TEST REPORT

TESTING DDOS DEFENSE EFFECTIVENESS AT 300 GBPS SCALE AND BEYOND

Ixia BreakingPoint DDoS Defense Test Methodology Report

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

Distributed denial of service (DDoS) attacks against critical business services are increasing in intensity, frequency and sophistication. To combat this swell in DDoS activity, organizations must make new investments in DDoS defense solutions. Businesses have suffered sticker shock when investigating expanding, doubling or tripling their DDoS defense capabilities with older, established providers. They need better ways to ensure they're investing in solutions that are more effective, scalable and that make economic sense, while also ensuring future protection.

To help companies understand the options available, A10 Networks and Ixia Communications ran a battery of tests to determine the effectiveness at scale of the A10 Networks Thunder® Threat Protection System (TPS™) 14045, the industry's highest performance DDoS mitigation appliance.

For this report, we assaulted the A10 Thunder 14045 TPS with a barrage of volumetric, network protocol and application attacks – real-world attack traffic – using the Ixia BreakingPoint security and applications testing platform.

Fifteen challenging DDoS attack vectors where applied at scales of up to 310+ Gbps with 360,000 attacking agents. The summary finding is that Thunder 14045 TPS, powered by A10 Networks Advanced Core Operating System (ACOS®) processing engine, was able to deflect the attack vectors individually and simultaneously without any impact to legitimate user traffic.

> *"Making investments in new technology is complex because data sheet statistics only tell part of the story. For quantifiable data on how a technology will actually work in their particular network, organizations must test at scale with real-world application traffic and security attacks."*
>
> **Sashi Jeyaretnam** | Director of Product Management, Ixia

TEST RESULT SUMMARY

- Successfully defended 310+ Gbps of attack and legitimate user traffic
- Less than 60% average CPU utilization while under full attack
- Detected and mitigated all fifteen attack vectors
- No interruption to legitmate user while under attack

WHAT IS A DDOS ATTACK?

Denial of service (DoS) is a technique an attacker uses to render an online service inaccessible to legitimate users. DoS attack tools and dark web services come in many shapes and sizes, but all focus on overwhelming the target's infrastructure. For example, a web server can be overwhelmed with excessive fake requests so legitimate requests cannot be met. Often, these attacks come from compromised computers or the Internet of Things (IoT), which are remotely controlled by an attacker and used to send the nefarious traffic. These compromised hosts, known as bots and distributed over the Internet, are enlisted in a botnet. This means the attack is launched from many different, distributed hosts simultaneously; which is why DDoS attacks are called distributed denial of service attacks. Attack traffic accumulates to larger and larger traffic rates, all destined for the victim's IP address.

DDOS TYPES

Technically speaking, DDoS attacks can be divided into several different categories:

VOLUMETRIC ATTACKS

DNS or NTP amplification attacks, are aimed at flooding and saturating a victim's network connection, thus rendering services unavailable. Amplification attacks use bots that send requests with a fake or "spoofed" IP address (the victim's IP address) to a service such as a DNS server, which sends a response much larger than the request to the victim's IP address. All of these responses, coming from many – usually unpatched or poorly configured – Internet servers accumulate large bandwidth data destined for the victim.

NETWORK PROTOCOL ATTACKS

SYN floods, ping of death and IP anomalies are aimed at exhausting a victim's protocol stack so it cannot respond to legitimate traffic. A SYN flood attack, for example, is based on the fact that a server reserves resources for uncompleted connection requests. Eventually the server times out the connection and frees up the reserved resources, but if these requests happen at a high enough rate, the server's resources deplete and it is overwhelmed, and thus it cannot respond to legitimate requests.

APPLICATION ATTACKS

Low-and-slow techniques, HTTP GET flood, DNS flood or SSL-based attacks specifically exploit a weakness in an application's function or attempt to overwhelm the service. The approach is similar; the attack intends to consume all resources of the application, eventually overwhelming it.

DDOS ATTACKS HAVE EVOLVED

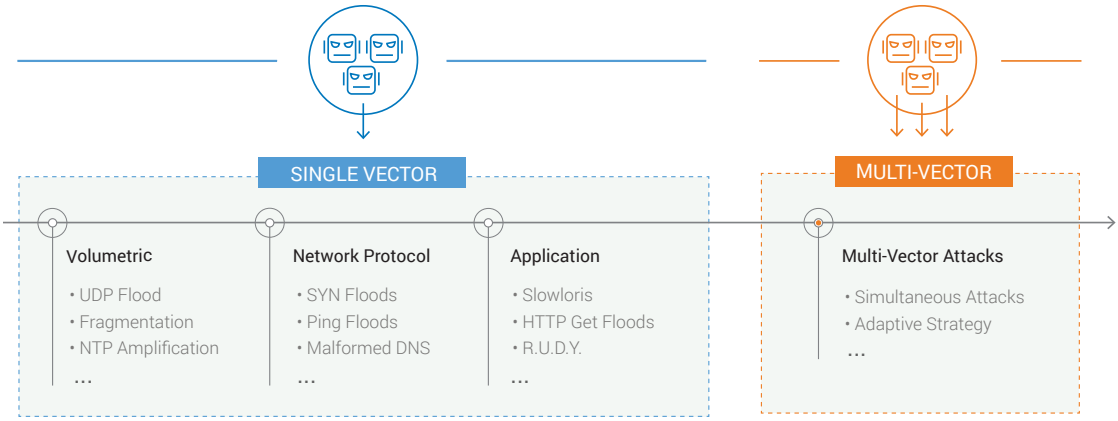


Figure 1: Evolution of multi-vector attacks

MULTI-VECTOR ATTACKS

Multi-vector attacks have become the norm. Attackers have weaponized their botnets with multiple capabilities to search out weaknesses in their target's defenses by applying multiple attack vectors in sequence or simultaneously to create a multi-vector attack. These types of attacks are the most problematic for a defender when combined with scale.

TESTING LOGISTICS

The following results summarize the extensive testing conducted by Ixia at A10 Networks' San Jose, California headquarters in August 2017. The test conducted and the results collected followed Ixia's DDoS defense validation methodology outlined by Ixia on its methodology paper. The DDoS attacks and legitimate user traffic were created by Ixia's BreakingPoint security and application testing platform run on the 100 GbE-enabled CloudStorm hardware system. A10 Thunder 14045 TPS was placed in L3 mode in-path to the Ixia platform to separate the untrusted zone, which included attacker traffic and legitimate user traffic aimed toward target servers in the trusted zone. The success criteria of the test were to monitor the trusted zone to understand how legitimate user traffic was affected during an attack and to determine if the DDoS attack traffic was adequately detected and mitigated.

THE EQUIPMENT USED TO CONDUCT THE TEST

ixia

- BreakingPoint all-in-one applications and network security testing platform, version 8.30.1 with IxOS 8.30EA-Patch1
- XGS12-HSL Chassis
- CloudStorm 100GE Load Module
- Cloud Storm 40GE Load Module

A10

- Thunder 14045 TPS, ACOS version 3.2.2-P1

TEST TOPOLOGY

The test models a large network with an untrusted zone with legitimate users accessing web services and a large number of attacking botnet agents generating DDoS attacks. The trusted zone is the network segment that includes the target servers protected by A10 Thunder TPS.

ITEM	PARAMETER
Untrusted zone physical network bandwidth	340 Gbps networking
# attacking agents defined	360,000
# legitimate user agents defined	138
# protected servers	30

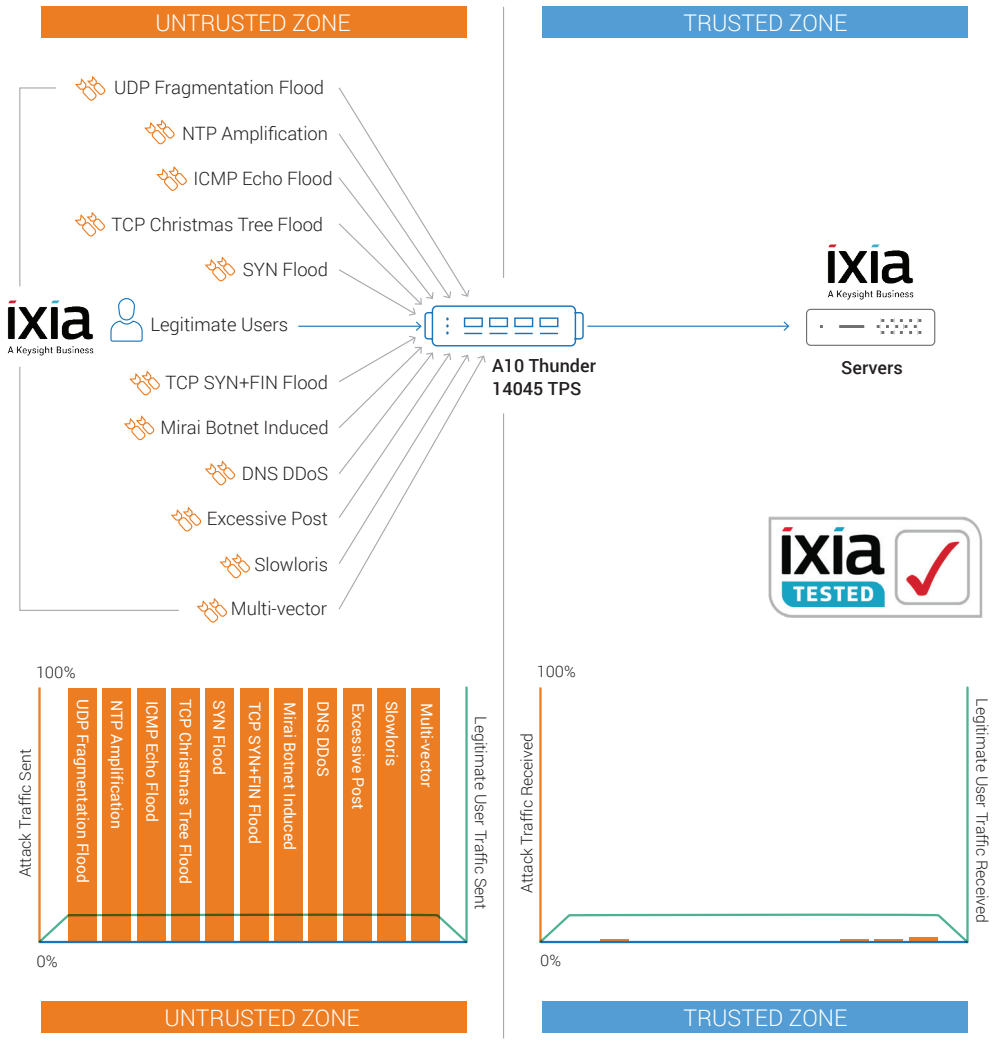


Figure 2: Network topology

The legitimate user traffic models HTTP GET requests and server responses. The attacker traffic comprised fifteen DDoS attack vectors. To determine the effectiveness of Thunder 14045 TPS, a baseline of legitimate users accessing web services was established. This traffic was monitored to understand the impact to legitimate users during an active DDoS attack. First, the DDoS attacks were generated in waves of one attack vector at a time at, followed by a multi-vector attack where all fifteen attacks and legitimate user sessions were applied.

TYPE OF ATTACK	*CATEGORY OF ATTACK*
UDP Fragmentation Flood: Fragmented UDP packet at high rates	Volumetric
NTP Amplification: Bots spoof NTP request to the victims server IP	Volumetric
ICMP Echo flood	Volumetric
TCP ChristmasTree Flood: TCP packet with PSH, URG and FIN flags set without any data, to exploit the protocol and exhaust resources	Network Protocol
SYN Flood: TCP SYN packets with 1024 bytes of data, sent at high rate to exhaust both memory and bandwidth of target	Network Protocol
TCP SYN+FIN Flood: Invalid TCP packet with SYN and FIN flags set, sent at high rate to exploit protocol and exhaust resources	Network Protocol
Mirai Botnet Induced Various Attacks: Variety of attacks including DNS Flood Attack, Botnet HTTP Flood Attack, Botnet UDP Flood Attack, UDP Plain Flood Attack, Valve Source Engine Query Flood Attacks	Volumetric Application Targeted
DNS DDoS: A mix of DNS queries and malformed large DNS requests	Application
Excessive Post: Flood attempts to post large files to web server	Application
Slowloris: HTTP sessions with incomplete header are attempted	Application
A combined multi-vector attack	Volumetric Application Targeted

Figure 3: Attack strategies applied

TEST RESULTS

ESTABLISH LEGITIMATE USER TRAFFIC BASELINE

The legitimate user traffic is modeled as users making HTTP GET requests and the server responses to those requests. These transactions followed normal user traffic patterns and were able to meet all TCP and HTTP authentication challenges.

PARAMETER	MEASURED RESULTS	NOTES
Average Throughput	GET request 300 Mbps GET response from server 5 Gbps	10,000 concurrent connections
Average Latency - Time To First Byte (TTFB)	8.6 ms	

Figure 4: Legitimate user traffic characteristics

Repeated HTTP GET requests were applied throughout the tests, and 5 Gbps of response traffic was sent back to the legitimate users without interruption during peacetime and while under attack.

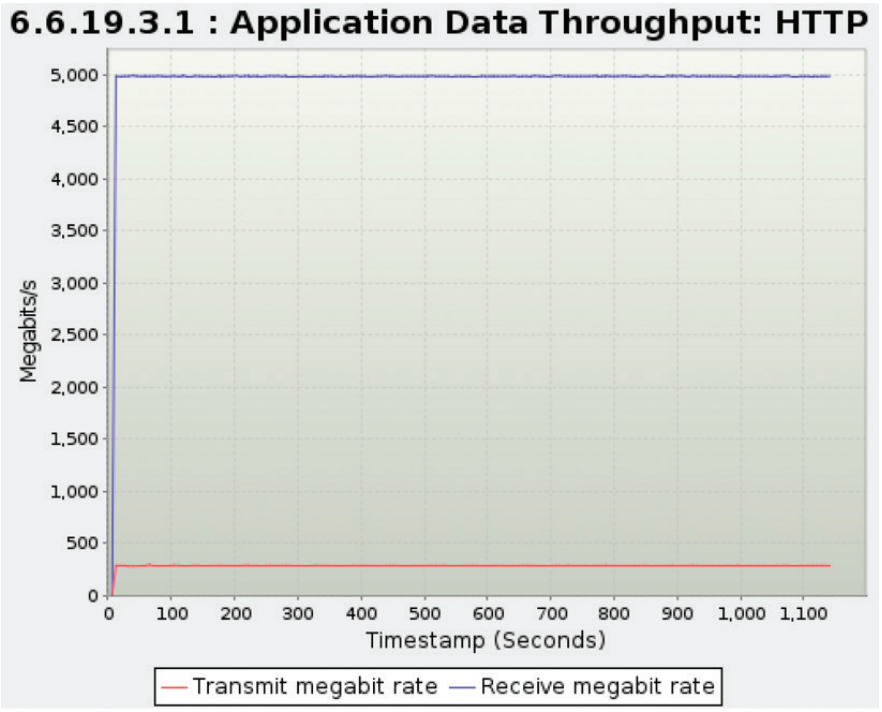


Figure 5: Unaffected legitimate users HTTP GET and responses (from BreakingPoint report)

SECURITY EFFECTIVENESS FOR EACH ATTACK TYPE

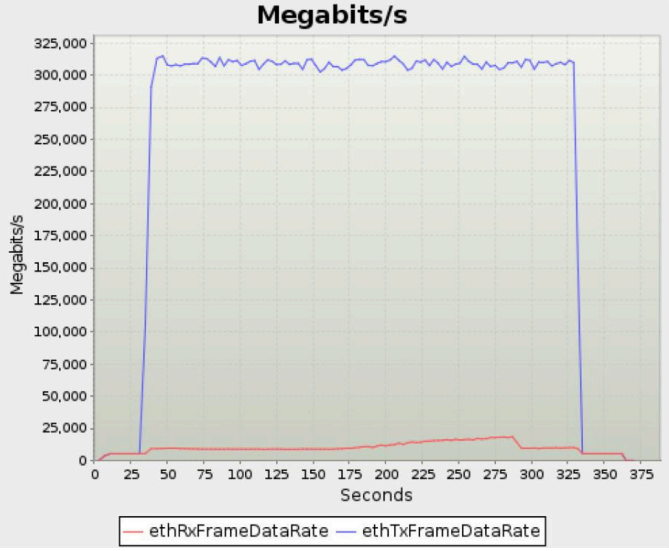
ATTACK STRATEGY		MITIGATION STRATEGY	RESULTS	
ATTACK TYPE	**ATTACK VOLUME OR RATE SENT**	**MITIGATION APPLIED**	**MITIGATION EFFECTIVENESS**	**IMPACT TO LEGITIMATE USERS**
Excessive HTTP POST	75 Gbps	HTTP Challenge POST rate limit	100%	0%
Slowloris	3 M simultaneous HTTP sessions at a rate of 100K sessions per second	Slow and low attack protection	100%	0%
Mirai	50K attacker at 100 Kpps	Drop traffic destined to undefined port Drop traffic from well known source port	100%	0%
NTP Amplification	90 Gbps	Drop traffic from well known source port Drop fragmented UDP packet	100%	0%
DNS DDoS	50 Gbps with 2M DNS queries per second	DNS authentication challenge DNS malformed query check Drop fragmented UDP packet	100%	0%
TCP Christmas Tree Flood	24 Mpps	Protocol anomaly filter done by hardware	100%	0%
SYN Flood	100 Gbps	TCP SYN authentication Drop traffic destined to undefined port	100%	0%
UDP Fragmentation Flood	100 Gbps with 9 Mpps	Drop fragmented UDP packet	100%	0%
TCP SYN+FIN Flood	23 Mpps	Protocol anomaly filter done by hardware	100%	0%

SECURITY EFFECTIVENESS MULTI-VECTOR ATTACK AT SCALE

ATTACK STRATEGY		RESULTS	
ATTACK TYPE	ATTACK VOLUME OR RATE SENT	MITIGATION EFFECTIVENESS	IMPACT TO LEGITIMATE USERS
Multi-vector – all of the individual attacks run together + ICMP echo flood	Aggregate traffic of 310 Gbps with 52 Mpps	100%	0%

Component	Test Results
ICMPEcho_Flood_Wave2	Test passed
SynFlood Wave2	Test passed
Server_Destination	Test passed
LegitimateHTTPClient	Test passed
DDoSChristmassTree_Wave2	Test passed
Syn_FIN_DDoS_Flood_Wave2	Test passed
NTPAmplificationWave2	Test passed
DNS_Malformed	Test passed
SynFlood Wave2 V2	Test passed
UDPFragmentationWave2	Test passed
DDoSDNS_Wave2	Test passed
ExcessivePostWave2	Test passed
Slowloris_Wave2	Test passed
MiraiAttackWave2	Test passed
Overall	Test passed

Figure 6: BreakingPoint test results summary (from BreakingPoint report)



"A10 Thunder TPS proved itself a powerful mitigation solution against all attack vectors, and simultaneously ensures service availability of legitimate users."

Amritam Putatunda
Technical Product Manager, Ixia

Figure 7: Aggregate BreakingPoint 310+ Gbps untrusted traffic and returned responses (from BreakingPoint report)

DDOS DEFENSE OBJECTIVES

When it comes to DDoS, the focus should always be on the legitimate user and ensuring that critical services are available to them. Although DDoS attacks are, by nature, largely brute force attacks, DDoS defense must be surgical and able to intelligently distinguish legitimate user traffic from attacking bot behavior. Strategies like Remote Triggered Black Hole (RTBH) and service rate limiting should be the last course of action, not the first, to prevent the service from falling over, because these strategies are indiscriminate and in effect help the attacker accomplish their objective of blocking availability of services to legitimate user.

Effective DDoS solutions will include many strategies for detecting and mitigating malicious DDoS behavior, including:

- Peacetime traffic behavioral learning and anomalous behavioral threshold setting
- Tracking of multiple behavioral indicators to spot deviation from normal patterns to applications or services
- Inspection traffic for anomalies at L3-L4
- Inspect traffic for protocol and application anomalous behavior
- Initiate authentication challenges at L4-L7
- Limit source session initiated traffic and query rates at network and application layers
- Policy-based automated mitigation severity escalation
- Integrates current, accurate threat intelligence at internet scale to stop known bad actors
- Offer an open API for automated orchestration
- And more

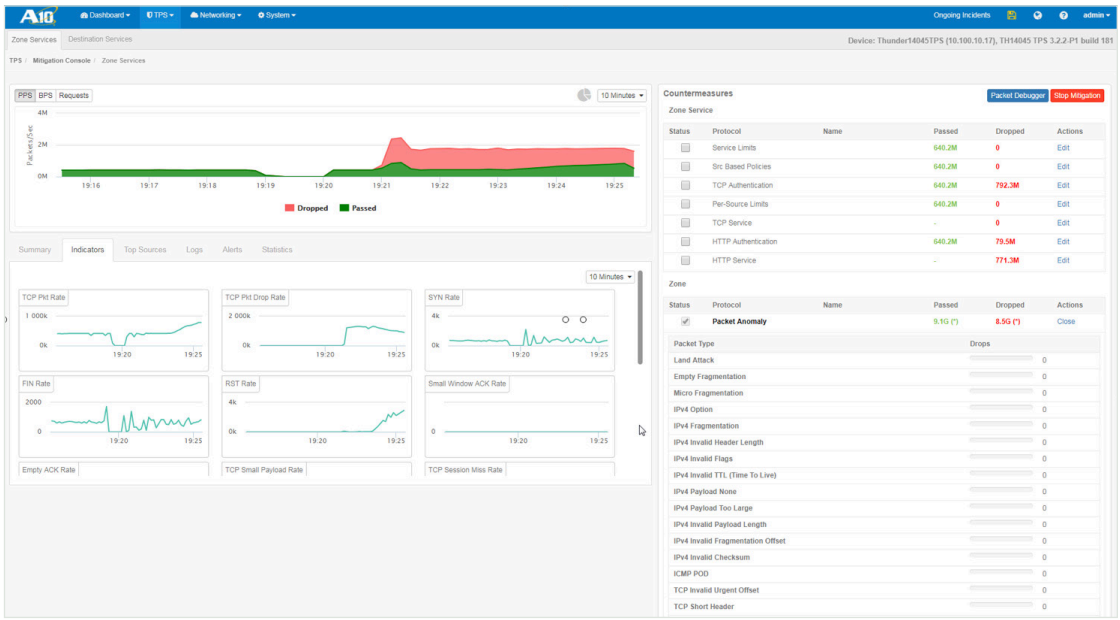
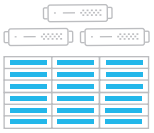
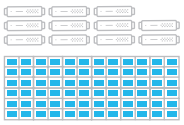


Figure 8: Thunder TPS mitigation console

KEY TAKEAWAYS

A10 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 busineses 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 VENDOR FLAGSHIP PLATFORMS

VENDOR & FLAGSHIP APPLIANCE	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 available	40 GbE 100 GbE
Rack units (RU)	3 RU	6 RU	2 RU	2 RU
Throughput	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 document's reading.*

Older, established vendors can't keep up with A10 Networks' innovation and continue to fall behind. The choice is clear. It is your money. Maximize your investment and get the best DDoS defense to protect against multi-vector attacks with precision and uncompromised scale.

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. A10 Thunder TPS offers the scalability and precision to defeat the most challenging multi-vector DDoS attacks to make your infrastructure resilient against DDoS attacks. Unlike outdated legacy DDoS protection products, Thunder TPS is built on A10's market-proven Advanced Core Operating System (ACOS) platform, which delivers scalable form factors and cost structures that make economic sense with a complete detection, mitigation and management solution.

A10 Networks Thunder 14045 TPS, the industry's highest performance DDoS defense appliance, was put to the test and was able to defeat DDoS attacks with precision and protect legitimate user at a rate of 310+ Gbps.

NOW YOU KNOW THE FACTS

Contact A10 and let's get started on a path to a more effective, scalable and cost effective approach to DDoS resilience.

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

ABOUT IXIA

Ixia, a Keysight Business, provides testing, visibility, and security solutions to strengthen networks and cloud environments for enterprises, service providers, and network equipment manufacturers.

Learn more at ixiacom.com.

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-WP-21144-EN-01 SEP 2017