WHITE PAPER

FOUR PILLARS FOR A MODERN DDOS PROTECTION STRATEGY

Precision, Scalability, Automation and Affordability

The four critical elements for an impermeable DDoS defense solution.

INTRODUCTION

Distributed Denial of Service (DDoS) attacks plague organizations of all sizes, and across all industries. The frequency, intensity and sophistication of modern attacks—and the attackers—threaten the most crucial aspect of running an online business: 24/7 availability.

The internet of things (IoT) exacerbates this problem. The question most asked by businesses: how do shrewd attackers weaponize connected devices and hijack them to do their bidding? The answer: by harnessing unsecured devices and turning them into massive botnets capable of launching paralyzing DDoS attacks that can exceed 1 terabit per second (Tbps).

In response to current attack complexity and intensity, and growing concerns over the fallout from a major DDoS attack, businesses are expanding their security defenses. A recent survey found that 74% of business say they are increasing their security spending to combat these unrelenting threats.

DDOS DEFENSE

74% businesses plan to increase security spending to combat DDoS Attacks

GET THE EBOOK:

► DDOS STRATEGIES FOR DEALING WITH A GROWING THREAT

Yet the questions remain: how do you choose the correct DDoS defense solution for your business? What makes one solution better than another? This white paper will help you understand the four critical considerations needed for evaluating DDoS solutions.

PILLAR 1

SURGICAL PRECISION TO PROTECT LEGITIMATE USERS

By nature, DDoS attacks are largely brute force; they are often perceived as crude. Legacy DDoS defense solutions were designed to protect network infrastructure from attacks, leaving legitimate users without a connection to the online resources they need. Maintaining service availability for users during a DDoS attack is the primary reason to deploy a DDoS protection solution. If legitimate users can't access the tools they need, then the solution has failed. Focus should be first on legitimate users, and then on protecting network infrastructure.

HOW TO KNOW IF YOU HAVE A DDOS SOLUTION BUILT ON LEGACY TECHNOLOGY:

- Relies on RTBH and traffic shaping
- Prone to false positives and false negatives
- Requires extensive manual intervention
- Lacks actionable threat intelligence
- Ineffective against sophisticated targeted network and application layer attacks

Effective DDoS defenses must be precise, with the ability to intelligently distinguish legitimate users from attacking bots. Solutions that focus on strategies like Remote Triggered Black Hole (RTBH) and service-rate limiting to detect attacking botnets fall short because they are indiscriminate and can block access for legitimate users. Meanwhile, legacy DDoS defense solutions rely primarily on bits per second (BPS) and packets per second (PPS) thresholds to protect infrastructure.

A surgically precise DDoS detection and mitigation solution, however, understands your environment in both peacetime and wartime, and can eliminate false positives and false negatives. It can also leverage up-to-the-second threat intelligence to pinpoint and eradicate known bad actors.

Additionally, surgical precision can lower operating costs, since frontline defenders won't be pulled off critical tasks to combat false and missed incidents.

SURGICAL PRECISION — ALL DAY, EVERY DAY

A10 Thunder TPS® uses surgical precision to detect and mitigate DDoS attacks. It tracks every access to the network and can therefore distinguish between legitimate users and attackers. Thunder TPS initiates source-based authentication challenges and applies limits only to policy violators that deviate from learned, peacetime behavior. Even if a sophisticated bot can validate the challenge, Thunder TPS tracks 28 behavioral indicators to catch bot-based deviations. If an attacking bot or misbehaving user breaks a defined policy, that misbehaving agent is blocked without creating collateral damage against legitimate users. Thunder TPS does this at an astounding scale of up to 128 million concurrent sessions thereby helping to keep networks online and available and eliminating false results.

PILLAR 2

SCALABILITY TO COMBAT MODERN THREATS

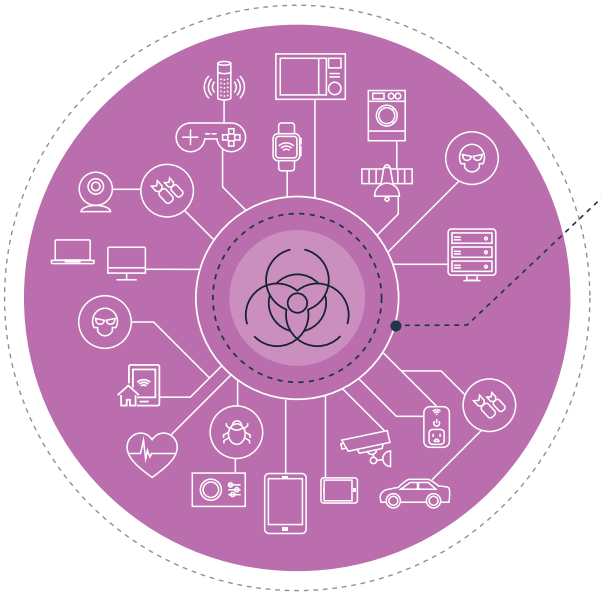
DDoS defenses are nearly useless if they can't scale to attackers' capabilities.

Attacks are increasing in size and sophistication, and as such DDoS defense solutions must scale to provide protection. Essentially, you must be prepared to defend against frequent and sophisticated attacks as small as 10 gigabits per second (Gbps) - and those rare occurrences when they exceed 1 Tbps.

Along with depth in mind, DDoS defenders must rethink their strategy and scale for the intensity and breadth of an attack.

An attacker's goal is to cause as much damage with as little effort as possible. It's often easier for them to throw many millions of small packets of attack traffic against your network's firewalls and servers rather than launch one massive volumetric flood.

This is where attacks from weaponized IoT devices can cause the most devastation—by exploiting the first "D" in DDoS: distributed. Legacy defenses were built to defend against thousands of coordinating DDoS attack agents, not millions of weaponized IoT endpoints, meaning this persistent barrage of attack traffic can slip through.



IOT DDOS
ATTACK TRAFFIC

Legacy defenses were built to defend against thousands of coordinating DDoS attack agents, **not millions of weaponized IoT endpoints.**

It is imperative for modern DDoS solutions to understand the intensity and breadth of an attack based on packets per second and millions of geographically distributed attacking agents, not just the size and intensity, based on Gbps of attack traffic.

Employing a hybrid DDoS defense solution ensures that you're capable of scaling to meet even the largest of attacks. Combining an always-on, on-premise solution with a cloud scrubbing service for when your Internet pipe is overwhelmed ensures that your network can stand up to attacks at any scale.

A10 Thunder TPS scales to defend against the IoT-fueled attacks and detects DDoS attacks through high-resolution packets or flow record analysis from edge routers and switches. Unlike outdated DDoS products, Thunder TPS is built on our market-proven Advanced Core Operating System (ACOS®)—the platform that delivers scalable deployment options and cost structures that make economic sense with a complete detection, mitigation and reporting solution.

Thunder TPS scales to protect organizations from attacks of all sizes, from 1 Gbps to 300 Gbps (or up to 2.4 Tbps in a list synchronization cluster). It detects and mitigates the largest multi-vector attacks including application and IoT-based assaults.

Thunder TPS supports protocol and packet anomaly checks and the forwarding of up to 440 million packets per second. It also enforces highly granular traffic rates of up to 100 millisecond intervals. Thunder TPS tracks 28 traffic and behavioral indicators and can apply escalating protocol challenges to surgically identify attackers from valid users for appropriate mitigation of up to 128 million concurrent tracked sessions.

And when attacks grow beyond an organization's bandwidth capacity, traffic is diverted to the A10 DDoS Protection Cloud, which works in concert with Thunder TPS to provide full-spectrum protection against attacks of any type. The service is backed by purpose-built, globally distributed scrubbing centers scaled to handle the largest known DDoS volumetric attacks, all orchestrated by A10's DDoS Security Incident Response Team (DSIRT).

THUNDER 14045 TPS

THE INDUSTRY'S HIGHEST PERFORMANCE APPLIANCE

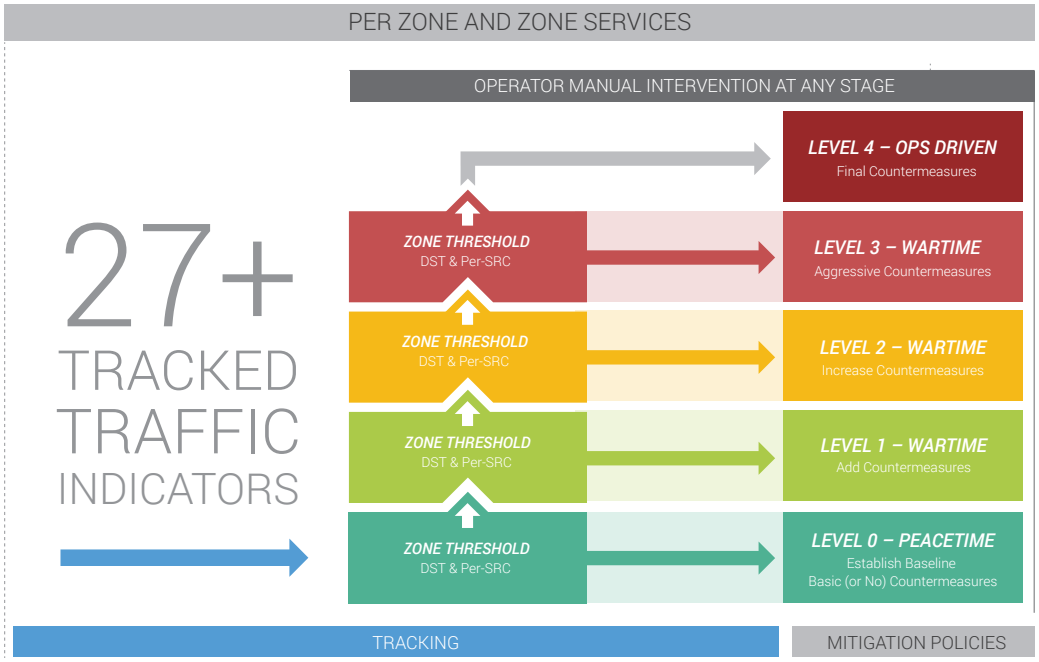
Throughput	300 Gbps
Packets Per Second	440 Mpps

PILLAR 3

AUTOMATION TO IMPROVE EFFICIENCY

No organization has unlimited people or resources. Because of that, efficiency is imperative. Yet legacy DDoS defense requires a lot of manual intervention during wartime. In fact, according to a Neustar survey, of the organizations that suffered a DDoS attack, 45 percent were attacked six or more times, requiring an average six people to defend against each DDoS attack. This is unsustainable for any organization. Not only does a DDoS attack diminish availability, it also takes people away from valuable work. Instead of working on tasks that benefit the business, people are pulled into a firefight.

Organizations need automated DDoS protection strategies that eliminate the manual intervention often required to defend against attacks. Leveraging automation based on pre-set policies maximizes effectiveness while minimizing the chances of false positives, thus preserving resources by keeping them focused on important tasks and not battling DDoS.



Managing a DDoS attack is like managing pure chaos. Organizations typically only have a few trained personnel available during an attack, often with more to contend with than they can handle. To maximize personnel effectiveness and tame the commotion of a resource-straining DDoS attack, A10 Thunder TPS supports five levels of programmatic mitigation escalation. Peacetime scenarios are learned and baselined for each protected zone. Administrators create custom policies for each protected service, and Thunder TPS automatically applies the required mitigation at each escalation level.

PILLAR 4

AFFORDABILITY TO MAXIMIZE YOUR BUDGET

Enterprises know they need DDoS defense, but the expense of obtaining it creates a huge obstacle as DDoS defense solutions are quite costly. A rip-and-replace approach is a hard decision to make and one that most businesses want to avoid. However, shedding legacy systems in favor of modern, nimble DDoS defense solutions can have a high return.

It's time to take a fresh look at DDoS defense. To be affordable, solutions need to be high-performance, yet compact by design. One way to shrink DDoS defense spending is to reduce the total number of appliances needed to meet your organization's capacity requirements. This not only reduces hardware costs, it also reduces power, cooling and data-center-space requirements, all of which helps to further decrease your overall expense.

Thunder TPS is an extremely powerful and cost-efficient DDoS defense solution. It delivers high performance in a small form factor to reduce operating expenses (OPEX) with significantly lower power usage, rack space and cooling requirements compared to bulky, legacy systems.

The world's highest-performance DDoS protection solution, Thunder TPS detects and mitigates terabit-sized DDoS attacks at the network edge. It's unmatched with an industry-leading 300 Gbps with 440 Mpps in a single appliance that offers up to 11 times the performance of legacy solutions with a lower total cost of ownership.

It is available in multiple deployment options and cost structures that make economic sense and deliver complete detection, mitigation and reporting.

VENDOR & ENTERPRISE ON-PREMISE SOLUTION

	A10 Thunder 14045	Arbor APS 2600	Radware DP 2016
Performance	5 Gbps	4 Gbps	4 Gbps
Bypass	Yes	Yes	Yes
Size	1 RU	2 RU	2 RU

DDOS DEFENSE NOW

Modern DDoS attacks require a new approach. They're bigger. They're faster. They're wider. They're more powerful than ever before. Legacy systems can no longer keep up, and they crumble under the might of today's DDoS attacks. But rethinking your DDoS strategy isn't easy; it takes careful consideration, thoughtful planning and a robust strategy.

How do you find the right DDoS protection to go toe-to-toe with today's unyielding threat environment? By examining and prioritizing the four key pillars of impenetrable DDoS defense: precision, scalability, automation and affordability.

A10 delivers bulletproof DDoS defense that is comprehensive and cost-effective and ensures that real-time service availability remains uninterrupted.

To learn more about A10's full spectrum DDoS defense solutions, visit a10networks.com/ddos

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @A10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-WP-21150-EN-01 APRIL 2018