NETSCOUT

| WHITE PAPER |

5 Things You Maybe Didn't Know

About DDoS Attacks That Can Cost You

SECURITY

TABLE OF CONTENTS

Introduction

To accurately determine your organization's risk of a DDoS attack, you must be aware of the latest trends in DDoS attacks and best practices in defense. For without this knowledge, much can be at stake, including increased costs and lost revenue due to service downtime or in effective mitigation.

The following paper will present some common misconceptions and facts about the modern-day DDoS attack that, if you are not aware of, could cost you significantly.

5 Facts About DDoS Attacks

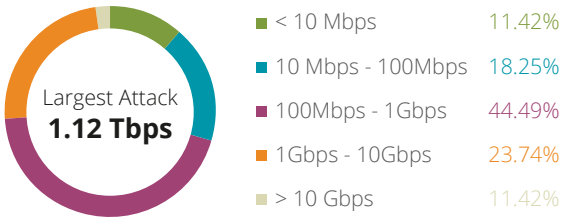
1. The vast majority of DDoS attacks are under 1 Gbps and last for only minutes.
2. There are many different types of types of DDoS attacks beyond just large flooding type attacks.
3. Relying solely upon a cloud-based mitigation service for DDoS protection is risky.
4. Firewalls should not be used for DDoS protection.
5. There are many motivations driving, and it's very easy to launch a DDoS attack.

Size

When it comes to measuring the size of a DDoS attack, there are multiple variables to consider.

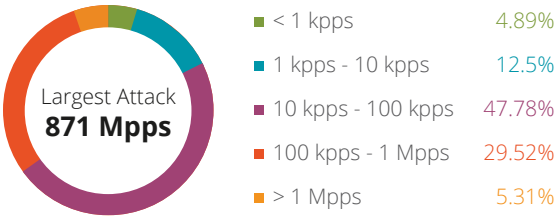
The first is Volume. Measured in Mbps (megabits per second), Gbps (gigabits per second), or even Tbps (terabits per second), this is what people commonly think of when they think of the size a DDoS attack. The media hype around Tbps-sized DDoS attacks only perpetuates this notion, leading one to believe that all DDoS attacks are massive. But this is not true.

Below is data from NETSCOUT's Cyber Threat Horizon, which tracks DDoS attack activity on a global basis. As you can see, some attacks are extensive (e.g., 1.12 Tbps), but the vast majority of DDoS attacks are under 1 Gbps.



Source: Cyber Threat Horizon, Volume of DDoS Attacks, Worldwide, 1st Half 2020.

The second variable is Speed. Measured in packets per second (pps), these types of attacks utilize large rates of packets. As seen in the chart below, these types of attacks can get as large as 871 Mpps (million packets per second), while the vast majority are under 1 Mpps. NETSCOUT has see an upward trend in pps attacks as attackers realize that their attacks don't have to be volumetric to be effective.



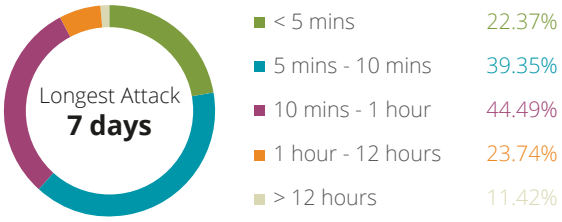
Source: Cyber Threat Horizon, Speed of DDoS Attacks, Worldwide, 1st Half 2020.

The 3rd variable is Vectors. A vector is a protocol the attacker exploits to launch a DDoS attack. Examples include UDP, NTP, TCP SYN, and many more. (Note: We will talk much more about the different types of attack vectors in the next section). When an attacker launches a DDoS attack, they will employ (independently or simultaneously) multiple attack vectors. According to NETSCOUT's 1H 2020 Threat Intelligence Report, there has been a considerable rise in the number of 15+ vector attacks over the last 5 years, with 26 vectors being the most recorded.

The last variable is Duration. Measured in minutes, hours, or days, a common misconception is that a DDoS attack is a long duration event. As seen from the chart below, some attacks can indeed last a long time (i.e., seven days), but most attacks last less than an hour.

To see a worldwide, real-time and historical view of DDoS attacks activity visit NETSCOUT's Cyber Threat Horizon.

https://www.netscout.com/horizon



Source: Cyber Threat Horizon, Speed of DDoS Attacks, Worldwide, 1st Half 2020.

Why is this important? It's not only the volume of a DDoS attack that you must be prepared for, but it's the speed, multiple vectors, and short-lived nature of attacks that you must also consider when deciding upon your DDoS protection solution.

Types

Simplistically, there are three broad categories of DDoS attacks.

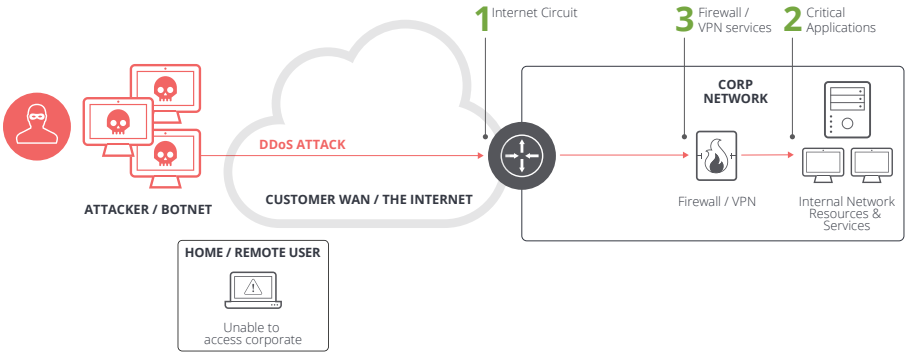
1. Volumetric
2. Application-layer
3. State Exhaustion

Let's look at each of these.

The Volumetric attack is commonly what most people think of as a DDoS attack. These attacks are designed to flood internet facing circuits with illegitimate traffic. Many times these types of attacks take advantage of millions of vulnerable IoT devices and/or exploitable services like memcached, NTP, DNS and SSDP, to launch spoofed queries which will flood the destination with large reply packets - a technique called reflection/amplification.

Application layer attacks are much smaller sized, stealthier, and designed to slowly exhaust resources in application servers. Examples include HTTP GET/PUT floods, partial requests, slow reads or excessive payload attacks.

State Exhaustion attacks, are smaller type flooding attacks designed to fill state tables in stateful devices such as your firewall, VPN concentrator, load balancer or IPS with illegitimate TCP connections. Examples include SYN Floods or SSL/TLS Exhaustion. These types of attacks were especially impactful during the COVID-19 pandemic, as work / learn from home users relied heavily upon the stateful VPN concentrator or firewall to gain access to corporate resources.



Why is this important? The modern-day DDoS is complex. Attackers can use a variety of DDoS attack vectors individually or simultaneously. Just as each vector has a different target and impact in mind, so too does each vector have a best practice for mitigation. Not having the proper mitigation in place for each vector is like having no protection at all–more on this in the next section.

Basically, there are Three Categories of DDoS Attacks:

1. Volumetric
2. Application-layer
3. State Exhaustion

But there are many different types of attacks within each category.

LEARN MORE

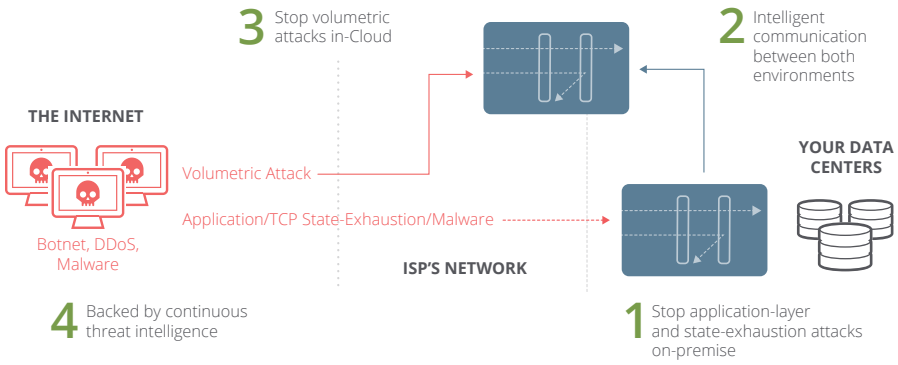
To learn more about each of these the different types visit NETSCOUT® What is a DDoS Attack?

https://www.netscout.com/what-is-ddos#component--2

Protection

The most common form of DDoS attack protection is a cloud-based mitigation service. (i.e. from your ISP or an ISP-agnostic DDoS protection service provider). You will indeed need your ISP or a cloud-based DDoS protection service provider to stop large, volumetric DDoS attacks that are larger than your internet circuits. But for smaller, state exhaustion and application-layer attacks, which are just as common, industry best practices recommend a stateless, on-premise solution.

To stop the modern-day, multi-vector DDoS attack, the most comprehensive form of protection is an intelligently automated combination of cloud-based and on-premise protection backed by continuous threat intelligence.



First, you want to deploy stateless, on-premise protection to stop the state exhaustion attacks that threaten the availability of stateful devices such as firewalls, VPN gateways, and load balancers. And because of your intimate knowledge of the critical applications running in your data center, on-premise protection is the best practice enabling you to configure attack countermeasures that match your local network and application environment.

Second, in the event of a large volumetric attack that will overwhelm your internet circuit, you want the ability to automatically and intelligently communicate with a cloud-based DDoS protection solution.

Where, thirdly, the volumetric attack gets mitigated in a cloud-based scrubbing center (e.g., from your ISP). After which, cleaned traffic gets redirected back to your original destination, where once again, your on-premise protection can block any vectors that may have been missed in the cloud.

And last but not least, this entire solution should be continuously armed with threat intelligence that allows you to stay abreast of the latest DDoS attacks vectors.

Why is this important? Relying solely upon a cloud-based DDoS protection service is risky and not comprehensive. Sure, you will need them during a volumetric attack. But they will struggle to stop those small sized, short lived DDoS attacks that an on-premise solution excels at. Many cloud-based solutions offer an "always on" mode, but this can be costly and still not be able to stop smaller application layer attacks which you can protect better by fine tuning your on-premise protection. The fact is, hybrid protection, that is, the intelligent combination of on-premise and cloud-based protection, offers the most comprehensive form of protection from the modern-day DDoS attack.

Industry analysis agree... Hybrid or Layered Protection is the Most Comprehensive form of DDoS attack protection.

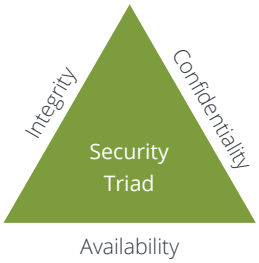
Firewalls

A common misconception is that firewalls can stop DDoS attacks. Technically they can. However, they are severely limited in their DDoS attack protection capabilities and can actually make matters worse. According to NETSCOUT's latest Worldwide Infrastructure Security Report Survey, more than 50% of respondents indicated that their firewalls failed or contributed to outages caused by a DDoS attack. The simple fact is that firewalls are not fundamentally designed to stop DDoS attacks. Below are several reasons why a firewall is not the right solution for DDoS attack protection.

- Because a firewall is a stateful device it is susceptible to state exhaustion attacks which fill finite sized, state tables with illegitimate connections causing it to stop legitimate connections – thus denying service.
- Firewalls offer rudimentary DDoS attack protection such as basic SYN, UDP, ICMP flood protection. But even this limited DDoS protection impacts the performance of more important functionality such as throughput of layer-7 inspection, SSL decryption and VPN termination.
- Since a firewall relies upon inspection of bi-direction connections, it cannot work in an asymmetric-routing scenario where only incoming DDoS attack packets are seen.
- A firewall will not provide you detailed the visibility into dropped DDoS attack traffic.
- A firewall will have no way to intelligently communicate with a cloud based solution for mitigation of large DDoS attacks.
- And finally, many firewall vendors recognize their DDoS protection limitations and sell in addition to their firewalls, a dedicated DDoS protection product.

The security triad of Confidentiality, Integrity and Availability is a well-known model in cyber security. One of its uses is to help categorize cyber security products. Let the firewall do what it was designed to do – protect Confidentiality. Let dedicated, intelligent DDoS protection products do what they were designed to do – protect Availability.

Why is this important? Dedicated, intelligent DDoS protection products can stop many more types of DDoS attacks at larger scale than a firewall. Be leery of firewall vendors trying to sell you costly firewall expansions to do things it was never designed to do. In fact, you can avoid these expenses and protect the availability of the firewall by deploying dedicated, stateless DDoS protection products in front of the firewall.



Let the firewall do what it was designed to do – protect Confidentiality. Let dedicated DDoS protection products maintain availability.

Motivations and Ease

So, what are the motivations or intentions behind DDoS attacks? There are many. Most people assume it's for monetary gain. True, that is a common motivation. Just like ransomware attackers are seeking to extort their victims. The difference is that with a DDoS attack, the attacker is holding your bandwidth or the availability of your service for ransom versus your data. But there are other motivations including:

Competition – Where one competitor tries to take our another via a DDoS attack. This has occurred in online retail and is quite common in the gaming industry.

Hacktivism or Geopolitical Protest – DDoS attacks are a common tool used amongst hacktivists. Sometimes times when you see an active, public demonstration, there's also a DDoS attack occurring related to that demonstration. We refer to this as the "cyber flection".

State Sponsored – Many nations states have accumulated botnets which they use for spam, phishing or DDoS attacks.

Try and Buy – DDoS is big business. Botnet owners advertising their DDoS attack services as Booter or Stresser services, will commonly offer free demonstrations or try and buys for their prospective clients.

Smokescreen – DDoS attacks can be used as a smokescreen to hide other malicious activity. For example during the 'Exfiltration' stage of the infamous Lockheed Martin Cyber Kill Chain, an adversary will launch a DDoS attack as a distraction while they steal confidential data.

Which brings us to the ease of launching DDoS attacks. You don't need to have an ounce of technical experience or a ton of money to launch a DDoS attack. There are plenty of free Do-It-Yourself or cheap DDoS for Hire Services (e.g. $5/hr) readily available for anyone to use to launch a large and sophisticated multi-vector DDoS attack.

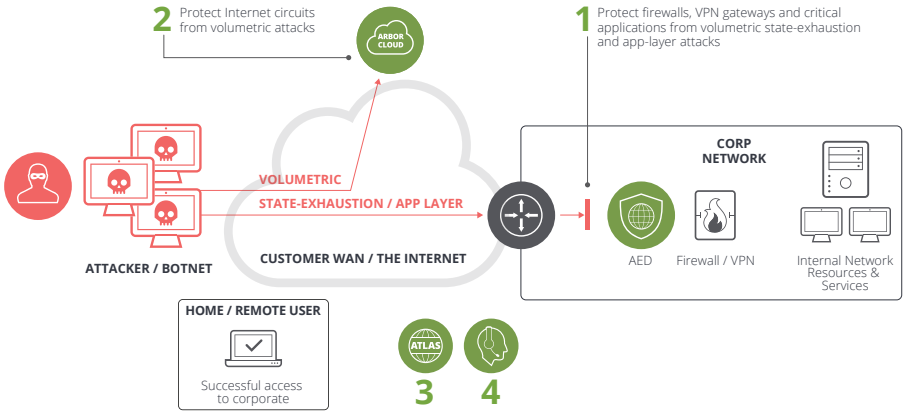
Why is this important? The combination of multiple motivations and plethora of cheap DDoS attack tools and services means the odds of your organization becoming the target of a DDoS attack are increasing. As previously mentioned, in most cases DDoS attacks come without warning, are small and short-lived. Therefore, you need to have DDoS attack protection solutions in place that can stop these attacks before the damage is done.

Increased DDoS Attacks

The increase in DDoS attack activity is partially due to the many motivations behind and the relative ease in launching them.

The NETSCOUT Solution

The NETSCOUT Arbor Smart DDoS Protection solution can protect your organization from the modern-day, multi-vector DDoS attack.



1. **Arbor Edge Defense (AED)** – A stateless packet processing appliance (or virtual machine) that resides on premise, in front of stateful firewall or VPN concentrators to protect them and business critical application services from volumetric (up to 40 Gbps), state exhaustion or application layer DDoS attacks. As an in-line device, dedicated to and customized for your specific environment, AED can instantaneously react to any attack, however small, protecting the availability of your network and service infrastructure. In the event of a large attack that will saturate the internet facing circuit, AED's Cloud Signaling feature can automatically redirect traffic to Arbor Cloud.
2. **Arbor Cloud** – A cloud-based DDoS attack mitigation service with over 11 global scrubbing centers with 14+ Tbps of mitigation capacity and manned 24x7 with DDoS attack mitigation experts. The fully integrated, intelligent combination of AED and Arbor Cloud delivers the industry best practice of hybrid DDoS defense which offers the most comprehensive form of protection.
3. **ATLAS Threat Intelligence Feed** – AED and Arbor Cloud™ are continuously updated with the ATLAS® Threat Intelligence Feed, which enables protection from latest DDoS and other threats.
4. **Fully Managed DDoS Protection Service** – The entire solution can be fully managed 24x7 by Arbor DDoS mitigation experts so you can focus on what you do best.

Bottom Line: NETSCOUT's Arbor Smart DDoS has the industry's broadest portfolio of DDoS attack protection products and services that enable organizations of any size to customize a solution to meet their technical and financial requirements of today – and the future.

LEARN MORE

For more information about the NETSCOUT Arbor Smart DDoS Protection Solution and how to protect your remote users' access to corporate resources visit:

www.netscout.com/business-continuity

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_019_EN-2001 09/2020