NETSCOUT

| WHITE PAPER |

An On-Premises Defense is the Cornerstone for Multilayer DDoS Protection

The NETSCOUT Vision

SECURITY

TABLE OF CONTENTS

Executive Summary

Industry analysts are coming to grips with the fact that due to today's growing frequency (e.g., 5M attacks in 1H 21), size (1.5 Tbps), and complexity of DDoS attacks, the need for a multilayer hybrid defense strategy is now a requirement. Furthermore, due to the creation of new attack vectors (Threat actors exploited or weaponized seven new reflection/amplification DDoS attack vectors within the seven months), the number of attack vectors being used in a single attack (31 attack vectors deployed in a single attack) and what's known as an Adaptive DDoS Attack which changes vectors based on the defense that is presented, the need for On-Premises protection with its inherent attack management agility and efficiency is a priority. It should be considered the foundation of a comprehensive DDoS protection strategy.

Introduction

DDoS attacks are getting more sophisticated, and attackers are increasingly shrewd and brazen; together, these pose a greater risk for organizations. Protection strategies of the past will suffice in some situations, like an attack designed to overwhelm your internet circuit before traffic arrives on your site; however, attacks specifically designed to evade those protections are the basis for the new attack landscape. Further, the ability to respond to attacks that dodged the cloud solution and hit the network edge is imperative and having the agility to change defenses quickly to adapt to subtle changes in attack vectors on site is crucial.

This paper will outline some of the vulnerabilities of a cloud-only option, present advantages of a comprehensive hybrid solution made up of a cloud solution alongside an on-premises component, and finally, support the stance that the on-premises part should be the foundation of the comprehensive solution and if given a choice a priority.

The vast majority of DDoS attacks are smaller than 1Gbps and last less than 10 minutes.

Source: NETSCOUT Omnis Threat Horizon, www.netscout.com/horizon

Why a Cloud-Only Approach is Not Enough

Cloud-Only DDoS providers have been available for some time., but as organizations applications and services have become more mission-critical with less tolerance for down-time and DDoS attacks have evolved to become more complex, cloud-only solutions are not enough.

Research and experience have proved that a multilayered DDoS defense strategy with an on-premises solution as the foundation is the only holistic approach to modern DDoS threats. To this extent, the security community has for a few years voiced strong support for this type of a multilayered DDoS defense strategy, backed by continuous threat intelligence.

Types of Cloud-Only Services

Cloud-based DDoS mitigation services fall into two major categories: CDN-based and traffic diversion-based.

CDN (Content Delivery Network) providers utilize their distributed infrastructure to absorb and mitigate attacks towards the assets that are served by their CDN. This approach suffers from a series of shortcomings:

- **Everything else is not protected.** Back-end databases or application services not on the CDN but still exposed to the Internet are susceptible. Internet connectivity to the corporate offices is unprotected as well.
- **Focus on web applications only.** CDN providers might lack the expertise, technology or flexibility to adapt their mitigation policies to anything other than HTTP(S)-based applications.
- **Lack of focus on security.** CDN providers might not be able to guarantee the availability of dedicated SOC personnel, and often lack a global view on the range of modern attacks, due to the lack of dedicated security research personnel.

Traffic diversion-based services usually offer more flexibility and are typically run by dedicated companies or business units of large ISPs. They have some inherent characteristics, though, that need to be complemented by on-premises systems:

- **Reactive.** Although it's possible to run an "always-on" traffic diversion to a cloud-based solution, the benefits of faster reaction times are frequently outweighed by performance impact, risk of false positives, or increased troubleshooting time in case of unidentified issues. For this reason, diversion-based services are usually run on-demand, and as such inevitably introduce delays in the time to mitigation. Combine this with the fact that the vast majority of attacks are less than 1Gbps in size and last for less than 10 minutes, it can be quite difficult for a cloud-based service to detect and stop these attacks before the damage is done. In many cases the duration of the attack-recovery time is far longer than the attack itself.
- **Latency.** With always-on full cloud solutions, legitimate clients might end up being penalized by unnecessary routing diversions, due to the location of the cloud service scrubbing center introducing annoying latency to users and customers.

External-only. Due to the nature of global routing, it is likely that attacks generated by sources located in the same ISP's network as the victim won't be diverted to the "cloud" and will instead be routed through the local, preferred path directly towards the victim:

- **Less granular.** Most ISP-agnostic, diversion-based services must rely on global BGP-based traffic diversion in order to provide maximum protection.[1] The smallest unit of address space that can typically be diverted is a /24 subnet, which means that legitimate traffic destined to hosts not under attack will be diverted through the mitigation infrastructure. Without visibility into the actual target of the attack, diversion-based services alone would usually need additional time to recognize the hosts not involved in it and apply the most appropriate mitigation policy for the actual victim.
- **Economical scalability.** Without visibility into the nature of attacks or even into the actual cause of outages that might be perceived as DDoS attacks, a cloud-only customer does not have another choice than to resort to the cloud every time. This can easily lead to increased costs and unnecessary traffic diversions.

Today's Targeted Complex Attacks Require On-Premises Components

Attackers react to mitigation policies by using multiple attack vectors, from volumetric such as reflection/amplification to application-specific "smart" floods, to state-exhaustion techniques, to attacks embedded in encrypted traffic.

Application-layer attacks typically conform to the protocols the applications are using, which often involve protocol handshakes and protocol/application compliance. An example of this type of attack would be a SLOW POST attack where the attacker sends legitimate HTTP POST headers that are compliant but the message body is sent at a painfully low speed meaning the server will subsequently slow to a crawl. Because the traffic within the attack appears to be legitimate, these attacks can go undetected by traditional on-demand cloud-based mitigation strategies.

Other typical targets for the bad guys are stateful devices like firewalls and VPN devices. In fact, according to NETSCOUT's Worldwide Infrastructure Security Report survey, 83% of respondents reported DDoS attacks which overloaded firewalls and/or VPN devices contributed to an outage, which is up 21% from prior year. To stop flood attacks on stateful devices like firewalls and VPNs within your network you need a solution that sits in front of those devices on the edge of the network and sees the attack traffic first. The second requirement is that the solution is stateless and not susceptible to the same attacks designed to take the firewalls and VPNs down. And finally, it needs to be always on so it is not subject to delays in the start of mitigation typical with an on demand cloud solution.

Attackers are getting more sophisticated as they increasingly hide their attacks in encrypted traffic. A key component of a security arsenal, therefore, is the ability to decrypt and inspect encrypted traffic securely and attest to its authenticity without slowing, or compromising it.

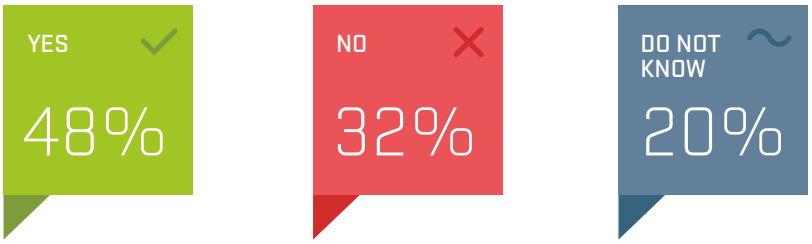
Another area of concern regarding decrypting and scanning packets is where the decryption is executed. Many organizations do not want their traffic being decrypted off site or by a cloud service because it may require sharing private certificates with the cloud provider, which is a security risk that many Enterprises aren't willing to take. In some situations, cloud providers themselves don't want the responsibility for managing private keys and the associated liability risk if the keys are leaked or exposed from their systems.

Because of the ideal DDoS solutions location at the edge of the network, that DDoS protection can also serve to detect and block IoCs with the help of a comprehensive threat intelligence resource.

[1] As opposed to DNS-based diversion, which however leaves several points vulnerable.

The threat with IoCs is the malware itself and the potential damage it can inflict. The challenge is reliably detecting the malware when it's present and stopping it by blocking communication to its C2 infrastructure for further instruction. IoCs may not necessarily "indicate" that an attack has occurred. But, if seen early enough, and analyzed, they can indicate that a network breach has occurred that precedes an imminent attack. For example, detecting a dropper prior to a ransom-ware attack. Confirming the attack, identifying the compromised device and blocking the potential C2 communication from the malware involved requires an in-depth security investigation. One of the things that makes this hard is ensuring you have an accurate and comprehensive list of potential indicators, combined with the necessary data or intelligence to confirm the threat, and take meaningful action to prevent the malware from causing harm.

The short duration of the majority of reported attacks as well as NETSCOUT's operational experience suggests that most attacks are surgically targeted, often generated by rent-by-the-hour botnets.



Source: NETSCOUT

Figure 1: Companies detecting multi-vector attacks.

Many of the attacks that require on-premises protection, due to the fact that they go undetected in a timely manner by other mitigation options, are usually multi-vector complex attacks that are very short in duration.

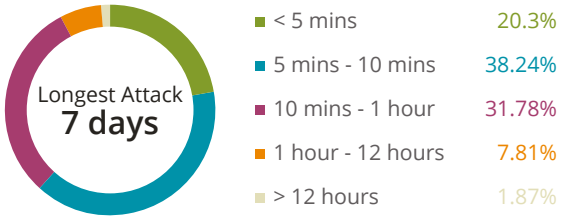


Figure 2: Attack duration.

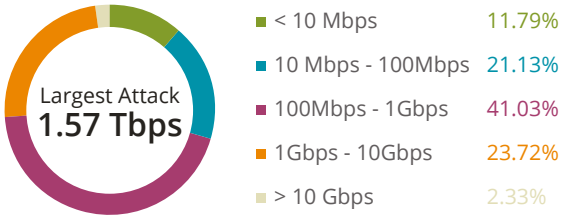
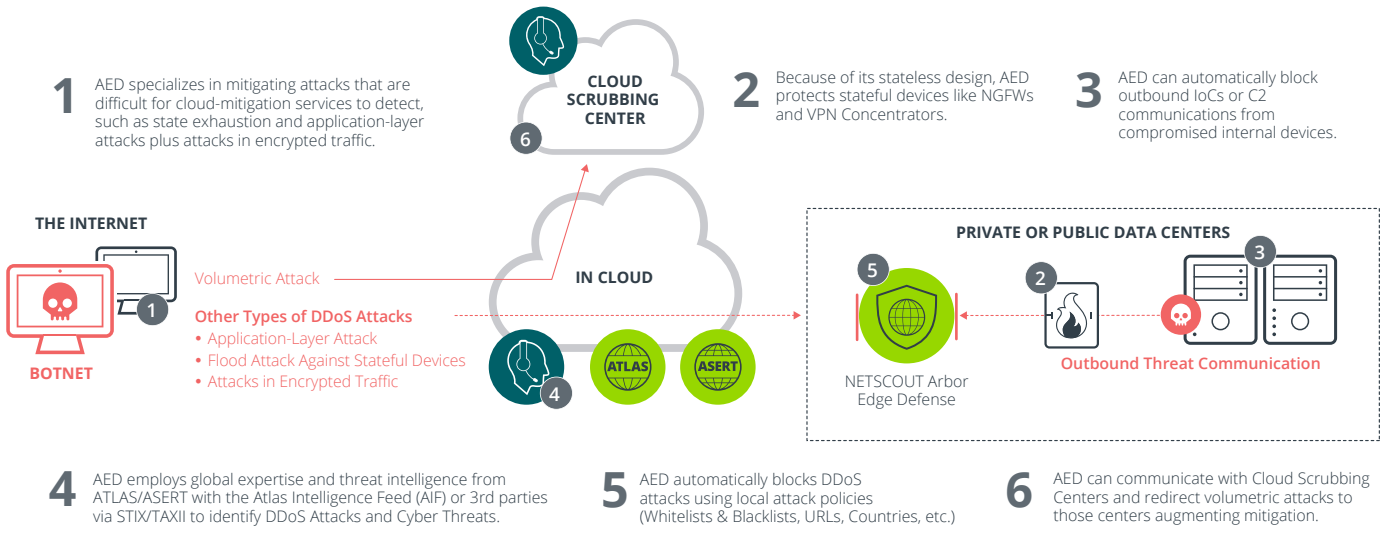


Figure 3: Attack size.



The NETSCOUT Solution

NETSCOUT has more than 20 years of experience in DDoS mitigation in the largest networks globally.

In 2011, NETSCOUT developed Cloud Signaling™, the first solution for automated and intelligent communication between on-premises DDoS protection devices (e.g. Arbor Edge Defense) and cloud-based services, pioneering the multilayer defense approach.

In 2013, NETSCOUT completed its vision by adding Arbor Cloud, an ISP-agnostic service that integrates in NETSCOUT's Arbor DDoS protection ecosystem.

NETSCOUT's multilayer protection strategy is designed to enable comprehensive DDoS protection in an increasingly complex environment. On-premises, dedicated, DDoS mitigation devices such as NETSCOUT Arbor Edge Defense provide stateless real-time protection, packet-level visibility, can be surgically tuned to any environment and can automatically and intelligently communicate with NETSCOUT Arbor Cloud or an ISP's cloud-based DDoS protection service to provide optimal protection.

AED provides advanced packet-based protection against internet scale threats, neutralizing the malware families that make up the global botnet threat. Armed with millions of reputation-based IoCs, NETSCOUT's packet-processing engine can detect and block inbound threats and outbound communication from internal compromised hosts that have been missed by other devices in the security stack – helping to stop further proliferation of malware and other tactics used within crimeware and advanced-threat campaigns.

Summary

Because of the damage that can be done by short duration attacks on an organization's critical business applications and services as well as the requirement for near real-time mitigation to stop these attacks, an always-on packet level mitigation solution that sits on the edge of your network is the foundation and a critical need for a multilayered comprehensive DDoS defense.

LEARN MORE

For more information about NETSCOUT Arbor Edge Defense visit:

www.netscout.com/product/netscout-aed

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_012_EN-2103 04/2022