SOLUTION BRIEF

EFFECTIVE SERVICE PROVIDER DDOS PROTECTION THAT SAVES DOLLARS AND MAKES SENSE

Building effective, affordable and scalable DDoS defense, then monetizing investments with value added scrubbing services to business customers is challenging, especially when working with older, established vendors. After the sticker shock of doubling or tripling defense with incumbent vendors wanes, service providers realize they need a modern alternative that adds pinpoint precision with lower operating overhead, and is scalable and makes economic sense. And it must ensure future protection.

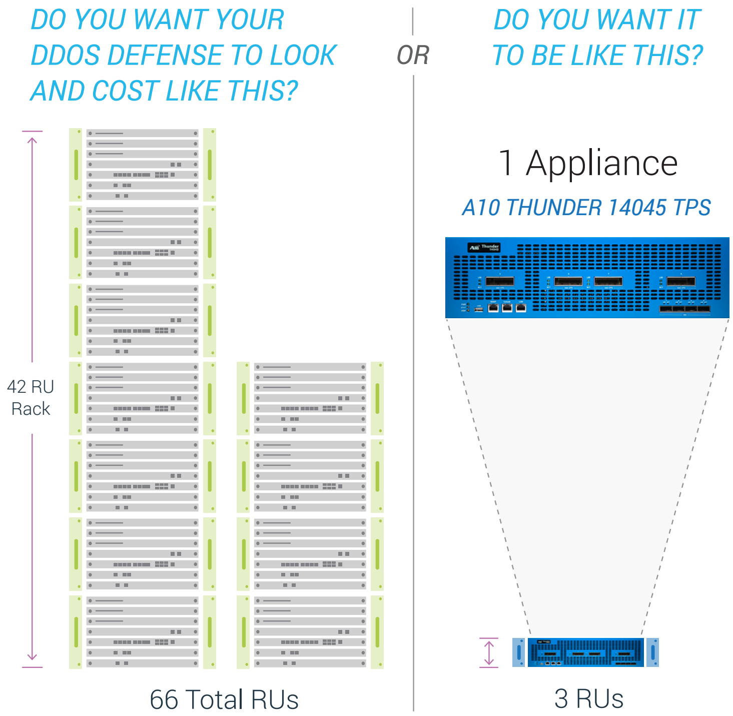

DO YOU WANT YOUR DDOS DEFENSE TO LOOK AND COST LIKE THIS?
OR
DO YOU WANT IT TO BE LIKE THIS?
42 RU Rack
66 Total RUs
1 Appliance
A10 THUNDER 14045 TPS
3 RUs

Figure 1: 440 Mpps with 40/100 GbE interfaces DDoS protection, similar performance, very different investment requirements

CHALLENGE

Service providers play a critical role in ensuring business, government and personal Internet communications are reliable and resilient against DDoS attacks, but building effective and scalable DDoS defense that are operationally effective, scalable and profitable is challenging.

SOLUTION

A10 Thunder TPS™ (Threat Protection System) is a surgical, multi-vector DDoS protection solution that ensures availability of business services at any scale. It's available in a wide range of form factors that make economic sense for service providers.

BENEFITS

- Ensure provider's network and services are resilient to multi-vector DDoS attacks
- Monetize DDoS protection investments with downstream business subscriber scrubbing services
- Protect up to 512,000 host, subnets and services across 3,000 zones
- Scale to 2.4 Tbps in a list synchronized cluster to protect the most challenging environments

THUNDER TPS CAPABILITIES

SURGICAL PRECISION AND INTELLIGENCE

DDoS defense should always focus on ensuring availability of services to legitimate users. Afterall, they are the life blood of your business and frustrated subscribers are not loyal. Although DDoS attacks are, by nature, largely brute-force, DDoS defense must be surgical in intelligently distinguishing legitimate users from attacking botnets. 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, in effect, accomplish the attack's objectives by blocking access to legitimate users.

Unlike legacy DDoS defense that rely primarily on BPS and PPS thresholds, Thunder TPS includes many strategies for surgical detection and mitigation including:

- Automatic peacetime behavioral learning and anomalous threshold setting
- Tracking more than 27 behavioral indicators to spot malicious behavior against applications or services
- Blocking L3-L4 packet anomalies
- Blocking protocol and application anomalies
- Initiating authentication challenges at L4-L7
- Limiting traffic and query rates by source and source sessions
- Mitigating slow and low application attacks
- Current, accurate threat intelligence to stop known bad actors
- And more

Even more important to your business, A10's surgical precision lowers operating costs by minimizing the number of false and missed incidences that consumes frontline defenders from critical tasks.

HIGH PERFORMANCE AND COST-EFFECTIVE

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 for service providers 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.

Figure 2: Thunder 14045 TPS, the industry's highest performance appliance

	THUNDER 14045 TPS
Throughput	300 Gbps
Packets Per Second	440 Mpps

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

SCALABLE PROTECTION FOR INFRASTRUCTURE, SERVICES AND BUSINESS SUBSCRIBERS

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

PROTECTION MODE	MAXIMUM IP AND SUBNET	NOTES
Protected Destination	64,000	Individual IP or network subnet
Protected Zones	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

SOURCE TRACKING BREADTH	MAXIMUM UNITS	NOTES
Monitored concurrent sessions	128,000,000	High resolution, zero sampling
Block known bad actors **Pass known good users**	96 million entries with 16 million entries per Class-list	Administrator specified A10 Threat Intelligence feed

24% | 24 hrs

ON AVERAGE, 24% OF THE IPS AND DOMAINS IN OUR THREAT INTEL ENGINE CHANGES EVERY 24 HOURS

A10 Threat Intelligence Service: current, accurate, powered by ThreatStop

SWIFT RESPONSE TIME DURING WARTIME

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

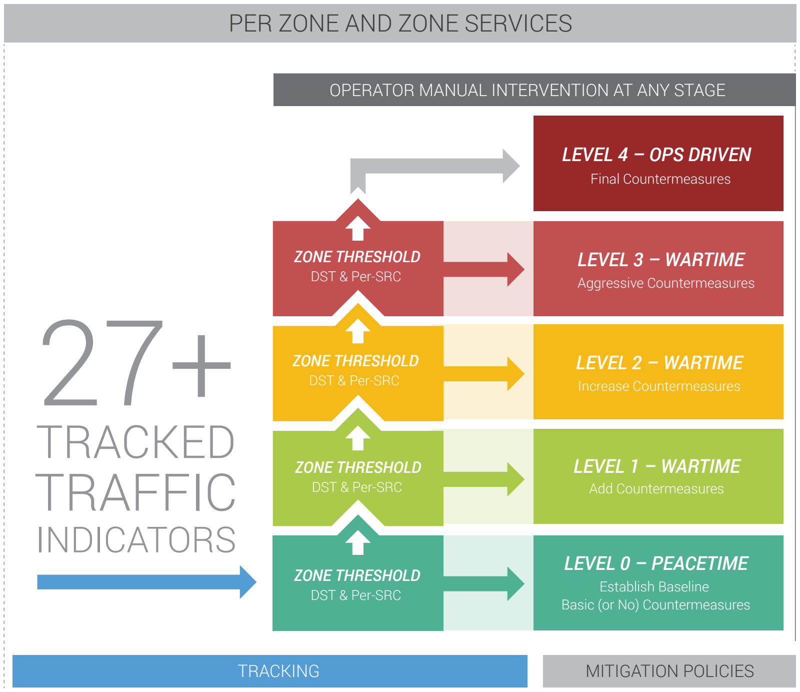


Figure 3: Policy-based automatic mitigation escalation

FLEXIBLE DEPLOYMENT FOR SERVICE PROVIDER NETWORKS

Thunder TPS supports proactive and reactive deployments to optimally support a service provider's business objectives. BGP, OSPF and IS-IS routing protocols support seamless integration into complex service provider environments.

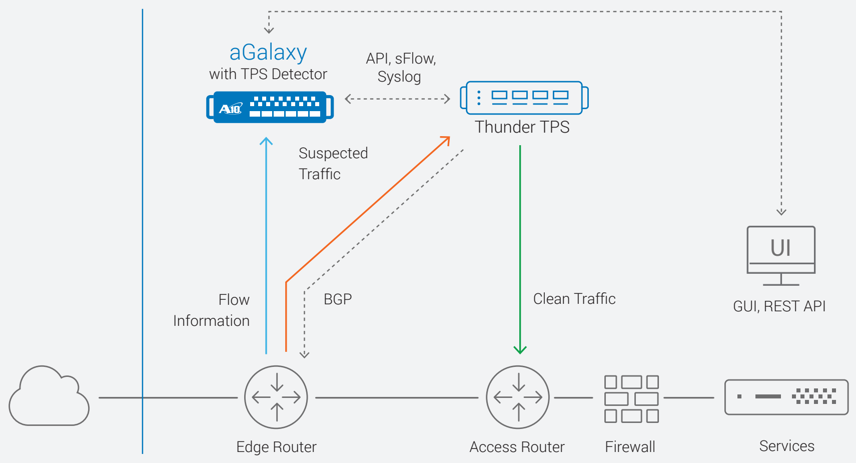


Figure 4: Reactive Deployment

REACTIVE DEPLOYMENT

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 indicators 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 the appropriate mitigation templates. Thunder TPS then initiates a BGP route change of the suspicious traffic for scrubbing before delivering the clean traffic to the intended destination.

Reactive deployments is a cost effective method that allows scrubbing resources to be shared as an oversubscribed protection resource for internal and downstream business customers.

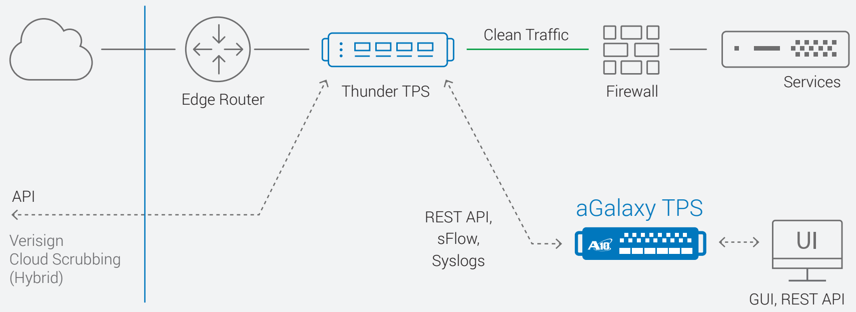


Figure 5: Proactive deployment

PROACTIVE DEPLOYMENT

When Thunder TPS is put in-path proactively, it provides continuous, comprehensive detection and fast mitigation. This mode is most useful where the user experience is critical like DNS and IMS services. TPS supports L2 or L3 in-path deployments. L3 deployment eliminates the need for network interruption during installation and required maintenance windows.

	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		✓

Figure 6: Recommended deployment architecture for service provider business objectives

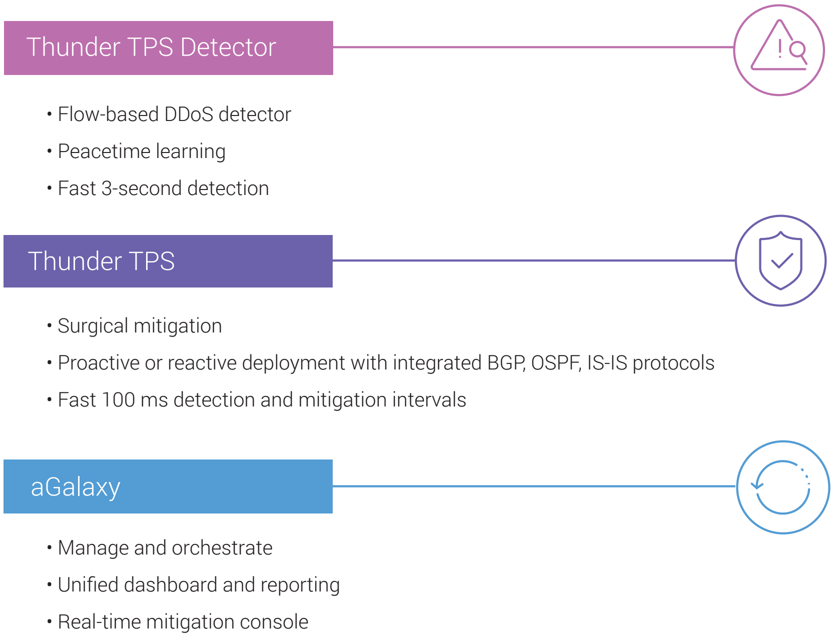
EASY NETWORK INTEGRATION

With multiple performance options and flexible deployment models, Thunder TPS may be integrated into any network architecture of any size, including MPLS. And with aXAPI®, A10's RESTful API, Thunder TPS easily integrates into third-party monitoring and detection solutions.

Figure 7: Monitoring and DDoS detection technology partners

HOW IT WORKS

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



Thunder TPS Detector

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

Thunder TPS

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

aGalaxy

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

Figure 8: Single vendor, total solution

FEATURES AND BENEFITS

- Lower acquisition costs with the industry's highest performance appliance delivering 300 Gbps, 440 Mpps and 128 million concurrent tracked sessions
- Make frontline defenders more effective and lowers operating cost with precision and automated mitigation escalation
- Minimizes collateral damage to legitimate users by tracking 27+ behavioral indicators to identify attackers
- Flexible integration for on-demand reactive deployments and L2 or L3 proactive deployments
- 100 percent API programmable policy engine for easy automated orchestration integration

SUMMARY

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. A10 Thunder TPS offers the scalability and precision to defeat the most challenging DDoS attacks to make service provider infrastructure resilient against DDoS attacks.

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

A10 provides 24x7x365 support and includes the A10 DDoS Security Incident Response Team (DSIRT) to help you analyze and respond to DDoS incidents and attacks. The A10 Threat Intelligence Service leverages global knowledge to proactively stop known bad actors.

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

©2017 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, A10 Lightning, A10 Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-SB-19182-EN-01 OCT 2017