THUNDER TPS

Next-generation DDoS Protection

Supported Platforms

Thunder TPS
physical appliance

aGalaxy
centralized management

APP

vThunder TPS

Overview

The Thunder TPS product line is a family of high-performance appliances that detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for your network infrastructure.

Thunder TPS support offerings include access to 24x7x365 support, DSIRT (DDoS Security Incident Response Team) assistance, and the A10 Threat Intelligence Service.

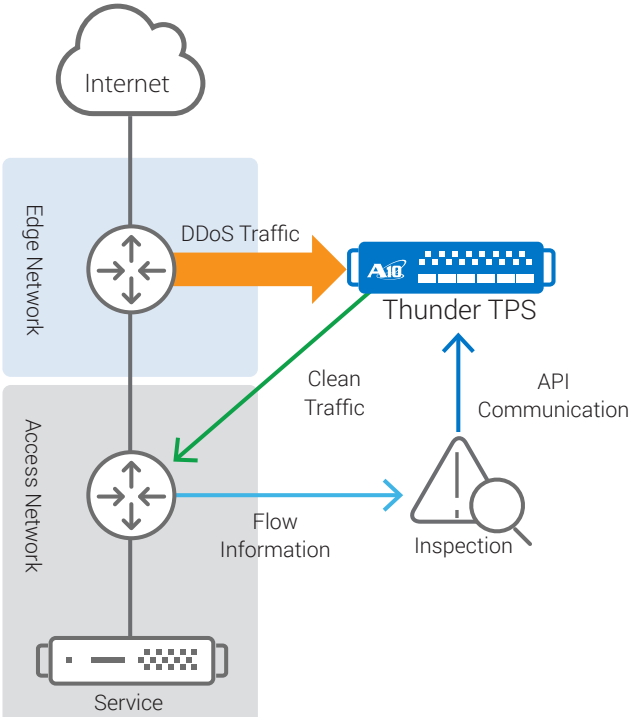
A10 Networks® Thunder TPS™ line of Threat Protection Systems provides agile and efficient, network-wide protection against the full spectrum of distributed denial of service (DDoS) attacks, including the challenging multi-vector attacks, which use a combination of high rate volumetric or network protocol attacks, and more sophisticated application attacks.

The Thunder TPS product line is built upon A10 Networks Advanced Core Operating System (ACOS®) platform, which delivers high performance and leverages a shared memory architecture to provide efficient tracking of network flows, as well as accurate DDoS protection enforcement for service providers, website operators and enterprises.

- **Full spectrum DDoS protection for service availability:** Organizations are increasingly dependent on the availability of their services, and on their ability to connect to the Internet. Downtime results in immediate revenue loss. Thunder TPS provides deep traffic analysis to automatically spot anomalies across the traffic spectrum, and protects against the full spectrum of attack vectors, including the extra challenging multi-vector attacks which leverage a combination of volumetric, protocol, and more sophisticated application-layer attacks, trying to take down the weakest link in your defenses.
- **High performance and efficiency to meet growing attack scale:** There is an undeniable increasing trend in DDoS attacks in terms of frequency, size and complexity. Thunder TPS, powered by ACOS, protects the largest, most demanding network environments. Performance scaling is maintained by distributing multi-vector detection and mitigation functions across optimal system resources. With the ability to offload common attack vectors to specialized hardware, the multicore, powerful CPU cores can focus on complex application layer attacks, which requires very resource-intense deep packet inspection (DPI) processing. Thunder TPS hardware appliances meet the highest demands, while being extremely efficient. The combination of high performance in a small form factor results in lower OPEX through significant lower power usage, reduced rack space and lowered cooling requirements.
- **Full control and smart automation for agile protection:** To easily integrate in various networking architectures, a vendor neutral, flexible DDoS mitigation solution is required. Various network deployment models for in- and out-of-band operations are available. With a RESTful API, aXAPI®, as well as leveraging open signaling standards, Thunder TPS enables integration to your custom or third-party detection solutions. The programmatic policy engine allows for fully customized policies leveraging regular expressions (regex) and Berkeley Packet Filter (BPF) pattern matching filters to perform application aware inspection. Several actions can be tied to a policy rule, such as running a script and/or DDoS signaling using BGP. This creates a powerful, automated yet flexible environment to quickly counteract adaptive attack strategies.

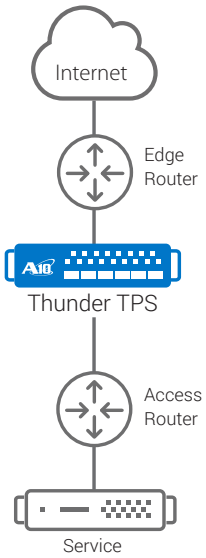
Architecture and Key Components

Asymmetric mode



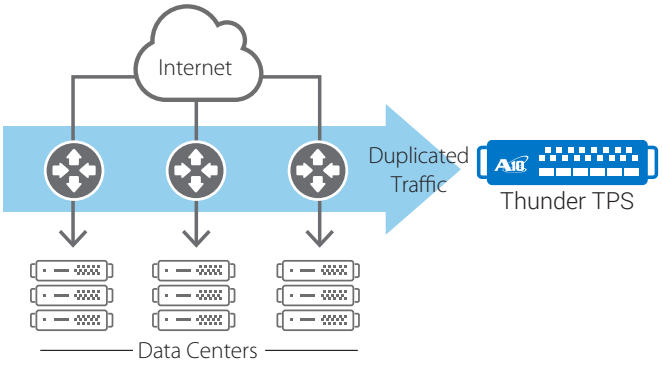
For on-demand, or permanent (proactive) mitigation, triggered manually or by flow analytical systems

Symmetric (Inline) mode



Provides continuous, comprehensive detection and mitigation, with more application-level attack mitigation options

Out-of-band (TAP) mode



For detailed telemetry analysis, define threshold violations, and synchronize white/black lists master to in-band Thunder TPS units

Features and Benefits

A10 Thunder TPS provides many features to detect and mitigate multi-vector DDoS attacks with unprecedented performance scalability and deployment flexibility.

Full Spectrum DDoS Protection for Service Availability

A10 Thunder TPS is able to detect and mitigate broad level of attacks, even if multiple attacks hit the network simultaneously.

- **Multi-vector attack protection:** Service availability is realized by detecting and mitigating DDoS attacks of many types, whether they are pure volumetric, protocol or resource attacks, or even application-level attacks. Hardware acceleration offloads the CPUs and make Thunder TPS particularly adept to deal with multi-vector attacks.
- **Smart threat detection and mitigation:** The system has access to a rich set of multi-protocol counters and behavioral indicators to learn peacetime network conditions, enabling precise detection of anomalies. Dynamic mitigation policies escalate suspect traffic through progressively tougher countermeasures to minimize legitimate traffic drops. DevOps can leverage event-triggered scripts for increased operational agility.
- **Granular connection rate protection:** Apply highly granular, multi-protocol rate limiting to prevent sudden surges of illegitimate traffic to overwhelm network and server resources. It is possible to apply limits per connection, defined by bandwidth or packet rate.
- **Hybrid DDoS Protection:** Volumetric attacks that exceed your network's capacity can be dealt with integrated DDoS Protection using Thunder TPS on premise and Verisign's cloud based DDoS Protection Services. The Verisign DDoS protection service is backed by global points of presence and multiple Tbps of global capacity.
- **A10 Threat Intelligence Service powered by ThreatSTOP.** This service combines and enhances reputation data from over three dozen security intelligence sources, including DShield and

Shadowserver, to enable Thunder TPS to instantly recognize and block traffic to and from known malicious sources.

A10's Threat Intelligence Service provides the following benefits:

- Protects networks from future threats
- Blocks non-DDoS related threats such as spam and phishing
- Increases Thunder TPS efficiency

With a threat intelligence network that continuously charts potential intruders on the Internet, customers can leverage global knowledge to block traffic from malicious Internet locations and offload Thunder TPS from identifying known bots and attack sources.

High Performance and Efficiency to Meet Growing Attack Scale

Over the last few years, DDoS attacks have rapidly proliferated in terms of bandwidth (Gbps) and packets per second (pps). Thunder TPS can leverage high-performance, specialized hardware as well as the latest, most powerful Intel Xeon CPUs to mitigate the largest and most sophisticated attacks. A10's Advanced Core Operating System (ACOS) platform enables efficient use of the specialized system resources.

- **High performance protection:** With mitigation throughput capacity ranging from 1 to 300 Gbps (or 2.4 Tbps in a list synchronization cluster) ensures that the largest, multi-vector DDoS attacks can be dealt with effectively. Select Thunder TPS models are equipped with high-performance FPGA-based FTA technology to detect and mitigate up to 60 common attack vectors immediately, before the data CPUs are involved. SYN cookies can be generated to validate client connection requests, at a rate of up to 440 Mpps. The Security and Policy Engine (SPE) hardware enforces highly granular traffic rates; as fine as 100 ms interval. SSL security processors are leveraged for detecting and mitigating SSL-based attacks, such as the POODLE vulnerability. More complex application-layer (L7) attacks (HTTP, DNS, etc.) are processed by the Intel Xeon CPUs, so that high-performance system scaling is maintained even for multi-vector attacks. Network connectivity is provided with 1, 10, 40 and 100 GbE interfaces.
- **Large threat intelligence class lists:** Eight individual lists, each containing up to 16 million list entries, can be defined. This allows a user to utilize data from intelligence sources such as the A10 Threat Intelligence Service, in addition to the dynamically generated entries of black/white lists.
- **Simultaneous protected objects:** To protect entire networks with many connected users and services, the Thunder TPS is able to simultaneously monitor 64,000 hosts or subnets.

Full Control and Smart Automation for Agile Protection

For network operators, it is critical that a DDoS mitigation solution can easily be inserted into the existing network architecture, so that the network remains prepared for imminent DDoS threats.

- **Programmatic Policy Engine:** Thunder TPS is able to perform application aware inspection on incoming packets and take defined actions to protect the application. For example, the system can enforce limits on various DNS query types, or apply security checks in many portions of the HTTP header. The detection and mitigation capabilities are extremely customizable, using regular expression (regex) and Berkeley Packet Filter (BPF) for high-speed pattern matching in policies. DevOps can leverage event-triggered scripts for increased operational agility.
- **Easy network integration:** With multiple performance options and flexible deployment models including MPLS inspection, Thunder TPS can be integrated into any network architecture, of any size. And, with aXAPI, A10's RESTful API, Thunder TPS can easily be integrated into third-party detection solutions.

  Leveraging open standards such as the BGP Blackhole functionality, Thunder TPS mitigation integrates easily with any DDoS detection solutions. Open APIs and networking standards support enables tight integration with many other devices, including SDN controllers and security products.
- **Centralized Management:** For larger deployments, our optional aGalaxy centralized management system ensures routine tasks can be performed at scale, across multiple appliances, regardless of physical location.

Product Description

The Thunder TPS product line is a family of high-performance appliances that detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for a network infrastructure.

Thunder TPS Hardware Appliances: The Thunder TPS line of hardware appliances protects large networks with entry-level models starting at 2 Gbps and moving up to a 300 Gbps high-performance appliance for your most demanding requirements. All models feature redundant power supplies*, solid-state drives (SSDs), and have no inaccessible moving parts for high availability. Select models benefit from our Security and Policy Engine (SPE) hardware acceleration, leveraging FPGA-based FTA technology among other hardware optimized packet processing to provide highly scalable flow distribution and hardware DDoS protection capabilities. Switching and routing processors provide high-performance network processing. Each appliance offers the best performance per rack unit, and "80 PLUS™ Platinum" certification* for power supplies to ensure a green solution and reduce power consumption costs. High density with 1, 10, 40 and 100 GbE port options are available to meet the highest networking bandwidth demands.

vThunder Virtual Appliances: The vThunder line of virtual appliances is designed to meet the growing needs of organizations that require a flexible and easy-to-deploy DDoS Protection solution running within a virtualized infrastructure. Each vThunder instance has the full set of DDoS protection features that can run atop your choice of commodity hardware and also your choice of leading hypervisor, for example, VMware ESXi and Microsoft Hyper-V.

* Except Thunder 840 TPS

Thunder TPS Hardware Appliance Specifications Table

	Thunder 840 TPS	Thunder 3030S TPS	Thunder 4435(S) TPS	Thunder 5435(S) TPS
Throughput	2 Gbps	10 Gbps	38 Gbps	77 Gbps
TCP SYN Auth/sec*1	1.5 million	6.5 million	35 million	35 million
SYN Cookie/sec*1	1.5 million	6.5 million	55 million	112 million
Network Interface				
1 GE Copper	5	6	0	0
1 GE Fiber (SFP)	0	2	0	0
1/10 GE Fiber (SFP+)	2	4	16	16
40 GE Fiber (QSFP+)	0	0	0	4
100 GE Fiber	0	0	0	0
Management Interface	Yes	Yes	Yes	Yes
Lights Out Management	No	Yes	Yes	Yes
Console Port	Yes	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes	Yes
Processor	Intel Communication Processor	Intel Xeon 4-core	Intel Xeon 10-core	Intel Xeon 10-core
Memory (ECC RAM)	8 GB	16 GB	64 GB	64 GB
Hardware Acceleration				
64-bit Linear Decoupled Architecture	Yes	Yes	Yes	Yes
Flexible Traffic Acceleration	Software	Software	1 x FTA-3+ FPGA	2 x FTA-3+ FPGA
Switching/Routing	Software	Software	Hardware	Hardware
SSL Security Processor ('S' Models)	N/A	Single	Dual	Dual
Hardware Bypass	Internal*3|*4 or External Option	External	External	External
Power Consumption (Typical/Max)*2	57W / 75W	131W / 139W	350W / 420W	400W / 480W
Heat in BTU/hour (Typical/Max)*2	195 / 256	447 / 474	1,195 / 1,433	1,365 / 1,638
Power Supply (DC option available)	Single 150W (AC only)	Dual 600W RPS	Dual 1100W RPS	Dual 1100W RPS
	100 - 240 VAC, 50-60Hz	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz		
Cooling Fan	Single Fixed Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.0 (W), 12 in (D)	1.75 in (H), 17.5 in (W), 17.45 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)
Rack Units (Mountable)	1U	1U	1U	1U
Unit Weight	8.8 lbs	20.1 lbs	34.5 lbs	35.5 lbs
Operating Ranges	Temperature 0° C - 40° C | Humidity 5% - 95%			
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, MSIP, EAC, FAC | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, MSIP, BSMI, RCM, EAC, NEBS | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, EAC, NEBS | RoHS
Standard Warranty	90-day Hardware and Software			

*1 Packets per second. Performance varies with deployment mode and configuration | *2 With base model. The value may vary with SSL and/or Hardware Bypass options |
*3 Hardware bypass model must be purchased for internal bypass function | *4 Available in Q4 2016 | ^ Certification in process

Thunder TPS Hardware Appliance Specifications Table (continued)

	Thunder 6435(S) TPS	Thunder 6635(S) TPS	Thunder 14045 TPS*4
Throughput	155 Gbps	155 Gbps	300 Gbps
TCP SYN Auth/sec*1	70 million	70 million	130 million
SYN Cookie/sec*1	223 million	223 million	440 million
Network Interface			
1 GE Copper	0	0	0
1 GE Fiber (SFP)	0	0	0
1/10 GE Fiber (SFP+)	16	12	0
40 GE Fiber (QSFP+)	4	0	4
100 GE Fiber	0	4 (CXP)	4 (CFP2 or QSFP28)
Management Interface	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Xeon Dual 12-core	Intel Xeon Dual 12-core	Intel Xeon Quad 18-core
Memory (ECC RAM)	128 GB	128 GB	512 GB
Hardware Acceleration			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	4 x FTA-3+ FPGA	4 x FTA-3+ FPGA	8 x FTA-3+ FPGA
Switching/Routing	Hardware	Hardware	Hardware
SSL Security Processor ('S' Models)	Quad	2 x Dual, 2 x Quad or 4 x Quad	TBD
Power Consumption (Typical/Max)*2	620W / 710W	995W / 1,150W	1,700W / 2,000W
Heat in BTU/hour (Typical/Max)*2	2,116 / 2,423	3,395 / 3,924	5,801 / 6,825
Power Supply (DC option available)	Dual 1100W RPS	2+2 1100W RPS	2+2 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz		
Cooling Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	5.3 in (H), 16.9 in (W), 28 in (D)	5.3 in (H), 16.9 in (W), 30 in (D)
Rack Units (Mountable)	1U	3U	3U
Unit Weight	39 lbs	74.5 lbs	102 lbs
Operating Ranges	Temperature 0° C - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, EAC, NEBS | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, EAC, FAC | RoHS	FCC Class A^, UL^, CE^, TUV^, CB^, VCCI^, China CCC^, BSMI^, RCM^ | RoHS^
Standard Warranty	90-day Hardware and Software		

*1 Packets per second. Performance varies with deployment mode and configuration | *2 With base model. The value may vary with SSL and/or Hardware Bypass options | *3 Hardware bypass model must be purchased for internal bypass function | *4 Available in Q4 2016 | ^ Certification in process

vThunder TPS Specifications

	vThunder TPS
Throughput	Up to 5 Gbps
Supported Hypervisors	VMware vSphere ESXi 5.5 or higher Microsoft Hyper-V on Windows Server 2008*1 or higher
Hardware Requirements	See installation guide
Licenses	Availability depends on hypervisor type. **Lab/Developer Editions:** 1 Gbps **Production Editions:** 1 Gbps, 2 Gbps and 5 Gbps*2
Standard Warranty	90-day Software

*1 Windows Server 2012 R2 is recommended for higher performance | *2 VMware ESXi only

Thunder 840 TPS

Thunder 3030S TPS

Thunder 4435(S) TPS

Thunder 5435(S) TPS

Thunder 6435(S) TPS

Thunder 6635(S) TPS

Thunder 14045 TPS (CFP2)

Thunder 14045 TPS (QSFP28)

Detailed Feature List*

(*Features may vary by appliance.)

High Performance, Scalable Platform

- ACOS Operating System
  - Multi-core, multi-CPU support
  - Linear application scaling
  - Linux on control plane
- ACOS on data plane
- IPv6 feature parity

Networking

- Asymmetric, symmetric, out-of-band (TAP)
- Transparent (L2), routed (L3)
- Routing: static routes, BGP4+
- VLAN (802.1Q)
- Trunking (802.1AX), LACP
- Access control lists (ACLs)
- Network Address Translation (NAT)
- MPLS traffic protection

Management

- Dedicated management interface (GUI, console, SSH, Telnet)
- Industry-standard Command Line Interface (CLI)
- SNMP, syslog, email alerts
- Port mirroring
- REST-style XML API (aXAPI) or SDK kit
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs

Flood Attack Protection

- SYN cookies
- SYN authentication
- ACK authentication
- Spoof detection
- SSL authentication*
- DNS authentication
- HTTP challenge
- TCP/UDP/ICMP flood protection
- Application (DNS/HTTP) flood protection
- Amplification attack protection

Protocol Attack Protection

- Invalid packets
- Anomalous TCP flag combinations (no flag, SYN/FIN, SYN frag, LAND attack)
- IP options
- Packet size validation (ping of death)
- POODLE attack

Resource Attack Protection

- Fragmentation attack
- Slowloris
- Slow GET/POST
- Long form submission
- SSL renegotiation

Application Attack Protection

- Application aware filter
- Regular expression filter (TCP/UDP/HTTP)
- HTTP request rate limit
- DNS request rate limit
- DNS query check
- HTTP protocol compliance
- HTTP anomalies

Protected Objects

- Protected zones for automated inspection and mitigation
- Source/destination IP address/subnet
- Source and destination IP pair
- Destination port
- Source port

Detailed Feature List* (continued)

(*Features may vary by appliance.)

- Protocol (HTTP, DNS, TCP, UDP, ICMP and others)
- DNS query type
- URI
- Class list/geo location
- Passive mode

Actions

- Capture packet
- Run script
- Drop
- TCP reset
- Dynamic authentication
- Add to black list
- Add to white list
- Log
- Limit concurrent connections
- Limit connection rate
- Limit traffic rate (pps/bps)
- Forward to other device
- Remote Triggered Black Hole (RTBH)

Telemetry

- Rich traffic and DDoS statistics counters
- sFlow v5
- netFlow (v9, IPFIX)
- Custom counter blocks for flow-based export
- High-speed logging
- CEF logging

Redirection

- BGP route injection
- IPinIP (source and terminate)
- GRE tunnel termination
- NAT

Detection/Analysis

- Manual thresholds
- Protocol anomaly detection
- Inspection within IPinIP
- Black/white lists
- IP/port scanning detection
- Traffic indicator and top talkers
- Mitigation console (GUI)
- Packet debugger tool

A10 Threat Intelligence Service**

- Dynamic updated threat intelligence feed, used by class-list

Advanced Hardware Highlights

- Redundant power supplies (AC or DC)*
- Smart fans (hot swap)*
- Solid-state drive (SSD)
- 1GbE, 1/10GbE, 40GbE and 100GbE ports
- Tamper detection*
- Lights Out Management (LOM/IPMI)*
- Hardware bypass*

*Features may vary by appliance
**Additional paid service

About A10 Networks

A10 Networks is a leader in application networking, 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, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com.**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DS-15101-EN-11
Oct 2016

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.