WHITE PAPER

6 CRITICAL CONSIDERATIONS BEFORE YOU SPEND ANOTHER $1 ON SERVICE PROVIDER DDOS DEFENSES

How to Achieve Effective and Profitable DDoS Resilience

TABLE OF CONTENTS

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and non infringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

EXECUTIVE SUMMARY

Like any business, service providers are vulnerable to crushing multi-vector distributed denial of service (DDoS) attacks carried out for political, social, criminal or competitive reasons. However, service providers must also contend with the DDoS domino effect: the added challenge of protecting their infrastructure from targeted attacks against subscribers that cause collateral damage to infrastructure and other unsuspecting business customers.

Building affordable, scalable defenses and monetizing investments through value added scrubbing services to business customers is challenging, especially when working with older, established vendors. After the sticker shock of doubling or tripling defenses with incumbent vendors wanes, service providers realize they need a modern alternative that adds pinpoint precision with lower operating overhead. They need a solution that is scalable and makes economic sense, while ensuring future protection.

It's your money and your business' reputation on the line. Doing things the old way is expensive and ineffective against increasingly sophisticated attackers. A10 Thunder TPS™ (Threat Protection System) is a surgical multi-vector DDoS protection solution that ensures availability of your business services at any scale. It's available in a wide range of form factors that make economic sense for your business.

This paper outlines six critical considerations that operators must investigate before making any additional investments into their existing DDoS defenses. A wise investment results in a significant payoff.

#1

WHY PRECISION MATTERS

When it comes to DDoS defense, the focus should always be on ensuring critical services are available to legitimate users. Although DDoS attacks are by nature largely brute-force, DDoS defenses must be surgical and intelligently distinguish legitimate users from attacking bots. Strategies like Remote Triggered Black Hole (RTBH) and service rate limiting should be the last courses of action, not the first, because these strategies are indiscriminate and achieve the attacker's goals of blocking availability of services to legitimate users. A10 Thunder TPS includes many strategies for surgically detecting and mitigating malicious DDoS behavior. Thunder TPS:

- Tracks more than 27 behavioral traffic indicators with surgical mitigation to distinguish attackers from legitimate users
- Initiates source-based mitigation at scales up to 128 million concurrent sessions
- Provides automatic peacetime learning and anomalous threshold settings
- Blocks protocol and application anomalous behavior
- Initiates authentication challenges at L4-L7
- Limits application request rates by query (request) type
- Integrates current, accurate threat intelligence to stop known bad actors
- Provides policy-based automatic mitigation severity escalation
- And more

Surgical precision lowers operating costs by minimizing the number of false incidents that consume frontline defenders from critical tasks. More importantly, surgical DDoS defenses are transparent to subscribers. Let us look at examples to clarify the point.

FALSE POSITIVE – WOLF, WOLF, WOLF

False positives are the bane of IT operations. Mistaken events block legitimate users and require a frontline operator to waste time on forensic analysis of non-existent events. Many of these false positives can be eliminated with a surgical detection and mitigation approach.

Example: Effective DDoS defenses should have two goals. The first goal is to keep the system available for legitimate users; the second is to protect systems and services from being overwhelmed. However, not all mitigation strategies are equal. In fact, many of the industry's commonly used mitigation strategies are plagued with false positives that cause collateral damage against legitimate users. This is because these strategies are focused on protecting systems with rate limits to prevent system failure. While this is one approach, it misses the point of why the system is in place to begin with, which is generating revenue or creating value from legitimate internal and external users.

The right strategy for DDoS defenses is to take a two-step approach. First, distinguish legitimate users from attacking bots, while only blocking the attacking bots. Although more advanced, in most cases surgically mitigating bots as a source of the attack will achieve greater system stability. Only when the attack threatens to knock the system offline should indiscriminate destination rate limits be applied.

You may ask, why do legacy DDoS products jump to destination-based mitigation so quickly? The reason is that tracking thousand or millions of sources is compute-intensive and the more distributed the attack, the the more taxing it is on limited compute and memory resources. Whereas enforcing destination rate limits is computationally easy, but creates collateral damage against legitimate users.

Thunder TPS is based on A10's Advanced Core Operating System (ACOS®) data processing engine that is able to tracks user behavior of up to 128 million sources concurrently in a single appliance. It initiates source-based authentication challenges and applies limits only to policy violators that deviate from learned, normal behavior. By using the Thunder TPS five stage automated mitigation escalation, defenders build policies with increasing severity of mitigation, which greatly reduces false positives.

FALSE NEGATIVE – WHAT ATTACK?

False negatives, conversely, are total misses. No alert is generated during a real event, eventually leading to an embarrassing customer notified escalation.

Example: Today, attackers have weaponized their botnets with sophisticated multi-vector capabilities that try to mimic real users. Attacks generated by smart bots are the most challenging to deflect with legacy solutions that largely rely on tracking bits per second (bps, bandwidth) or packets per second (pps, rates) to detect anomalous traffic. Bps and pps are effective in detecting obvious volumetric attacks, but miss many attacks that utilize less noisy, more sophisticated approaches like resource starvation or slow-low application attacks, with devastating consequences.

Bots, by their nature, will deviate from human behavior. The challenge is to find the deviation from learned normal behavior by tracking multiple behavioral characteristics that go beyond bps and pps.

Thunder TPS tracks more than 27 traffic indicators as well as applications layer access characteristics. By tracking every session for deviation of multiple indicators and applying surgical mitigation, Thunder TPS greatly reduces the number of attacks missed by legacy BPS and PPS techniques.

TCP-BASED SERVICE		UDP-BASED SERVICE	ICMP	IP PROTOCOL OTHER
Packet Rate	Small Payload Rate	Packet Rate	Packet Rate	Packet Rate
SYN Rate	Bytes-to / Bytes-from	Packet Drop Rate	Packet Drop Rate	Packet Drop Rate
FIN Rate	Syn Rate / FIN Rate	Bytes-to / Bytes-from	Fragment Packet Rate	Fragment Packet Rate
RST Rate	Session Miss Rate	Pkt Drop / Pkt Rcv'd	Pkt Drop / Pkt Rcv'd	Bytes-to / Bytes-from
Small Window ACK Rate	Packet Drop Rate	Concurrent Sessions	Concurrent Sessions	Pkt Drop / Pkt Rcv'd
Empty ACK Rate	Pkt Drop / Pkt Rcv'd			
Concurrent Sessions				

Figure 1: Examples of Thunder TPS tracked traffic indicators

HTTP	DNS	SSL
Slow-Low Attack Check	ANY Query Check	Renegotiation Limit
Malformed Check	Malformed Check	SSLv3 Check
Get Request (Per Destination, Source)	FQDN Label Check	Connection Request
Post Request (Per Destination, Source)	Per Query Type (Per Destination, Per Source) - A,AAAA, CNAME, MX and Many More	
Based on Size of HTTP Response		

Figure 2: Examples of Thunder TPS tracked application access

#2

PERFORMANCE BY DESIGN ENABLES COST EFFECTIVE SCALE UP

To combat the swell in DDoS activity, service providers must make new investments in DDoS defense solutions. As mentioned, business units have suffered sticker shock when investigating expanding, doubling or tripling their DDoS defense capabilities with older, established providers.

Service providers benefit from A10 Networks' solutions because Thunder TPS was designed to deliver high performance with surgical precision to increase the effectiveness of DDoS defense. It is available in a range of form factors that make economic sense to businesses of any size. Thunder TPS offers unrivaled scale, enabling you to reduce the number of units your business must purchase, which has a dramatic positive impact on TCO and overall reliability.

COMPARISON AGAINST OLDER ESTABLISHED VENDORS' FLAGSHIP PLATFORMS

VENDOR & FLAGSHIP APPLIANCE	A10 Thunder 14045	Arbor Networks TMS 5000	Arbor Networks* TMS HD 1000	Radware* DP model 400-160
Network interfaces speed available	40 GbE 100 GbE	40 GbE 100 GbE	No 40 GbE or 100 GbE	40 GbE 100 GbE
Rack units (RU)	3 RU	6 RU	2 RU	2 RU
Mitigation bandwidth	300 Gbps	100 Gbps	160 Gbps	160 Gbps
Mitigation packets per second	440 Mpps	40 Mpps	110 Mpps	330 Mpps
Number of appliances and RU needed to match Thunder 14045 bandwidth capabilities	1 appliance 3 RU	3 appliances 18 RU	2 appliances 4 RU	2 appliances 4 RU
Number of appliances and RU needed to match Thunder 14045 packet rate capabilities	1 appliance 3 RU	11 appliances 66 RU	4 appliances 8 RU	2 appliances 4 RU

* *As advertised on the vendor websites. Highest performance advertised appliance from the vendor may or may not be in production at the time of this documents reading.*

COMPARISON AGAINST LEGACY FLOW-BASED DETECTOR

VENDOR	A10	Arbor Networks
Flagship flow detection appliance	aGalaxy with integrated TPS detector	SP 7000
Max flow per second (fps) processing rate	500K fps	240K fps

A10 solutions deliver the most performance per appliance over older, established providers, and Thunder TPS can scale to 2.4 Tbps with a list synchronization cluster.

#3 SCALE OUT TO PROTECT INFRASTRUCTURE AND BUSINESS SUBSCRIBERS

Service providers' network infrastructures are large and complex. When protecting downstream business customers, the number of hosts and services that must be protected can expand into the many thousands. Thunder TPS supports these large networks through either Protected Destination or Protected Zones to ensure DDoS defense investments can be effectively monetized at scale as a scrubbing service.

PROTECTION MODE	MAXIMUM IP AND SUBNET	NOTES
Protected Destination	64,000	Individual IP or network subnet
Protected Zone	512,000 with up to 3,000 active Protected Zones	Each Zone includes up to 512 IPs, subnets and the services provided by the hosts

There is another element of scale we need to consider: breadth. One thing missing from the vast coverage of the Mirai attack in the fall of 2016 is that attacks are growing in breadth and are increasingly distributed geographically. These trends will bring compute bound legacy DDoS defense to its knees. Thunder TPS, however, has the ability to track up to 128 million sessions without sampling or taking other short cuts that impact effectiveness at the most crucial times. Also, by leveraging Thunder TPS massive Class-list size of 96 million entries, blacklisting known bad actors with A10's threat intelligence can be done at Internet scale.

An additional benefit of using A10's threat intelligence is network efficiency. According to an Imperva report (Bot Traffic Report, 2017), bad botnet traffic accounts for 28.9 percent of the total Internet traffic.

BAD BOTNET TRAFFIC ACCOUNTS FOR

28.9% OF THE TOTAL INTERNET TRAFFIC

Imperva (Bot Traffic Report, 2017)

That is an astounding number. Bad botnets, in addition to being agents for DDoS attacks, are the foot soldiers running reconnaissance scans against your infrastructure, spamming websites and scraping content. Following this line of thought, nearly a third of a service provider network is clogged with traffic the operator has no intention to service. By leveraging Thunder TPS' Class-list, which is populated with current, accurate threat intelligence of known malicious bots, operators can dramatically improve bandwidth efficiencies throughout their network, while reducing the attack surface.

What could your organization do if it could get back 28.9 percent of the network and eliminate the damage done by bad bots?

SOURCE TRACKING BREADTH	*MAXIMUM UNITS*	*NOTES*
Concurrent monitored sessions	128 million	Track every session, no sampling required
Blacklist-whitelist known good and bad IPs	Up to 96 million entry Class-list, with up to 16 million entrys per list	Operator created and A10 threat intelligence feed, updated every two hours by default

24% | 24 hrs *ON AVERAGE, 24% OF THE IPS AND DOMAINS IN OUR THREAT INTELLIGENCE CHANGES EVERY 24 HOURS*

Current, accurate threat intelligence, powered by ThreatStop

#4 *DEPLOYMENT FLEXIBILITY IMPROVES BUSINESS OBJECTIVES*

The first step in building DDoS defense is choosing the right deployment architecture for your business objectives. There are two primary DDoS deployment modes: reactive and proactive. Each deployment mode has benefits and drawbacks an operator should consider.

REACTIVE DEPLOYMENT ARCHITECTURE

Reactive deployments leverage flow records from edge routers to gain metadata visibility of traffic to detect anomalies suspected of being a DDoS attack. Once an anomaly is detected, a signal is sent to change the routing structure and the suspected traffic is diverted to a pool of packet-based detection and mitigation appliances to scrub the traffic clean then re-route that traffic to the desired destination.

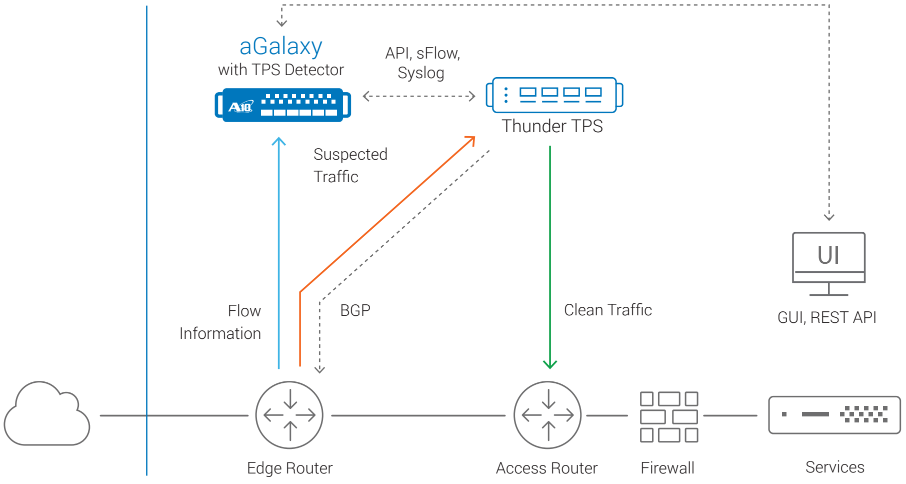


Figure 3: Reactive deployment topology

Larger networks benefit from reactive architectures from the cost savings of deploying oversubscribed mitigation sized to a fraction of the total edge network capacity. Thunder TPS fits any network configuration with integrated BGP and other routing protocols. This eliminates the need for any additional diversion and re-injection routers. Reactive mode features:

- Anomaly detection using edge router flow records
- 100 percent metadata resolution visibility to all edge traffic
- Mitigation that can be scaled to a fraction of total traffic and applied as needed

BENEFITS

- Less expensive for larger networks due to oversubscribed mitigation
- User traffic is uninterrupted during peacetime
- Flow data is already available for other network monitoring functions
- Effective against volumetric and most network protocol attacks

DRAWBACKS

- Slower to detect and mitigate attacks compared to proactive deployments
- Less effective against resource exhaustion attacks
- Not effective against application layer attacks
- Added risk due to mitigation scaled to a fraction of total ingress traffic

PROACTIVE DEPLOYMENT ARCHITECTURE

Proactive deployment is an always-on, high precision defense strategy. DDoS detection and mitigation are accomplished from a single appliance placed inline, most commonly at the edge of the network or at peering locations.

Proactive mode provides continuous, comprehensive detection and faster mitigation. This mode is most useful where user experience is critical. Thunder TPS supports L2 or L3 in path deployments. L3 deployments eliminate the need for network interruption at installation or during required maintenance windows by utilizing integrated dynamic routing protocols and ECMP.

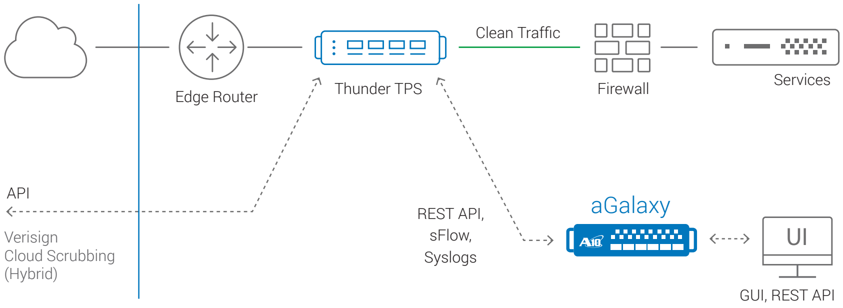


Figure 4: Proactive deployment topology

PROACTIVE MODE DELIVERS

- Detection and mitigation at the edge
- High-resolution packet-level visibility of all traffic at all times
- Detection and mitigation sized to equal the edge ingress or the specific service being protected

BENEFITS

- Highest precision packet-based detection
- Thunder TPS detection and mitigation down to 100ms intervals
- Detects and mitigates all forms of DDoS attack, including slow and low application attacks

DRAWBACKS

- Can be expensive for larger networks due to no oversubscription capabilities

BLENDED PROACTIVE AND REACTIVE DEPLOYMENT FOR SERVICE PROVIDER NETWORKS

Service provider networks are complex and sprawling environments that have differing availability risk attributes per service or elements of the infrastructure. A10 DDoS defense solutions provide the flexibility in deployment architectures to match operators' business objectives.

RECOMMENDED DEPLOYMENT ARCHITECTURE FOR BUSINESS OBJECTIVES

	Proactive	**Reactive**
Volumetric attack protection		✓
Bi-directional protection	✓	✓
Protect critical DNS services from all categories of attacks	✓	
Protect real-time IMS infrastructure	✓	
Protect internal hosted client	✓	✓
Protect external hosted client		✓
Managed security services	✓ Customer premises	✓ Clean pipe
Business customer scrubbing service		✓

For service providers, utilizing reactive deployments to protect data services and downstream business customers, then layering proactive defenses for critical services (DNS, IMS, etc.), provides the best strategy for managing availability risk and achieving business objectives.

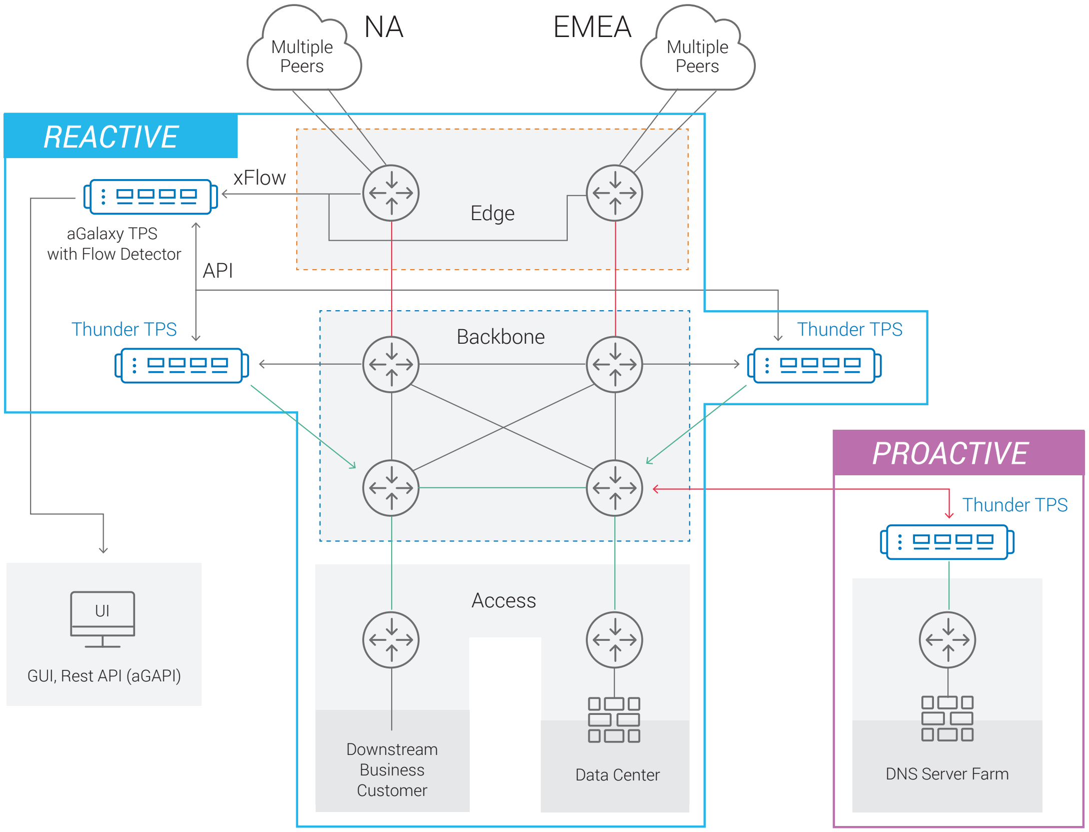


Figure 5: Blended proactive and reactive deployment

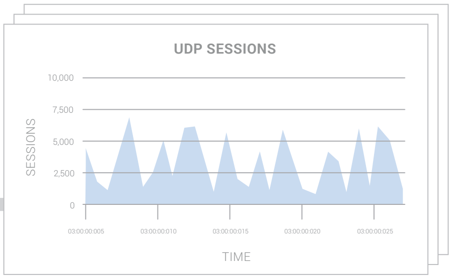
#5 *GET THE MOST OUT OF YOUR TIME-STRAPPED FRONTLINE DEFENDERS*

No organization has unlimited trained personnel or resources. To maximize personnel effectiveness while under attack, Thunder TPS supports five levels of programmatic mitigation escalation and de-escalation against learned peacetime baselines per Protected Zone and service. Administrators can create custom policies for each protected service and Thunder TPS automatically applies the required mitigations at each escalation level. This removes the need for frontline personnel to make time-consuming manual changes, minimizes collateral damage against legitimate users and improves response times during attacks. Administrators have the option to manually intervene at any stage of an attack.

EXAMPLE ESCALATION POLICY FOR DNS DEFENSE

	TRACKED INDICTORS	*MITIGATION APPLIED*	*ACTION*
LEVEL 4 – WARTIME Final Countermeasures	Continue tracking indicators Zone threshold 4	BGP black hole signaling Administrator manual intervention All level 3 mitigations	Create custom regular expression Create custom Berkley Packet Filter Log
LEVEL 3 – WARTIME Increase Countermeasures	Continue tracking indicators Zone threshold 3	DNS-authentication-force-tcp Dst-rate-limit-request All level 2 mitigations	Advanced challenge Drop Destination rate limit Blacklist source Log
LEVEL 2 – WARTIME Increase Countermeasures	Continue tracking indicators Zone threshold 2	DNS-authentication-force-retry Malformed-DNS-query-check-extended Src-rate-limit-by-request-type All level 1 mitigations	Challenge Drop Source query type rate limit Blacklist source Log
LEVEL 1 – WARTIME Add Countermeasures	Continue tracking indicators Zone threshold 1	Malformed-DNS-query-check-basic DNS-any-check FQDN-label-length FQDN-rate-limit-domain-name-suffix FQDN-label-count All level 0 mitigations	Drop FQDN check Source rate limit Blacklist source Log
LEVEL 0 – PEACETIME Establish Baseline, Minimum Countermeasures	TCP-conn-miss-rate TCP-pkt-drop-ratio TCP-syn-rate TCP-src-threshold TCP-zone-threshold UDP-pkt-drop-ratio UDP-pkt-rate UDP-src-threshold UDP-zone-threshold	FTA L3/L4 packet anomaly check	Drop Log

TRACK 27+ INDICATORS FOR AUTOMATED ESCALATION AND DE-ESCALATION



Learned Normal Traffic Behavior

Figure 6: Auto-mitigation and auto-escalation example

#6 OPEN AUTOMATION FOR SECOPS - 100% PROGRAMMABLE API

New customers benefit from A10's flexible controls available via an easy to use graphical user interface (GUI) or a powerful yet familiar command line interface (CLI). A10 provides guides, samples and easy-to-modify prebuilt configurations and templates to simplify initial setups and ongoing operational enhancements.

However, many organizations are moving to agile SecOps/DevOps models with system-wide orchestration to speed delivery of applications, virtual infrastructures and their defenses. Like many other network equipment vendors, A10's DDoS solution offers a RESTful application programming interface (API) to facilitate automation. A10 differs from legacy DDoS products in the openness of the system. All functions accessible via CLI are also configurable through API calls for maximum programmability. Additionally, Thunder TPS offers thousands of statistics delivered through the API as well as the sFlow counter block export mechanism for high efficiency when dealing with large volumes of statistical data.

Many A10 customers have benefited from A10's openness and 100 percent programmable API, as they transitioned away from legacy vendors' closed systems.

HOW IT WORKS

A10's DDoS defense detects and mitigates multi-vector DDoS attacks at the network edge and scales to defend against the DDoS of Things and traditional zombie botnets. It does this by tracking more than 27 traffic behavioral indicators and applying surgical mitigation against learned peacetime traffic to detect anomalous behavior and surgically distinguish legitimate users from attacking bots. Multiple layers of protection are provided for infrastructure and services that include source-based rate limiting, authentication challenges, abusive behavior blocking, blacklisting and more.

Thunder TPS provides extensive customization capabilities from the graphical user interface (GUI), command line interface (CLI) or over open API to ensure defenders' services are resilient to multi-vector DDoS attacks.

THUNDER TPS DEFENSE COMPONENTS

A10 DDoS defense are comprised of three key components: Thunder TPS, Thunder TPS Detector and aGalaxy. These components can be modularly deployed to scale to the demands of any network environment.

Thunder TPS

- Surgical mitigation
- Proactive or reactive deployment with integrated BGP, OSPF, IS-IS protocols
- Fast 100 ms detection and mitigation intervals

Thunder TPS Detector

- Flow-based DDoS detector
- Peacetime learning
- Fast 3-second detection

aGalaxy

- Manage and orchestrate
- Unified dashboard and reporting
- Real-time mitigation console

THUNDER TPS DETECTOR

Reactive DDoS detection is facilitated through the collection and analysis of exported flow data records from routers and switches for IPv4 and IPv6 traffic. Thunder TPS Detector enters traffic behavioral-learning mode to build a peacetime profile for Protected Zones. Once in monitoring mode, the flow-based detector tracks up to 17 flow data traffic indictors to spot anomalous behavior for inbound or bi-directional traffic. When an attack is detected, the flow-based DDoS detector alerts aGalaxy TPS to instruct Thunder TPS to apply appropriate mitigation templates and initiate a BGP route change of the suspicious traffic for DDoS scrubbing before delivering the clean traffic to the intended destination.

THUNDER TPS

Thunder TPS is the heart of A10's DDoS defense. When Thunder TPS is put in-path with suspicious traffic, it detects and mitigates DDoS attacks of many types, including volumetric, protocol or resource attacks; and application-level and IoT-based attacks. Hardware acceleration offloads the CPUs and makes Thunder TPS particularly adept to deal with simultaneous multi-vector attacks.

Thunder TPS tracks more than 27 traffic behavioral indicators and can apply escalating authentication challenges to surgically identify attackers from valid users. Powered by A10's Advanced Core Operating System (ACOS) with advanced parallel processing, it can do this at a scales up to 128 million concurrently tracked sessions. Embedded SSL security processors offload CPU intensive tasks, and mitigate SSL/TLS-based attacks. Therefore, high-performance system scaling is maintained, even for multi-vector attacks.

AGALAXY FOR THUNDER TPS

aGalaxy for Thunder TPS gives organizations a global view of their environments to rapidly identify and remediate attacks, and ensure that policies are consistently enforced from a central point. Administrators can configure, monitor and comprehensively analyze their Thunder TPS deployments to view DDoS attacks in real-time, and drill down to see details of connections handled by an individual protected service.

aGalaxy is available with an optional integrated Thunder TPS Detector that supports tightly integrated orchestration of Thunder TPS DDoS mitigation, flow-based DDoS detection, system-wide management and robust reporting.

CONCLUSION

New threat vectors have changed the breadth, intensity and complexity of options available to attackers. Established solutions, which rely on ineffective, signature-based IPS or only traffic rate limiting, are no longer adequate to defend sprawling service provider networks and their business subscribers against modern DDoS attacks. A10 Thunder TPS offers scalability and precision to defeat the most challenging DDoS attacks, making service provider infrastructure resilient against DDoS attacks.

Unlike outdated DDoS products, Thunder TPS is built on A10's market-proven Advanced Core Operating System (ACOS), which delivers scalable form factors that make economic sense with a complete mitigation, detection and reporting solution.

After you have researched these six critical considerations, give A10 a call and let's get started on a path to a more effective, scalable and profitable approach to DDoS resilience.

NEXT STEPS

To learn more about the A10 Thunder TPS DDoS protection solution, please contact your A10 representative or visit a10networks.com/thunder-tps.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. 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-21147-EN-01 OCT 2017