both a technical and business standpoint, you can adjust it to improve execution during future incidents. Here are some items to evaluate:

- Consider those preparation steps you could have taken to respond to the incident faster or more effectively.
- Adjust assumptions that affected the decisions made during DDoS incident preparation (if necessary).
- Assess the effectiveness of your DDoS response process in relation to communications.
- Consider what relationships inside and outside your organizations could help you with future incidents.

Attack & Mitigation Analysis

As part of the post-mortem, review the impact of the intrusion in order to evaluate the effectiveness of your DDoS mitigation solution. Analyze security reports from your WAF to investigate attack trends. Also examine alert logs from your security information and event management system, as well as your network monitoring tools.

- What type of DDoS attack targeted you (volumetric, application layer)? What was its size and duration?
- Which equipment helped you mitigate, even it was only partially successful?
- Which attack traffic had the most impact and why?
- Which systems suffered the most?

The answers to these questions will help you decide whether you need to purchase better equipment and/or switch to a different DDoS protection service. It will also help you focus your protection (or redundancy) on the systems that need it most.

DDoS Glossary

Application DDoS Attacks
These attacks seek to overload resources upon which an application is running, for example, by making excessive log-in, database-lookup or search requests. This type of attack typically mimics legitimate user traffic so as to evade an organization's common security measures (including network layer anti-DDoS solutions). Also known as Layer 7 attacks.

BGP (Border Gateway Protocol)
BGP is used to make core routing decisions on the Internet and is the protocol used by organizations to exchange routing information. Incapsula uses BGP to enable organizations to redirect network traffic through its scrubbing centers.

Bot
A web robot, or simply "bot," is a computer that is under control of a third party.

Botnet
A botnet is a network of bots ("zombies") that can be commanded as a single group entity by a command and control system. Botnets receive instructions from command and control systems to launch DDoS attacks.

DNS
The Domain Name System (DNS) is the way that Internet domain names are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

DNS Amplification (Reflection)
By forging a victim's IP address, an attacker can send small requests to a DNS server and ask it to send the victim a large reply. This allows the attacker to have every request from its botnet amplified as much as 70 times in size, making it much easier to overwhelm the target.

DoS (Denial of Service)
DoS is an acronym for denial of service. A DoS attack typically uses one or a few computers to cause an outage on the target.

DDoS (Distributed Denial of Service)
A distributed denial of service (DDoS) attack uses many computers (often bots) distributed across the Internet in an attempt to consume available resources on the target. DDoS assaults are intended to do just what the name implies – render a server or network resource unavailable to its intended users.

ICMP (Ping) Flood
An ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, causing a significant overall system slowdown.

Layer 3 and Layer 4 DDoS Attacks
Layer 3 and 4 DDoS attacks are types of volumetric DDoS attacks on a network infrastructure. Layer 3 (OSI model network layer) and Layer 4 (protocol layer) DDoS attacks rely on extremely high volumes (floods) of data to slow down web server performance, consume bandwidth and eventually shut down access for legitimate users. These attack types typically include ICMP, SYN and UDP floods.

Layer 7 DDoS Attack
A Layer 7 (OSI model application layer) DDoS attack is an attack structured to overload specific elements of an application server infrastructure. Layer 7 attacks are especially complex, stealthy, and difficult to detect because they resemble legitimate website traffic.

Network Layer Attacks
This type of DDoS attack clogs the "pipelines" connecting your network, website, or online service to the Internet. They send huge amounts of traffic, overwhelming connection capacity until your systems become unavailable. Also known as Layer 3/4 attacks.

Parameter Tampering
Parameter tampering targets web data such as referrer fields, form fields and cookies. By changing the data in the files, servers can be made to process unexpected large amounts of data which can exhaust their resources.

Scrubbing Centers
Scrubbing centers are technical facilities designed for filtering malicious DDoS traffic from inbound traffic streams when mitigating DDoS attacks.

Security Operations Center (SOC)
A security operations center (SOC) is a centralized venue staffed with IT security experts who monitor and defend enterprise networks and their components. Incapsula's 24x7x365 SOC provides customers with proactive response and event management, continuous real-time monitoring, policy tuning, summary attack reports and 24x7 support.

SSL Floods
Decrypting SSL traffic on the server side requires 15 times more resources than encrypting the traffic on the client side. SSL floods exploit this asymmetry to overwhelm web servers, which are typically able to handle up to 300 concurrent SSL requests.

SYN Flood
A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (i.e., the "three-way handshake"). The client tries to establish a TCP connection with the host server, but doesn't respond to the host server's request for acknowledgment. The host system continues to wait for acknowledgment for each of the requests, tying up resources until no new connections can be made, and ultimately resulting in denial of service.

Tear Drop Attacks (TCP Fragment Flood)
A teardrop attack involves sending TCP fragments with overlapping, over-sized payloads to the target machine. When the server attempts to assemble the packet, these mangled packets can cause the server to crash.

UDP Flood
This type of attack floods random ports on a remote host with numerous UDP packets, causing the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP Destination Unreachable packet. This process saps host resources, and can ultimately lead to inaccessibility.

Volumetric Attacks
Volumetric DDoS attacks are also known as floods. DDoS attackers seek to overwhelm the target with excessive data, often using reflection and amplification DDoS techniques. See also Layer 3 and Layer 4 attacks.

Web Application Firewall (WAF)
A web application firewall controls access to a specific application or service by applying a set of rules to incoming HTTP traffic. A WAF is critical for detecting and preventing stealthy Layer 7 DDoS attacks that mimic regular application traffic.

Learn more about the Imperva Incasula Web Application Firewall.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance. Over 3,500 customers in more than 90 countries rely on our SecureSphere platform to safeguard their business. Imperva is headquartered in Redwood Shores, California.

Learn more at www.imperva.com.

www.imperva.com